

Ad	Dijital Vatandaşlık Eğitici Eğitimi Katılımcı El Kitabı
Versiyon	Rehber, Basılı Materyal
Genel Koordinatör	Mustafa CANLI
Yayın Koordinatörü	Sümeyye Hatice ERAL
Bölüm Yazarları	Zeynep Beyza KARAKOÇ, Cem ATAY, Emine ÖZTÜRK, Gülfidan AYDIN, Kübra YİĞİT, Mustafa Kemal PİŞKİNER, Neslihan YILDIZ, Raziye GÜNEŞ, Semiramis PİJNENBURG
Editörler	Zeynep Beyza KARAKOÇ, Halime Gülçin BAYRAM, Neslihan YILDIZ
Proje Koordinatörü	Zeynep Beyza KARAKOÇ
Yayın Tarihi	
Yayıncı Adı	Millî Eğitim Bakanlığı D.S.İ. / Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
ISBN	978-975-11-8562-4
Lisans	Creative Commons Lisansı

Bu yayın Millî Eğitim Bakanlığı Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü tarafından hazırlanmıştır. Bu yayın Millî Eğitim Bakanlığının kurumsal görüşlerini yansıtmaz. Yayın içeriği tamamen yazarların sorumluluğu altındadır. Yayın ve referans olarak kullanılması kaynak gösterilmek şartıyla Millî Eğitim Bakanlığının iznini gerektirir. Yayın Creative Commons License Attribution – Noncommercial (CC-BY-NC) koşulları altında kullanıma sunulmuştur.

İçindekiler

Modül 1 Dijital Okuryazarlık

Modül 2 Dijital Sağlık

Modül 3 Dijital Erişim

Modül 4 Dijital İletişim

Modül 5 Dijital Ticaret

Modül 6 Dijital Güvenlik

Modül 7 Dijital Etik

Modül 8 Dijital Hukuk

Modül 9 Dijital Hak ve Sorumluluklar

Modül 10 Yetişkin Eğitimi ve Mahallî Eğitimler

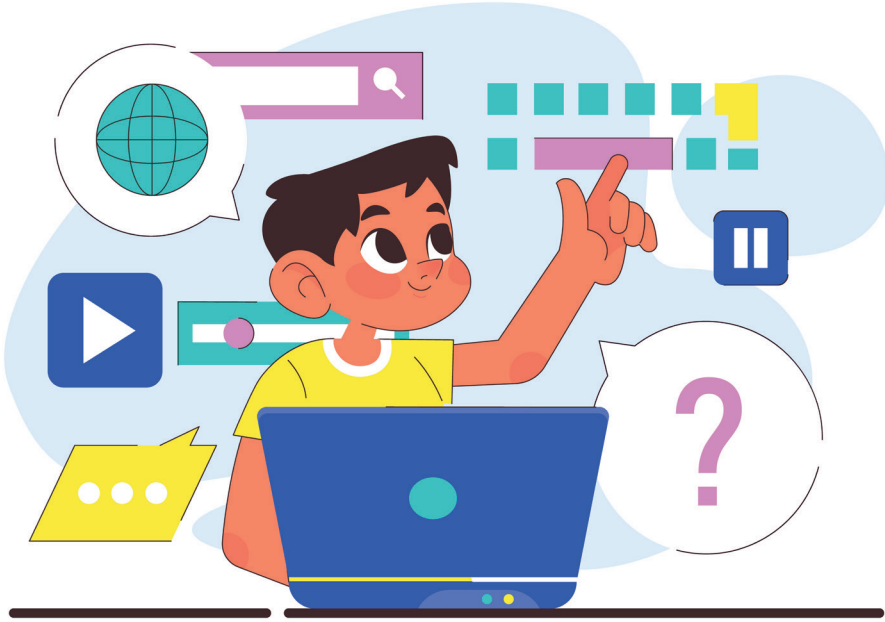


**T.C. MİLLÎ EĞİTİM
BAKANLIĞI**
Yenilik ve Eğitim Teknolojileri
Genel Müdürlüğü

DİJİTAL VATANDAŞLIK EĞİTİCİ EĞİTİMİ KATILIMCI EL KİTABI

MODÜL 1

Dijital Okuryazarlık



Modül Kapsamı

Bu modül, eğitimcilerin dijital okuryazarlık alanında beceri kazanmalarını sağlayacak bir eğitim programıdır. Dijital dünyada öğretmenlerin, öğrencilere gerekli olan bu becerileri kazandırmalarında yeterli bilgi ve donanımına sahip olmaları oldukça önemlidir. Dijital okuryazarlık kavramı dört başlık altında toplanmaktadır: Bilgi Okuryazarlığı, Eleştirel Okuryazarlık, Medya Okuryazarlığı ve Teknoloji Okuryazarlığı. Bilgi okuryazarlığı; doğru ve güvenilir bilgi kaynaklarına ulaşabilme, bu kaynakları etkili bir şekilde değerlendirme ve kullanma becerisidir. Eleştirel okuryazarlık; bilgi ve medya içeriklerine karşı eleştirel bir bakış açısı kazandırmak için bilgi ve medyayı sorgulama, analiz etme ve eleştirel düşünme becerilerini artırır. Medya okuryazarlığı; medya araçlarını kullanarak eğitimcinin kendi medya içeriğini oluşturmaları, medya üretimi süreçlerini anlamaları, medya içeriğini eleştirel olarak ele alması ve bilinçli medya kullanıcısı olmaya yönlendirmesini kapsar.

Öğrenme Kazanımları

- Dijital ortamlarda güvenilir bilgiye erişme ve bu bilgiyi etkin bir şekilde kullanma yeteneği kazandırmak.
- Dijital içerikleri eleştirel bir bakış açısıyla analiz etme ve doğru ile yanlış bilgiyi ayırt etme becerisini geliştirmek.
- Medya içeriklerini doğru anlama ve medya araçlarını etkin kullanma becerilerini kazandırmak.
- Dijital teknolojileri güvenli, verimli ve etik bir şekilde kullanmayı öğretmek.

İçerik Ağacı

Dijital Okuryazarlık

1. Bilgi Okuryazarlığı
2. Eleştirel Okuryazarlık
3. Teknoloji Okuryazarlığı
4. Medya Okuryazarlığı

Dijital Okuryazarlık

Dijital Okuryazarlık Nedir?

Dijital okuryazarlık, bireylerin dijital teknolojileri etkili ve bilinçli bir şekilde kullanarak bilgiye erişim sağlamalarını; bu bilgiyi doğru bir şekilde değerlendirip yeni içerikler üretebilmelerini, bu içerikleri paylaşabilmelerini ve uygulamaları güvenli kullanabilmelerini destekleyen geniş bir kavramdır (Üstündağ vd., 2017). Dijital okuryazarlık; bireylere sadece dijital araçları kullanmanın ötesinde, bu araçların sunduğu bilgileri analiz etme, kaynakları sorgulama ve aynı zamanda etik bir biçimde kullanma olanağı tanır (Özden, 2024).

Bu modül, dijital okuryazarlık becerilerinin öğrencilere kazandırılması sürecinde siz kıymetli öğretmenlerimize yol gösterici olması amacıyla hazırlanmıştır. Dijital araçların etkin ve etkili kullanımı, ulaşılan içeriğin analizinin yapılmasında izlenmesi gereken noktalar ve güvenilir kaynaklara nasıl ulaşılabileceğiyle ilgili konular üzerinde durulacaktır. Bu süreçte dijital okuryazarlık, dijital güvenlik ve dijital rehberlik konularında farkındalık oluşturmak önceliklendirilecektir.

1. Bilgi Okuryazarlığı

Bilgi okuryazarlığı; bireylerin bilgiye ulaşma, elde ettiği bilgiyi değerlendirme ve bilgiyi etkili kullanma becerisidir. Bilgiye erişimin kolaylaştığı dijital dünyada doğru bilginin seçilmesi ve güvenilir bilgiye ulaşma konusunda bilgi okuryazarlığı daha da önemli hâle gelmiştir. Bilgi okuryazarlığı; sadece internetten bilgi aramayı değil, bulunan bilginin sorgulanmasını, analiz edilmesini ve doğru bağlamda kullanılmasını da içerir.

İyi bir bilgi okuryazarı olmak, bilgiye erişme ve değerlendirme süreçlerini bilinçli bir şekilde yönetmeye dayanır. Öyleyse, bilgi okuryazarlığı; bilgi arama, değerlendirme ve etik kullanım becerileridir.

1.1. Bilgiye Erişim Yöntemleri ve Bilgi Arama Stratejileri Nelerdir?

- Bilgiye Erişim Yöntemleri, Bilgi Arama Stratejileri:** Arama motorları, veri tabanları ve çevrim içi kaynaklar, anahtar kelime seçimi, filtreleme ve sonuçları değerlendirme.
- Bilginin Güvenilirliği:** Kaynak güvenilirliği, bilimsel kaynaklar ve doğrulama yöntemleri.
- Bilgiyi Etik Kullanma:** Alıntılama kuralları, intihalden kaçınma ve dijital telif hakları.
- Dijital Bilgi Kaynakları:** Çevrim içi kütüphaneler, akademik veri tabanları, açık erişim platformları.
- Arama Motoru Kullanımı:** Arama motorlarında etkili bilgi arama teknikleri, filtreleme araçları ve ileri düzey arama seçenekleri.

- **Bilgi Arama Stratejileri:** Doğru anahtar kelimelerin seçimi, hedef odaklı arama stratejileri geliştirme, arama motoru algoritmalarını anlama.
- **Kaynak Güvenilirliği Kriterleri:** Bilgi kaynağının yazarı, yayımlayan kurum, kaynak tarihi ve referansların geçerliliği.
- **Bilimsel Kaynaklar ve Popüler Kaynaklar:** Bilimsel kaynaklar ile popüler medya kaynakları arasındaki farklar.
- **Doğrulama Yöntemleri:** Bilginin doğruluğunu kontrol etme yolları, üçüncü taraf doğrulama araçları (hikâye doğrulama siteleri, veri tabanları).

Modüllerde birden fazla etkinlik seçeneği sunulmuştur, uygun bulduğunuz etkinliği kullanabilirsiniz.



Etkinlik

Tablo 1. Gerçek ve sahte haberler arasında farkı ayırt etme üzerine grup çalışması

	Kaynağın güvenilirliği: Haberi yayımlanan web sitesi veya yazar güvenilir mi?	
	Başlık: Haber başlığı sansasyonel mi? İlgiyi çekmek için abartılı ifadeler mi kullanıyor?	
	İddiaların doğruluğu: Haberin içeriği doğrulanabilir mi? Kaynaklar belirtilmiş mi?	
	Resimler ve videolar: Haberde kullanılan görsellerin orijinal olup olmadığını kontrol edin(örneğin, tersine görsel arama yaparak).	
	Yayın tarihi: Haber güncel mi, yoksa eski bir haber mi tekrar paylaşıyor?	

Katılımcılar, çeşitli web siteleri ve akademik makalelerden örnekler inceleyerek güvenilirlik değerlendirmesi yaparlar.

İnceleme Süreci

Grup Çalışması: Katılımcılar küçük gruplara ayrılır, her grup diğer gruba incelemek ve güvenilirlik kriterleri açısından değerlendirilmek üzere güvenilir ve güvenilir olmayan iki kaynak iletir. Gruplar materyali değerlendirir. Gruplar, belirlenen kriterler doğrultusunda kaynakları incelemeye başlar.

Her grup, web sitesinin/makalenin güvenilirlik seviyesini sorgulamak için kriterlere göre ayrı ayrı analiz yapar. Kaynakları değerlendirmek için tersine görsel arama gibi teknikleri kullanabilirler. Bu, görsellerin başka bir bağlamda kullanılıp kullanılmadığını anlamalarına yardımcı olur.

Sunum: Gruplar raporlarını sınıfla paylaşır ve hangi kaynakları güvenilir bulduklarını, hangi kaynakları güvenilir bulmadıklarını ve bunun nedenlerini açıklayarak sınıfta tartışır.

1.2. Bilgi Nasıl Organize Edilir ve Nasıl Kullanılır?

Bilgiyi organize etme ve kullanma, dijital çağda etkili bilgi yönetimi ve sunum becerilerini gerektirir. Bilginin düzenlenmesi, sunulması, saklanması ve etik kullanımı bireysel ve kurumsal başarının temel taşlarından biridir.

- **Bilgi Yönetimi Araçları:** Dijital ortamda bilgi organizasyonu için kullanılan araçlar.
- **Bilginin Etkili Sunumu:** Bilgiyi etkili bir şekilde düzenleyerek sunma, grafik ve tablo kullanımı.
- **Bilgiyi Saklama ve Arşivleme:** Bilgi depolama ve dijital arşiv oluşturma yöntemleri.
- **Alıntılama Kuralları:** Bilgiyi etik bir şekilde kullanma, intihalden kaçınma, kaynak gösterme ve alıntı yapma teknikleri.
- **Telif Hakları ve Dijital Telif:** Dijital dünyada telif hakları, Creative Commons lisansları ve dijital içeriklerin kullanımıyla ilgili yasal düzenlemeler.
- **Dijital Bilgi Paylaşımı:** Bilgi paylaşırken dikkat edilmesi gereken etik ilkeler, sosyal medya ve bloglar üzerinden doğru bilgi yayma.



Etkinlik

Dijital içeriklerin etik kullanımı üzerine grup çalışması (Creative Commons lisanslarının uygulamaları).

- **Katılımcılar dijital not alma ve bilgi yönetim araçlarını kullanarak bir proje hazırlarlar.**
- **Farklı bilgileri bir araya getirip etkili bir sunum veya rapor oluşturma üzerine çalışma yapılır.**

- Bilgilerin güvenli bir şekilde depolanması ve düzenlenmesi üzerine uygulamalar planlanır.
- Katılımcılar, belirli bir konuda araştırma yaparak doğru alıntı yapma ve kaynak gösterme yöntemlerini uygularlar.

Örnek makaleler üzerinden intihal kontrolü yapılır, intihalin nasıl önleneceği konusunda pratik yapılır.

Adımlar:

1. Giriş ve Bilgilendirme

- **Creative Commons nedir?**
 - o Creative Commons (CC); içerik üreticilerine, eserlerini nasıl kullanabileceğini belirleme özgürlüğü tanıyan lisans türleridir. Bu lisanslar; telif hakkıyla korunan eserlerin belirli kurallara uygun olarak başkaları tarafından paylaşılmasını, kopyalanmasını ve yeniden kullanılmasını sağlar.
- **Creative Commons Lisans Türleri:**
 - o **CC BY (Atıf):** İçerik, orijinal kaynağa atıf yapılarak kullanılabilir.
 - o **CC BY-SA (Atıf – Benzer Paylaşım):** İçerik, aynı lisans koşullarında paylaşıldığı sürece atıf yapılarak kullanılabilir.
 - o **CC BY-ND (Atıf – Türetilemez):** İçerik, atıf yapılarak kullanılabilir ancak değiştirilmesine izin verilmez.
 - o **CC BY-NC (Atıf – Ticari Olmayan):** İçerik, atıf yapılarak kullanılabilir ancak ticari amaçla kullanılamaz.
 - o **CC BY-NC-SA:** Ticari olmayan amaçlarla atıf yapılarak kullanılabilir ve aynı lisans koşulları altında paylaşılmalıdır.
 - o **CC BY-NC-ND:** İçerik; ticari olmayan amaçlarla, değiştirilmeden ve atıf yapılarak kullanılabilir.



Etkinlik

Grup Çalışması

Kursiyerler 3-4 kişilik küçük gruplara ayrılır. Her gruba bir veya daha fazla dijital içerik (görsel, video, makale, vb.) örneği verilir. Bu içerikler farklı CC lisanslarına sahip olmalıdır. Gruplardan, verilen içeriklerin Creative Commons lisanslarını incelemeleri ve bu lisanslar doğrultusunda içeriği nasıl kullanabileceklerini tartışmaları istenir.

Görevler:

- İçeriğin hangi Creative Commons lisansına sahip olduğunu tespit etmek.
- Lisansın koşullarını analiz etmek: Bu içerik nerede ve nasıl kullanılabilir?
- İçeriğin etik ve yasal olarak nasıl paylaşılabileceği veya yeniden nasıl kullanılabileceği üzerine tartışmak.
- Örnek: CC BY-SA lisanslı bir görseli bir blog yazısında nasıl kullanırsınız? Atıf yapmanız gereken yerler neresi olur?

Uygulama ve Tartışma

Gruplar, verilen içeriklerin lisanslarına göre nasıl kullanılması gerektiğini tartıştıktan sonra kendi örnekleri üzerinden etik kullanım yollarını sınıfa sunar. Sunum sırasında:

- Hangi Creative Commons lisansını tespit ettiklerini ve bunun anlamını açıklarlar.
- İçeriği nasıl kullanabilecekleri üzerine görüşlerini belirtirler.
- Creative Commons lisanslarının içerik üreticileri ve kullanıcıları açısından nasıl faydalı olduğunu tartışırlar.



Etkinlik

Creative Commons Lisanslarının Uygulamalı Kullanımı

Gruplardan, kendi içeriklerini yaratmalarını ve bu içeriklere uygun bir Creative Commons lisansı eklemelerini isteyin. Örneğin; öğrenciler bir fotoğraf, video veya makale hazırlayarak bu içerikleri için uygun bir Creative Commons lisansı seçebilirler.

Sorular: Hangi CC lisansını seçtiler ve neden? İçeriklerinin nasıl kullanılmasını istiyorlar?

Aşağıdaki tablo bilgiye erişim, bilgiyi değerlendirme ve etik bir şekilde kullanma süreçlerini daha bilinçli hâle getirmek için tasarlanmıştır. Öğrencileriniz bir bireyin veya grubun topladığı bilgilerin güvenilirliğini ve doğruluğunu nasıl analiz etmesi gerektiği konusunda tereddüte düştüğünde bu tablodan yararlanabilirler. Tablonun çıktısı alınarak sınıfta görünür bir yere asılabilir.

ADIM	SORU	KONTROL
Bilgiye Eriřim	Doğru arama terimlerini kullandım mı? Güvenilir bilgi kaynaklarına erişebildim mi?	
Bilgiyi Değerlendirme	Elde ettiğim bilgiyi sorguladım mı? Yeterince analiz ettim mi?	
Kaynağın Güvenilirliğini Kontrol Etme	Bilgiyi sağlayan yazar ve kuruluş güvenilir mi?	
Bilginin Güncelliğini Değerlendirme	Bilgi güncel mi? Eski veya geçerliliğini yitirmiş olabilir mi?	
Çapraz Kaynak Kontrolü	Bilgiyi farklı kaynaklarla karşılaştırdım mı? Doğrulama yaptım mı?	
Bilginin Tarafsızlığını Sorgulama	Bilgi tarafsız mı yoksa belirli bir ideolojiye veya grubun çıkarına mı hizmet ediyor?	
Bilgiyi Etik Kullanma	Bilgiyi etik bir şekilde kullandım mı? Başkasının emeğine saygı gösterdim mi?	
Doğru Alıntılama ve Kaynak Gösterme	Doğru alıntı yaptım mı ve kaynak gösterdim mi? İntihalden kaçındım mı?	
Bilgiyi Düzenleme ve Organize Etme	Bilgiyi düzenli ve sistematik bir şekilde organize ettim mi?	



2. Eleştirel Okuryazarlık

Eleştirel okuryazarlık; bireylerin dijital ve basılı ortamlarda karşılaştıkları bilgiyi sorgulama, analiz etme ve eleştirel bir bakış açısıyla değerlendirme yeteneğini tanımlayan önemli bir beceridir.

2.1. Eleştirel Düşünme Nedir ve Sorgulama Becerileri Nelerdir?

Eleştirel düşünme; bireylerin bilgiyi değerlendirme, analiz etme, yorumlama ve akıl yürüterek doğru sonuçlara ulaşma becerisidir. Bu beceri, özellikle dijital bilgi çağında yanıltıcı ve yanlış bilgileri ayırt etmek için hayati bir öneme sahiptir.

- **Eleştirel düşünmenin temelleri:** Bilgiyi sorgulama, alternatif bakış açıları geliştirme.
- **Bilginin kaynağını ve doğruluğunu sorgulama:** Kim söylüyor? Neden söylüyor? Söylenen ne kadar güvenilir?
- **Ön yargı ve yanıltıcı bilgilere karşı dikkatli olma:** Bilgiyi yayarken ya da analiz ederken ideolojik veya duygusal manipölasyonlara karşı farkındalık geliştirme.
- **Soru sorma teknikleri:** Bilgiyi derinlemesine analiz edebilmek için hangi soruların sorulması gerektiğini bilme.



Etkinlik

Katılımcılar 3-4 kişilik gruplara ayrılarak belirli bir medya içeriğini alır ve içerikteki eksik bilgiyi, ön yargı ve manipölasyon unsurlarını bulmaya çalışır. Farklı bakış açılarına sahip içerikleri karşılaştırarak içeriklerin ortak noktalarını ve çelişkilerini analiz ederler.

2.2. Bilgi Manipölasyonu ve Yanlış Bilgi (Dezenformasyon)

Yanlış bilginin yayılması, bireylerin ve toplumların dijital platformlardaki güvenilir bilgiye erişimini zorlaştıran önemli bir sorundur. Bu başlık altında bilgi manipölasyonu ve yanlış bilgiye dair temel kavramlar, bu tür bilgilerin nasıl yayıldığı ve bilgiyi doğrulama yöntemleri ele alınmaktadır.

- **Yanlış bilgi türleri:** Dezenformasyon (bilerek yanlış bilgi yayma), manipölasyon, eksik bilgi.
- **Dijital ortamlarda yanlış bilginin yayılması:** Sosyal medya, bloglar ve forumlar gibi platformlardaki yanlış bilgi yayılma dinamikleri.
- **Tıklama tuzağı ve sahte haberler:** Yanıltıcı başlıklar ve içeriklerin tespit edilmesi.
- **Doğrulama yöntemleri:** Hikâye doğrulama siteleri ve doğrulama araçlarının kullanımı.



Etkinlik

- Katılımcılar çeşitli haber ve içerik platformlarından örnekler inceler, sahte haberleri tespit etmeye çalışırlar.
- Sosyal medyada hızla yayılan bir bilgi üzerinde çalışarak bu bilginin doğruluğunu çapraz kaynak kontrolüyle araştırırlar.

2.3. Medya ve İdeolojik Mesajları Analiz Etme

Medya okuryazarlığı bireylerin medya içeriklerini analiz etme, değerlendirme ve bilinçli tüketme becerisidir. Eleştirel bir bakış açısı geliştirmek için aşağıdaki noktalara dikkat etmeliyiz.

- **Medya okuryazarlığı ve eleştirel bakış açısı:** Medya içeriklerinin analizinde dikkat edilmesi gereken unsurlar.
- **Medya manipülasyon teknikleri:** Görsel ve dilsel manipülasyonlar, haberlerde kullanılan yanıltıcı dil.
- **İdeolojik mesajları ayırt etme:** Medyada yer alan içeriklerin arka planındaki ideolojik çıkarları analiz etme.
- **Toplumsal mesajlar ve stereotipler:** Medyanın topluma dayattığı kalıp yargıları ve mesajları analiz etme.



Etkinlik

- Farklı medya kanallarından alınan haberler ve içerikler karşılaştırılarak hangi mesajların ideolojik ya da yanlı olduğu tartışılır.
- Katılımcılar, medya içeriklerinde kullanılan dil ve görsellerin analizini yaparak olası manipülasyonları ve taraflı mesajları incelerler.

2.4. Eleştirel Okuryazarlık

- **Toplumda eleştirel düşünceye katkı:** Eleştirel düşünen bir birey olarak topluma sağlanabilecek katkılar.
- **Sosyal medya okuryazarlığı:** Sosyal medya içeriklerini analiz etme, sosyal medyada doğru bilgi paylaşımı.



Etkinlik

- Katılımcılar, sosyal medyada karşılaştıkları güncel olaylara ilişkin içerikleri analiz ederek eleştirel düşüncelerini paylaşır.
- Grup çalışmaları ile dijital etik ve sorumlu vatandaşlık üzerine tartışmalar yürütülür.

Eleştirel Okuryazarlık (Nasıl Sorgulamalıyım?)

Durum: Aynı politik olayı farklı iki haber kaynağından izlediğinizi düşünün. Eleştirel okuryazar; kaynakların olaylara farklı açılardan baktıklarını fark eder ve her iki kaynağın da kendi perspektiflerini temsil ettiğini bilir, yankı odalarından kaçınmayı hedefler.	Soru: Haberi sunan kişi veya kuruluşun bakış açısı nedir? Bu kişi veya kuruluşun benzer konularda tutumları nedir?
Durum: Sosyal medya platformunda karşımıza çıkan, tanınmış bir kişiye ait olduğu iddia edilen alıntılar. Eleştirel okuryazar, bu alıntının doğru olup olmadığını anlamak için kaynak arar.	Soru: Bu içerik doğru mu? Bilginin kaynağı güvenilir mi? Alternatif kaynaklardan doğrulama yapmalı mıyım?
Durum: Televizyonda bir cilt bakım ürününün mucizevi etkilerinden bahseden bir reklam izliyorsunuz. Eleştirel okuryazar, bu ürünün gerçekten iddia ettiği gibi etkili olup olmadığını sorgular ve reklamda sunulan bilgileri araştırır.	Soru: Reklamda kullanılan dil gerçekçi mi yoksa abartılı mı? Bu ürünle ilgili tarafsız kaynaklardan daha fazla bilgi edinebilir miyim?
Durum: “Bu yöntemle beş günde zengin oldu!” şeklinde bir başlıkla karşılaşan eleştirel okuryazar, başlığı hemen kabul etmek yerine içeriğin gerçekçi olup olmadığını anlamak için daha fazla bilgi arar.	Soru: Bu başlık içerikle ne kadar örtüşüyor? Başlık okuyucuyu yanıltmak için mi kullanılmış?
Durum: Bir araştırma raporu okurken eleştirel okuryazar araştırmanın finansörlerini, kullanılan yöntemlerini ve raporun olası yanlılıklarını analiz eder.	Soru: Bu araştırma kim tarafından finanse edilmiş? Kullanılan yöntemler bilimsel mi?



3. Teknoloji Okuryazarlığı

Teknoloji okuryazarlığı, bireylerin dijital teknolojileri etkin ve verimli kullanabilme becerisidir. Öğrencilerin bu beceriyi kazanmaları, günümüz bilgi çağında başarılı bir birey olmaları için önemlidir. Eğitimcilerin teknoloji okuryazarlığı becerilerini kazanmaları ve bu becerileri öğrencilere etkili şekilde aktarabilmeleri önem arz etmektedir. Teknoloji okuryazarlığı; dijital cihazların, yazılımların ve çevrim içi kaynakların bilinçli bir şekilde kullanılmasını, dijital etik kurallara uyulmasını ve dijital güvenlik farkındalığı geliştirilmesini kapsar.

3.1. Dijital Güvenlik ve Etik

Dijital güvenlik ve etik bireylerin çevrim içi dünyada güvenli, bilinçli ve sorumlu bir şekilde var olmalarını sağlamak için gerekli bilgi ve becerileri kapsar. Dijital çağda; bireylerin kişisel bilgilerini koruması, çevrim içi tehditlere karşı önlem alması ve etik kurallara uygun hareket etmesi hayati önem taşır.

- **Güvenli İnternet Kullanımı:** Güvenli internet kullanımı kişisel bilgilerin korunması, sosyal medya ve çevrim içi platformlarda güvenlik önlemleri gibi konuları kapsar. Bu kapsamda özellikle iki kavramın öneminden bahsedebiliriz.
- **Kişisel Verilerin Korunması:** Çevrim içi platformlarda kimlik bilgileri, adres, telefon numarası gibi hassas verilerin paylaşımından kaçınılmalıdır.
- **Sosyal Medya Güvenliği:** Güçlü şifreler kullanmak, hesapları iki faktörlü kimlik doğrulama ile korumak ve gizlilik ayarlarını düzenlemek temel önlemler arasındadır.
- **Siber Tehditler:** Oltalama (phishing), kötü amaçlı yazılım (malware), virüsler ve bilgisayar korsanlarına karşı nasıl korunulacağı anlatılır. Eğitimcilerin bu tehditleri öğrencilere nasıl aktarabileceği üzerinde durulur.
- **Dijital Etik:** Çevrim içi dünyada etik kuralların önemi, sosyal medya platformlarında doğru davranış, dijital ayak izi, çevrim içi itibar gibi konular ele alınır. Eğitimciler, öğrencilerine çevrim içi ortamda nasıl sorumlu bir birey olacaklarını öğretirler.



Etkinlik

Dijital Etik Draması

- **Amaç:** İnternette etik kurallara uygun davranmanın önemini öğretmek.
- **Aktivite:** Katılımcılar gruplara ayrılır, çevrim içi ortamlarda yaşanabilecek bir durumu ele alarak bir senaryo oluştururlar. Bu senaryolar, dijital dünya sorunlarını ve etik davranışları ele alır. Her grup senaryosunu sahneler ve diğer katılımcılar etik olmayan davranışları belirleyip tartışır.

Veri Hikâyeleri Yaratma

- **Amaç:** Verilerin ne kadar güçlü olduğunu göstermek.
- **Aktivite:** Katılımcılara anonim veri setleri verilir ve bu verileri kullanarak yaratıcı hikâyeler oluşturmaları istenir. Bu sayede verilerden hangi sonuçların çıkarılabileceği ve bu sonuçların nasıl yanlış yorumlanabileceği üzerine bir tartışma yapılır.



Etkinlik

1.1.1 Teknoloji Okuryazarlığı Testi

Kolay Sorular (1 Puan)

1. Aşağıdakilerden hangisi güçlü bir şifre oluşturmanın en iyi yoludur?
 - a) İsminizi ve doğum yılınızı kullanmak.
 - b) Kısa ve kolay hatırlanacak bir kelime seçmek.
 - c) Harf, rakam ve sembol karışımı kullanmak.
 - d) Şifreyi bir yere yazıp saklamak.
2. Aşağıdakilerden hangisi iki faktörlü kimlik doğrulamanın (2FA) amacıdır?
 - a) Hesabınızı çift kişiye açık hâle getirir.
 - b) Ekstra bir güvenlik katmanı ekler.
 - c) İnternet hızınızı artırır.
 - d) Telefonunuza virüs bulaştırır.

3. Oltalama (phishing) saldırısı nedir?

- a) Güvenlik yazılımının bilgisayar taraması.
- b) Gerçek bir web sitesine benzer sahte siteler veya e-postalar aracılığıyla kişisel bilgi çalmaya çalışma.
- c) Bilgisayarın yavaşlamasına neden olan bir virüs türü.
- d) Sadece sosyal medya hesaplarını hedef alan bir saldırı türü.

4. Hangi sıklıkta şifre değiştirmek en güvenli yöntemdir?

- a) Hiç değiştirmemek.
- b) 1 yılda bir değiştirmek.
- c) Düzenli olarak, özellikle şüpheli bir durum olduğunda değiştirmek.
- d) Her gün değiştirmek.

5. Aşağıda HTTPS kontrolü ile ilgili verilenlerden hangisi doğrudur?

- a) Güvenli internet taraması sağlar.
- b) Tarayıcı hızını artırır.
- c) Spam e-postaları filtreler.
- d) Bilgisayarın şarj süresini uzatır.

Orta Zorlukta Sorular (2 Puan)

6. Aşağıdakilerden hangisi bir cihazı açık Wi-Fi ağında kullanırken oluşabilecek bir güvenlik riskidir?

- a) İnternet hızının düşmesi.
- b) Bilgilerinizin başkaları tarafından izlenebilmesi.
- c) Cihazın aşırı ısınması.
- d) Pil ömrünün azalması.

7. Aşağıdakilerden hangisi güçlü şifre oluşturma kurallarından birisidir?

- a) Aynı şifreyi tüm hesaplar için kullanmak.
- b) En az on iki karakter kullanmak.
- c) Şifreyi sadece büyük harflerden oluşturmak.
- d) Şifreyi her ay değiştirmek.

8. Bir e-posta ekini açmadan önce ne yapmalısınız?

- a) Zaman kaybetmemek için hemen açmalısınız.
- b) E-posta adresinin güvenilir olup olmadığını kontrol etmelisiniz.
- c) E-posta konusu ilgini çekiyorsa hemen indirip açabilirsiniz.
- d) Virüs taraması yapmadan açabilirsiniz.

9. Bir sosyal medya platformunda konum bilgilerinizi paylaşmanın en güvenli yolu nedir?

- a) Her zaman konumunuzu açık tutmak.
- b) Sadece güvendiğiniz kişilerle gerektiğinde paylaşmak.
- c) Konumunuzu sürekli gizli tutmak.
- d) Tüm takipçilerinizle paylaşmak.

10. Bir bilgisayarın zararlı yazılımla enfekte olup olmadığını nasıl anlarsınız?

- a) Bilgisayar daha yavaş çalışmaya başlar.
- b) Sık sık istenmeyen pop-up pencereleri görünür.
- c) Hepsi
- d) Hiçbiri

Zor Sorular (3 Puan)

11. Aşağıdakilerden hangisi kimlik avı saldırısından korunmanın en etkili yoludur?

- a) Bilinmeyen kişilerden gelen e-postaları açmamak.
- b) Bilgisayarınızı düzenli olarak yeniden başlatmak.
- c) Bilgisayarınızdaki güvenlik yazılımını güncel tutmak.
- d) Tüm e-postaları açmadan silmek.

12. Şifre yöneticisi ne işe yarar?

- a) Tüm şifrelerinizi kolayca hatırlamanızı sağlar.
- b) Güçlü şifreler oluşturur ve bu şifreleri güvenli saklar.
- c) Bilgisayar hızını artırır.
- d) İnternet bağlantısını hızlandırır.

13. Aşağıdaki durumlardan hangisi zararlı bir yazılımın (malware) bulaşma yollarından biridir?

- a) Güvenilir olmayan bir web sitesinden dosya indirmek.
- b) Bilgisayarın uzun süre çalışıyor olması.
- c) İnterneti sürekli açık bırakmak.
- d) Yüksek hızda internet kullanmak.

14. Eğer bir bilgisayarda fidye yazılımı (ransomware) varsa aşağıdakilerden hangisinin olması beklenir?

- a) Bilgisayarınız aniden kapanır.
- b) Bilgisayarınızdaki dosyalar şifrelenir ve şifreyi açmak için para ödemeniz istenir.
- c) Bilgisayarınızın işlemcisi yanar.
- d) İnternet bağlantınız yavaşlar.

15. Dark Web nedir?

- a) İnternetin genel halk tarafından erişilemeyen bir kısmıdır.
- b) Hızlı internet bağlantısı sağlanan bir ağıdır.
- c) Tüm dünyadaki bilgisayar ağlarının adıdır.
- d) Güvenli alışveriş yapılan bir internet bölgesidir.

3.2 Veri Yönetimi ve Bulut Teknolojileri

- **Veri Güvenliği:** Kişisel verilerin güvenli şekilde saklanması ve yedeklenmesini ifade eder. Verileri bulut ortamında güvenli şekilde depolamanın ve şifrelemenin yolları açıklanır.
- **Bulut Teknolojileri:** Eğitimciler; Google Drive, OneDrive, Dropbox gibi bulut hizmetlerini nasıl kullanacaklarını öğrenirler. Ayrıca bulut sistemlerinin öğrenci projeleri, dosya paylaşımı ve öğretmenler arasındaki iş birliği için nasıl kullanılabileceği gösterilir.

3.3. Dijital İletişim Araçları

Dijital iletişim araçları; modern eğitim ve iş dünyasında bilgi paylaşımı, iş birliği ve etkili iletişim için temel bir rol oynar (Bayrakçı ve Narmanlıoğlu, 2021). Ancak bu araçların verimli ve güvenli bir şekilde kullanılması, bireylerin dijital becerilerinin geliştirilmesiyle mümkün olur.

- **E-posta Kullanımı ve Güvenliği:** Profesyonel e-posta yazma kurallarını, e-posta güvenliğini (spam, kimlik avı e-postaları) ve e-posta yönetimini içerir.
- **Çevrim İçi Toplantı Araçları:** Zoom, Microsoft Teams gibi çevrim içi toplantı araçlarının nasıl kullanılacağı; uzaktan eğitimde verimliliği artırmak için bu platformların nasıl yönetileceği gösterilir.
- **Sosyal Medya Kullanımı:** Sosyal medya platformlarının eğitimde nasıl kullanılacağına, öğrencilerle bilgi paylaşımı ve güvenli sosyal medya kullanımına dair bilgiler sunulur.



4. Medya Okuryazarlığı

Medya okuryazarlığı; bireylerin medya içeriklerini anlama, analiz etme, değerlendirme ve bu içeriklere eleştirel bir bakış açısıyla yaklaşma becerilerini geliştiren önemli bir yeterliliklerdir. Medya okuryazarlığı sayesinde dijital ve geleneksel medya kanallarındaki mesajların nasıl üretildiğini, nasıl yayıldığını ve bu mesajların bireyler üzerindeki etkilerini anlamak mümkün olur. Bu modül, katılımcıların medya okuryazarlığı becerilerini geliştirmeyi amaçlamaktadır.

4.1. Medya İçeriklerinin Anlaşılması ve Çözümlemesi

Medya içeriklerinin anlaşılması ve çözümlemesi, bireylerin medya mesajlarını bilinçli bir şekilde değerlendirmelerini sağlar. Medya; kullandığı dil, görsel unsurlar ve semboller aracılığıyla belirli mesajlar ve anlamlar ileterek bireylerin düşünce ve davranışlarını etkileyebilir (Buckingham, 2015). Bu mesajlar genellikle editoryal süreçler ve ticari amaçlar doğrultusunda şekillenir. Bu nedenle, medya mesajlarının nasıl oluşturulduğunu ve hangi amaçlarla sunulduğunu anlamak eleştirel medya okuryazarlığı için temel bir beceridir. Medya içeriklerini çözümlemek, bireylerin farkındalığını artırarak bilgiye daha bilinçli ve sorgulayıcı bir şekilde yaklaşmalarına olanak tanır. Aşağıda bu konuyla ilgili önemli kavramlar verilmiştir.

- **Medya Mesajları:** Medya içeriklerinde kullanılan dilin, sembollerin ve görsel unsurların analizi.
- **Medya Üretim Süreci:** Haberlerin ve medya içeriklerinin nasıl oluşturulduğu, editoryal süreçler ve medyanın ticari amaçları.
- **Medya Okuryazarlığının Temel İlkeleri:** Medya mesajlarının nasıl okunup çözümlenebileceğini öğrenme.



Etkinlik

- Katılımcılar; gazete haberleri, televizyon reklamları ve sosyal medya içerikleri üzerinde inceleme yaparak bu içeriklerin alt metinlerini ve sembolik anlamlarını analiz ederler.
- Farklı medya kanallarında yer alan bir haberin, farklı açılardan nasıl ele alındığını incelerler.

4.2 Medyada Kullanılan Manipülasyon Teknikleri

Medya; bilgi iletiminin güçlü bir aracı olmasının yanı sıra, bazen toplumsal algıyı yönlendirme amacıyla manipülasyon teknikleri de kullanır. Bu teknikler; bireylerin düşüncelerini ve tutumlarını etkilemek için yanıltıcı dil, yanlış yönlendirme ve propaganda stratejileri içerir. Medyada sıkça karşılaşılan manipülasyon tekniklerinden biri, görsellerin veya metinlerin çarpıtılmasıdır. Ayrıca dezenformasyon ve sahte haberler, toplumu yanıltarak yanlış bilgi yayılmasına neden olabilir (Avrupa Konseyi, 2022). Başlıklar ve görsellerin tıklama tuzağı yaratacak şekilde kullanılması, dikkat çekme stratejilerinin başında gelir. Bu tür manipülasyonları tanıyabilmek ve eleştirel bir bakış açısıyla medya içeriklerini değerlendirebilmek, dijital okuryazarlığın önemli bir parçasıdır. Aşağıda bu konuyla ilgili önemli kavramlar verilmiştir.

- **Manipülasyon Teknikleri:** Medyada kullanılan yanıltıcı dil, yanlış yönlendirme, propaganda teknikleri ve manipülatif görseller.
- **Sahte Haberler:** Sahte haberlerin tanınması, yanlış bilgi yayma teknikleri ve dezenformasyon.
- **Tıklama Tuzağı ve Sansasyonel İçerikler:** Başlıklar ve görselleri yanıltıcı şekilde kullanarak dikkat çekme stratejileri.



Etkinlik

- Katılımcılar, çeşitli medya içeriklerinden örnekler alarak bu içeriklerdeki manipülasyon unsurlarını tespit ederler.
- Sahte haber örnekleri üzerinde çalışma yaparak bu haberlerin doğru bilgi olup olmadığını araştırırlar.

4.3 Dijital Medya ve Sosyal Medya Okuryazarlığı

Dijital medya ve sosyal medya, günümüz toplumunda bilgi alışverişinin en çok yapıldığı alanlardan biri hâline gelmiştir. Ancak bu platformların işleyişi ve içerik dinamikleri, kullanıcıların doğru bilgiye ulaşmasını zorlaştırabilir. Sosyal medya algoritmaları, kullanıcıların ilgi alanlarına göre içerik önerirken aynı zamanda bilgi kirliliği ve yanıltıcı içeriklerin yayılmasına da zemin hazırlayabilir. Bu nedenle dijital medya okuryazarlığı, kullanıcıların sosyal medya içeriklerini eleştirel bir bakış açısıyla değerlendirmelerini ve yanlış bilgileri ayırt etmelerini sağlar. Dijital medya etiği ise doğru ve güvenilir bilgi yayma sorumluluğu, içerik üretirken ve paylaşırken dikkat edilmesi gereken etik ilkeleri kapsar. Sosyal medyanın sorumlu bir şekilde kullanılması, bireylerin dijital ortamda daha bilinçli ve etik bir şekilde var olmalarını destekler. Aşağıda bu konuyla ilgili önemli kavramlar verilmiştir.

- **Sosyal Medya Dinamikleri:** Sosyal medya platformlarının işleyişi, algoritmalar ve içerik önerme sistemleri.
- **Dijital Medyada Bilgi Kirliliği:** Sosyal medyada yayılan yanlış bilgi, propaganda ve yanlış içeriklerin tespiti.
- **Dijital Medya Etiği:** Sosyal medyada doğru bilgi yayma, dijital içerik üretimi ve paylaşımı sırasında dikkat edilmesi gereken etik kurallar.



Etkinlik

- Katılımcılar, sosyal medyada karşılaştıkları güncel içerikleri analiz eder ve içeriklerin doğruluğunu çapraz kaynak kontrolü ile değerlendirirler.
- Dijital medya araçları kullanılarak üretilen içeriklerin toplum üzerindeki etkileri tartışılır.

4.4. Medya İçeriklerinin Toplumsal Etkileri

Medya; toplumsal hayatın önemli bir parçası olarak bireylerin algılarını, değerlerini ve davranışlarını şekillendirme gücüne sahiptir. Gazetelerden televizyon programlarına, sosyal medyadan dijital platformlara kadar uzanan geniş bir yelpazede medya; hem bilgi kaynağı hem de bir iletişim aracı olarak toplum üzerinde derin etkiler bırakır. Medya içerikleri, bireylerin dünyayı nasıl gördüklerini ve toplumsal olaylara nasıl tepki verdiklerini etkilerken kültürel kimliklerin temsilinde ve sosyal hareketlerin yayılmasında kritik bir rol oynar (Buckingham, 2015). Bu nedenle; medya okuryazarlığı ve içeriklerin eleştirel analizi, bireylerin bilinçli ve etkili medya tüketicileri olmalarını sağlar. Aşağıda bu konuyla ilgili önemli kavramlar verilmiştir.

- **Medyanın Toplum Üzerindeki Etkisi:** Medya içeriklerinin toplumsal algılar, değerler ve davranışlar üzerindeki etkileri.
- **Medya ve Kültürel Temsil:** Medyada yer alan stereotipler, kültürel kimliklerin temsili ve ön yargılar.
- **Medya ve Sosyal Hareketler:** Medyanın toplumsal hareketlerde ve kitle iletişiminde oynadığı rol.



Etkinlik

- Katılımcılar, medyada yer alan çeşitli kültürel temsilleri inceleyerek bu içeriklerin toplumsal algılar üzerindeki etkilerini tartışır.
- Sosyal medyada yaygınlaşan sosyal hareketler ve bu hareketlerin medya tarafından nasıl ele alındığı üzerine grup çalışmaları yapılır.

KAYNAKÇA

Avrupa Konseyi (2022). Dijital Vatandaşlık Eğitimi El Kitabı. Avrupa Konseyi Yayınları

Bayrakcı, S., ve Narmanlıoğlu, H. (2021). Digital Literacy as Whole of Digital Competences: Scale Development Study. Düşünce ve Toplum Sosyal Bilimler Dergisi, 3(4), 1-30. Retrieved from <https://dergipark.org.tr/en/pub/dusuncevetoplum/issue/63163/945319>

Buckingham, D. (2015). Defining digital literacy-What do young people need to know about digital media?. Nordic journal of digital literacy, 10 (Jubileumsnummer), 21-35.

JISC (2014). Developing Students' Digital Literacy. Digital Capabilities Framework. Erişim adresi: <https://www.jisc.ac.uk/guides/developing-students-digital-literacy>. Erişim Tarihi: 01.11.2024

Özden, M., Meydan, E., & Günay, G. (2024). Dijital Okuryazarlık Becerisi Ölçeği: Güvenirlik ve Geçerlik Çalışması. Eğitimde Kuram Ve Uygulama, 20(1), 38-48. <https://doi.org/10.17244/eku.1359401>

Üstündağ, M. T., Güneş, E., & Bahçivan, E. (2017). Dijital Okuryazarlık Ölçeğinin Türkçeye Uyarlanması ve Fen Bilgisi Öğretmen Adaylarının Dijital Okuryazarlık Durumları. Journal of Education and Future(12), 19-29.

MODÜL 2

Dijital Sağlık



Modül Kapsamı

Bu modül; dijital teknolojilerin bireyler üzerindeki fiziksel, zihinsel, sosyal ve bilişsel olumsuz etkilerine odaklanmaktadır. Eğitim boyunca; uzun süreli ekran kullanımı nedeniyle oluşan fiziksel rahatsızlıklar, ergonomik çalışma düzeni oluşturma ve göz yorgunluğunu önleme gibi konular ele alınacaktır. Ayrıca; sosyal medya ve dijital bağımlılığın zihinsel sağlık üzerindeki etkileri, dikkat dağınıklığı ve bilgi kirliliği gibi bilişsel sorunlar incelenecek; sosyal medya kaynaklı anksiyete, depresyon ve siber zorbalık gibi sosyal sorunlar tartışılacaktır. Eğitim; bu olumsuzlukları en aza indirmek için sağlıklı dijital alışkanlıklar geliştirme, dijital detoks uygulamaları ve teknoloji kullanımını dengeleme stratejilerini içermektedir.

Öğrenme Kazanımları

- Dijital teknolojilerin fiziksel, zihinsel ve sosyal etkilerini öğrenmek.
- Katılımcılara ve bireylere dijital sağlığın korunması konusunda öneriler sunmak.
- Dijital detoks ve sağlıklı dijital alışkanlıklar hakkında farkındalık kazanmak.

İçerik Ağacı

1. Dijital Teknolojilerin Neden Olduğu Fiziksel Olumsuz Etkiler
2. Dijital Teknolojilerin Zihinsel Sağlık Üzerindeki Olumsuz Etkileri
3. Dijital Teknolojilerin Bilişsel ve Sosyal Etkileri
4. Dijital Sağlık ve Teknoloji Kullanımı Konusunda Çözümler ve Öneriler

Bölüm 1: Dijital Teknolojilerin Neden Olduğu Fiziksel Olumsuz Etkiler

1.1. Ekran Süresi ve Fiziksel Sağlık

Günlük hayatımızın büyük bir kısmını ekran başında geçirdiğimizde, gözlerimiz sürekli bir odaklanma ve yorgunluk problemi yaşar. Bilgisayar ve mobil cihazlara uzun süre bakmak, gözlerin düzenli olarak yeniden odaklanmasını zorlaştırır ve göz kaslarının aşırı çalışmasına yol açar (BOSTANCI, 2016). Bu durum zamanla “Bilgisayar Görme Sendromu” olarak bilinen dijital göz yorgunluğuna yol açar.

Modüllerde birden fazla etkinlik seçeneği sunulmuştur, uygun bulunan etkinlik kullanılabilir.



Etkinlik

Göz Egzersizi Bingo Oyunu

Amaç:

Katılımcıların göz sağlığını korumalarına yardımcı olmayı ve göz egzersizlerini eğlenceli bir şekilde öğretmeyi amaçlar.

Gerekli Malzemeler:

- Bingo kartları (her katılımcı için bir adet)
- Kalem veya işaretleme araçları
- Egzersizlerin yazılı olduğu bir liste
- Ödül (küçük bir ödül, çıkartma vb.)

1. Bingo Kartı Tasarımı:

5x5'lik kare şeklinde bingo kartları hazırlayın.

Her bir kareye farklı göz egzersizleri yerleştirin.

Göz Egzersiz Listesi:

- 1 -10 saniye gözlerini kapat.
- 2 -Uzak bir nesneyi 10 saniye boyunca gözle takip et.
- 3 -Gözlerinle daire çevir.
- 4 -Yakın bir nesneyi 5 saniye incele.
- 5 -Göz masajı yap.

6 -Odak deęiřtir (yakın ve uzak nesne).

7 -Her iki gözle farklı yönlerde bak.

8 -Göz kırp (30 saniye boyunca hızlıca).

9 -Göz hareketi yap (sağdan sola, yukarıdan aşağı).

10 -5 saniye boyunca gözlerini dinlendir.

Bingo kartları dağıtılır, her katılımcıya bir bingo kartı ve kalem verilir.

1. Oyun Başlatma:

Katılımcılara göz egzersizlerinin nasıl yapıldığı gösterilir. Her bir katılımcı, listedeki egzersizlerden birini seçerek yapmalıdır.

2. Egzersizlerin Uygulanması:

Eğitmen, sırayla göz egzersizlerini okur. Katılımcılar, okunan egzersizi tamamladıktan sonra bingo kartındaki o egzersizin kutusunu işaretler.

3. Bingo İlanı:

Katılımcılar; yatay, dikey veya çapraz olarak beş egzersizi işaretlediklerinde “Bingo!” diye bağırabilirler.

Bingo yapan katılımcının egzersizleri doğru bir şekilde tamamlayıp tamamlamadığı kontrol edilir ve katılımcı ödüllendirilir.

Oyun bittikten sonra, katılımcılarla göz sağlığı hakkında konuşulur. Hangi egzersizleri en çok sevdikleri ve hangilerinin en çok işe yaradığı tartışılır.



Etkinlik

Harf Avı Oyunu:

Harf avı, katılımcıların göz sağlığını geliştirmeye yardımcı olabilecek eğlenceli ve etkileşimli bir oyundur.

Oyunun Amacı:

-Katılımcıların dikkatini artırmayı ve göz kaslarını çalıştırmayı amaçlamaktadır.

Gerekli Malzemeler:

-Farklı boyutlarda ve renklerde harf kartları veya nesneler (örneğin; karton harfler, yazılı etiketler)

-Kâğıt ve kalem (her katılımcı için)

-Zamanlayıcı

Hazırlık Aşaması:

1-Harfler hazırlanır (A, B, C, D gibi harfleri yazın ve bunları karton veya kalın kâğıttan kesin. Farklı renkler ve boyutlar kullanarak harfleri çeşitlendirebilirsiniz.).

2-Harflerin yanı sıra, harfleri temsil eden nesneler (örneğin; A için elma, B için balon resmi) de kullanılabilir.

3-Sınıfın içinde veya dışarıda bir alan seçilir. Harfler bu alana yerleştirilir. Harfleri dağıtarak onları bulmak için çeşitli yerler seçilir (masaların üzerinde, duvarlarda, bahçede).

Oyun Kuralları:

-Katılımcılara harf avının nasıl oynanacağı açıklanır. Her katılımcının belirli bir süre içinde en fazla harfi bulması gerektiği belirtilir. Katılımcılara belirli bir süre (örneğin, 5-10 dakika) verilir. Bu süre içinde harfleri bulup toplamaları istenir. Katılımcılar, eğitmenin belirlediği alanda harfleri aramaya başlar. Buldukları harfleri veya nesneleri kâğıtlarına yazarak veya yanlarına alarak sayabilirler. En fazla harfi bulan öğrenci kazanır.

Ekip Çalışması:

-Katılımcıları gruplara ayırarak takım hâlinde oynamalarını sağlayabilirsiniz. Bu, iş birliği ve iletişim becerilerini geliştirir.

1.2. Ergonomi ve Vücut Duruşu Bozuklukları

Bilgisayar ve mobil cihaz kullanımının boyun, sırt ve omuz ağrılarına etkisi:

Uzun süre bilgisayar veya mobil cihaz kullanımı; özellikle yanlış duruş ve ergonomik olmayan çalışma koşulları nedeniyle boyun, sırt ve omuz ağrılarına yol açabilir. Boynun sürekli öne eğilmesi ve omuzların yuvarlaklaşması, kaslarda gerginliğe ve duruş bozukluklarına neden olur. Zamanla bu durum kronik ağrılara ve postür bozukluklarına yol açabilir.

Ergonomik cihaz kullanımı ve doğru oturma pozisyonları:

Ergonomik bir çalışma ortamı oluşturmak, vücut duruşunu korumanın en önemli adımlarından biridir. Sandalyeniz sırtınıza tam destek sağlamalı, ayaklarınız yere tam basmalı ve dizleriniz 90 derecelik açıda olmalıdır. Ekranın göz hizasında yer alması ve klavye-fare kullanımının rahat olması da önemlidir. Ergonomik fare, klavye ve ayarlanabilir masalar kullanarak bu ağrıların önüne geçilebilir (Vural vd., 2010).

1.3. Fiziksel Hareketsizlik

Uzun süreli hareketsizliğin (oturma, ekran karşısında geçen süre) obezite, kalp rahatsızlıkları ve diyabet üzerindeki etkisi:

Dijital cihazlar karşısında geçirilen uzun süreler, fiziksel aktiviteyi büyük ölçüde azaltarak hareketsiz bir yaşam tarzına yol açar. Sürekli oturma, vücudun metabolik işlevlerini olumsuz etkileyebilir; bu da obezite, kalp hastalıkları ve tip 2 diyabet gibi sağlık sorunlarına neden olabilir. Ayrıca, kas ve eklem zayıflıkları da bu durumun yaygın sonuçları arasındadır.



Etkinlik

“Her 20 Dakikada Bir” Oyunu

Amaç: Katılımcıların bilgisayar başında geçirdiği süre zarfında düzenli olarak hareket etmelerini sağlamayı ve hareketsizliğin olumsuz etkilerini azaltmayı amaçlar.

Nasıl Oynanır?

Zamanlayıcı Kurma: Bilgisayardan, cep telefonundan bir zamanlayıcı ayarlanır (20 dakikada bir).

Hareket Talimatları: Her 20 dakikada bir, belirli bir hareket yapmanız gerektiğini belirten bir liste oluşturulur.

-1 dakikalık ayakta durma

-1 dakikalık yavaş yürüyüş

-Kol ve bacak esnetme hareketleri gibi hareketler çeşitlendirilebilir.

Zamanlayıcı çaldığında, belirttiğiniz hareket yapılır. Bu, tüm katılımcılar için eğlenceli bir mola olacaktır. Bireysel veya grup içinde oynanabilir. Grup ile oynandığında tüm katılımcılar aynı anda hareketi yapabilir. Böylece birlikte hareket etmenin getirdiği motivasyon artmış olur. Katılımcılar zamanla farklı hareketler ekleyebilir veya daha fazla zorluk isteyebilir. Böylece oyun daha dinamik ve eğlenceli hâle gelir. Katılımcılar, günlük hedefler belirleyebilir (örneğin, toplamda 100 tek ayak üzerinde zıplama yapmak gibi).

Oyun sonunda katılımcılar, gün boyunca nasıl hissettiklerini ve hangi hareketlerin kendilerine en iyi geldiğini tartışabilir. Bu, deneyimlerini paylaşmalarına olanak tanır ve hareketsizlik ile ilgili farkındalıklarını artırır.

Fiziksel aktiviteyi artırmak için dijital çözümler (ör. adım sayar uygulamaları):

Dijital çözümler, hareketsizliği azaltmak ve fiziksel aktiviteyi artırmak için kullanılabilir. Adım sayar uygulamaları, kişilerin günlük hareket hedeflerini takip etmelerine yardımcı olurken düzenli egzersiz hatırlatıcıları ve sağlık uygulamaları da aktif bir yaşam tarzı benimsemeyi teşvik eder.

Bölüm 2: Dijital Teknolojilerin Zihinsel Sağlık Üzerindeki Olumsuz Etkileri

2.1. Anksiyete, Depresyon ve Dijital Bağımlılık

Sosyal Medya Kullanımı ve Zihin Sağlığı

Sosyal medya platformları, insanların hayatlarının sadece en iyi yönlerini sergilediği bir ortam yaratabilir. Bu durum, kullanıcıların kendi hayatlarını sürekli başkalarıyla kıyaslamasına neden olur. Başkalarının başarıları, tatilleri, fiziksel görünüşleri veya sosyal yaşamları ile yapılan bu kıyaslamalar; kişilerin kendilerini yetersiz hissetmelerine ve mükemmeliyetçilik baskısı altında kalmalarına yol açabilir. Zamanla bu durum, öz güven düşüklüğüne ve olumsuz bir benlik algısına sebep olabilir.

Sosyal medyanın anksiyete, depresyon ve yalnızlık üzerindeki etkileri:

Sosyal medya, sürekli olarak “daha iyi” bir yaşam arayışı içinde olma hissini pekiştirebilir. Sürekli çevrim içi olma ve sosyal medyada aktif olma zorunluluğu, bireylerde stres ve anksiyete seviyelerini artırabilir. Ayrıca sosyal medyada geçirilen uzun süreler gerçek hayattaki sosyal etkileşimlerin yerini aldığı anda, kişiler kendilerini daha yalnız hissedebilirler. Bu da zamanla depresyon belirtilerinin ortaya çıkmasına neden olabilir.



Gelişmeleri Kaçırma Korkusu: Sürekli çevrim içi olma baskısı:

Sosyal medya, kullanıcıların “bir şeyleri kaçırma” korkusu (FOMO) yaşamalarına neden olabilir. Sürekli olarak yeni içeriklerin, etkinliklerin ve haberlerin paylaşılması bireylerde her an bir şeyleri kaçırma endişesi yaratır. Bu durum; sürekli çevrim içi olma baskısı yaratır ve kişinin ekran başında daha fazla zaman geçirmesine neden olabilir, bu da psikolojik olarak kaygı seviyelerini yükseltir.

2.2. Dijital Bağımlılık

Oyun, sosyal medya ve mobil uygulamaların aşırı kullanımının bağımlılık yapıcı etkileri:

Sosyal medya platformları, mobil oyunlar ve çeşitli uygulamalar, kullanıcıları platformda tutmaya yönelik tasarlanmıştır. Bildirimler, ödül sistemleri ve sosyal onay mekanizmaları, kullanıcıların bu uygulamalara daha fazla bağlanmasına yol açar. Zamanla bu kullanım bağımlılık yapıcı hâle gelebilir ve bireyler günlük aktivitelerini, iş veya okul hayatlarını aksatarak dijital dünyaya daha fazla vakit ayırmaya başlayabilirler. Bu durum; zaman yönetimi sorunlarına, fiziksel ve zihinsel sağlık problemlerine yol açabilir (Muslu ve Bolışık, 2009).

Bağımlılıkla başa çıkma yöntemleri ve dijital detoks:

Dijital bağımlılıkla başa çıkmak için bilinçli adımlar atmak önemlidir. İlk olarak, sosyal medya ve dijital uygulamaların kullanımını sınırlamak ve ekran süresi hedefleri belirlemek faydalı olabilir. Bildirimleri kapatmak, kullanım sürelerini izlemek ve sosyal medyayı amaçlı kullanmak bağımlılık riskini azaltabilir. Dijital detoks ise belirli dönemlerde sosyal medyadan ve dijital cihazlardan uzaklaşarak zihni dinlendirme yöntemidir. Haftalık veya günlük belirli sürelerle dijital detoks yaparak bireyler, teknolojiye olan bağımlılıklarını azaltabilir ve zihinsel sağlıklarını dengeleyebilirler.

2.3. Uyku Bozuklukları ve Mavi Işık Etkisi

Mavi Işık ve Uyku Kalitesi

Dijital cihaz ekranları (bilgisayar, telefon, tablet vb.) tarafından yayılan mavi ışık, gözlerimizdeki fotoreseptörler aracılığıyla beynimize iletilir ve melatonin hormonunun salgılanmasını baskılar. Melatonin, uyku döngüsünü düzenleyen bir hormondur ve gece boyunca vücudun uykuya hazırlanmasını sağlar. Mavi ışık, vücuda hâlâ gündüz olduğu sinyalini vererek uykuya dalmayı zorlaştırabilir. Bu nedenle; özellikle yatmadan önce ekran başında çok vakit geçirmek, uyku kalitesini düşürebilir ve sirkadiyen ritmini bozarak uykusuzluğa neden olabilir.

Ekran süresi ile uyku arasındaki ilişki ve dijital cihaz kullanımının sınırlandırılması önerileri:

Araştırmalar, uzun süre ekran başında kalan kişilerin uyku kalitesinin düştüğünü ve uykusuzluk riskinin arttığını göstermektedir. Uykuya dalmadan en az bir saat önce dijital cihaz kullanımını sonlandırmak, mavi ışığın olumsuz etkilerini en aza indirmeye yardımcı olabilir. Ayrıca, cihazlarda gece modu veya mavi ışık filtresi ayarlarını kullanarak mavi ışık maruziyetini azaltmak mümkündür. Böylece, gözler ve beyin uykuya daha iyi hazırlanır.



Dijital Detoks ve Uygulama Önerileri

1) Düzenli ekran molaları verme:

Ekran başında uzun süre vakit geçirdiğinizde, gözler ve zihin yorgun düşebilir. Bu nedenle, düzenli olarak ekran molaları vermek önemlidir. “20-20-20” kuralı bu noktada yardımcı olabilir: Her 20 dakikada bir, 20 saniye boyunca en az 20 metre uzağa bakarak gözlerinizi dinlendirin. Aynı zamanda, her birkaç saatte bir ayağa kalkıp esneme hareketleri yaparak vücut üzerindeki hareketsizlik etkilerini azaltabilirsiniz. Bu molalar, zihinsel tazelenme sağlayarak odaklanmayı artırır.

2) Sağlıklı uyku alışkanlıkları geliştirme:

Dijital detoksun en önemli faydalarından biri, sağlıklı uyku alışkanlıklarının gelişmesine yardımcı olmasıdır. Yatmadan önce dijital cihazlardan uzak durmak, zihni rahatlatmak ve melatonin seviyelerinin düşmesini engellemek için etkili bir yöntemdir. Bu süre zarfında kitap okumak, meditasyon yapmak veya düşük ışıktaki sakinleştirici aktivitelerle uykuya hazırlanmak önerilir. Ayrıca; uyku rutini oluşturarak her gün aynı saatte yatıp kalkmak, sirkadyen ritmini düzenler ve daha kaliteli bir uyku sağlar.



Etkinlik

Dijital Dedektif Etkinliği

Katılımcıların teknoloji bağımlılığı ve dijital detoks konusunu sorgulamalarını ve araştırmalarını sağlamayı amaçlayan bir oyundur.

Amaç: Katılımcıların teknoloji ile olan ilişkilerini sorgulamalarını sağlamayı, dijital bağımlılığın etkilerini ve çözüm yollarını bulmalarını teşvik etmeyi amaçlar.

Hedef Kitle: Her yaş grubundan katılımcılar

Gerekli Malzemeler: Kâğıt, Kalem, Zamanlayıcı, Poster veya Beyaz Tahta

Görev Kartları: Farklı görevleri içeren kartlar (örneğin, “Günlük ekran sürenizi %30 azaltmanın yollarını bulun”).

Etkinlik hakkında kısa bir tanıtım yapılır. Katılımcılara, dijital dedektif rolü üstlenecekleri ve görevlerini yerine getirerek dijital bağımlılıkla ilgili çözümler bulacakları açıklanır. Dijital bağımlılık ve detoks konusunun önemine değinilir.

Katılımcılar 4-5 kişilik gruplara ayrılır. Grupların birbirleriyle etkileşimde bulunabilmesi için farklı yaş gruplarından karışık gruplar oluşturmaya çalışılır.

Görev Kartlarının Dağıtılması: Her gruba bir veya daha fazla görev kartı verilir. Görev kartları, dijital bağımlılıkla ilgili çeşitli konuları içermelidir:

- “Dijital detoksun faydaları nelerdir? Araştırın.”
- “Sosyal medyanın etkileri üzerine bir sunum hazırlayın.”
- “Ekran sürenizi nasıl azaltabileceğinizi düşünün ve öneriler oluşturun.”
- “Teknoloji kullanımınızı azaltmak için yeni hobiler keşfedin.”

Gruplara belirli bir süre verilir. Bu süre zarfında, gruplar görevlerini yerine getirmek için araştırma yapar. Katılımcılar; internetten, kitaplardan veya kendi deneyimlerinden yararlanabilir.

Her grup, bulgularını ve önerilerini diğer gruplarla paylaşmak için sırayla sunum yapar. Sunumlar 5-7 dakika sürmeli ve ardından diğer gruplardan sorular alınmalıdır. Sunum sırasında, gruplar yaratıcı yöntemler kullanabilir (örneğin; poster, sunum yapma veya canlandırma). Sunumlardan sonra, katılımcılar arasında tartışma yaparak her grubun önerileri değerlendirilir. Hangi önerilerin en etkili olduğu ve nedenleri konuşulur. Katılımcılardan, kendi deneyimlerini ve dijital detoks hakkında düşündüklerini paylaşmaları istenebilir.

Bölüm 3: Dijital Teknolojilerin Bilişsel ve Sosyal Etkileri

3.1. Dikkat Dağınıklığı ve Odaklanma Problemleri

Multitasking (Çoklu Görev Yürütme) ve Bilişsel Yük

Multitasking, aynı anda birden fazla dijital görevi yerine getirme eğilimini ifade eder ve modern dijital dünyada oldukça yaygın bir alışkanlıktır. Ancak, araştırmalar gösteriyor ki insan beyni bu tür çoklu görevleri verimli bir şekilde işleyememektedir. Multitasking, dikkat süresini azaltarak bilişsel yükü artırır ve kişinin her göreve tam olarak odaklanmasını engeller. Bu durum, yapılan işin kalitesini düşürebilir ve hata yapma olasılığını artırabilir. Aynı zamanda, sürekli görev değişimleri zihinsel yorgunluğa yol açarak üretkenliği önemli ölçüde azaltır.

Dikkat yönetimi ve derin odaklanma becerilerinin geliştirilmesi:

Dikkati yönetmek ve derin odaklanma becerilerini geliştirmek, aynı anda birden çok iş yapmanın olumsuz etkilerini dengelemek için oldukça önemlidir. Bu becerileri geliştirmek için yapılabilecek en etkili adımlardan biri, görevler arasında geçiş yapmaktan kaçınarak tek bir işe odaklanmak ve bu işi tamamlamak için belirli zaman dilimleri ayırmaktır. Pomodoro Tekniği gibi zaman yönetimi yöntemleri, odaklanma sürelerini artırarak dikkati yönetmede yardımcı olabilir. Ayrıca; çevresel dikkat dağınıcılarını azaltmak ve görev sırasında cihaz bildirimlerini kapatmak, derin odaklanmayı güçlendiren adımlardır.



Etkinlik

“Sessiz Zihin Oyunu”

Amaç: Dijital bağımlılığın odaklanma üzerindeki etkilerini katılımcılara hissettirmeyi ve teknolojiden uzaklaşarak odaklanmalarını sağlayacak bir ortam oluşturmayı amaçlar.

Gerekli Malzemeler:

- Küçük zorluk kartları (odaklanma gerektiren görevlerle)
- Zamanlayıcı (isteğe bağlı)
- Sessiz bir ortam

1. Giriş ve Hazırlık:

Katılımcılardan telefonlarını veya diğer dijital cihazlarını tamamen kapatmaları istenir ve cihazlar bir kutuya konur. Oyunun amacı, dijital dünyadan tamamen koparak odaklanmalarını test etmektir.

2. Zorluk Kartları Dağıtma

Her katılımcıya birer “zorluk kartı” verilir. Kartlarda odaklanma gerektiren basit ama dikkat dağıtıcı görevler yer almalı. Örneğin:

“Sessizce oturun ve gözlerinizi kapatın. Sadece nefesinize odaklanın ve başka hiçbir şey düşünmeyin (5 dakika).”

“Önünüzdeki nesneye (örneğin, bir kalem veya masa) odaklanın. Nesnenin tüm ayrıntılarını gözlemleyin ve 3 dakika boyunca dikkatinizi dağıtmayın.”

“Bir kâğıda 10 kelimelik kısa bir hikâye yazın, yalnızca hikâyenize odaklanın”

Her kartın süresi 3-5 dakika olacak şekilde ayarlanır.

3. Görevleri Tamamlama

Zorluk kartındaki görevleri tamamlamaları için her katılımcıya belirli bir süre verilir. (örneğin, her görev için 3-5 dakika). Katılımcılardan bu süre boyunca tamamen sessiz olmaları ve sadece karttaki göreve odaklanmaları istenir. Zamanlayıcı ayarlanır ve sürenin sonunda herkes görevini bitirmiş olacaktır. Tüm görevler tamamlandıktan sonra, katılımcılarla birlikte bir değerlendirme oturumu yapılır.

Sorulabilecek sorular:

“Görev boyunca dikkatinizi dağıtan bir şey oldu mu? Hangi aşamalarda dikkatiniz dağıldı?”

“Bu odaklanma alıştırmaları size nasıl hissettirdi?”

“Dijital cihazlar olmadan odaklanmak size daha kolay geldi mi?”

Bu etkinlik, katılımcıların dikkatlerini toplamalarını sağlarken aynı zamanda dijital cihazlardan uzaklaşmanın odaklanma üzerindeki olumlu etkilerini hissetmelerine yardımcı olacaktır.

Bilgi Kirliliği

Fazla bilgiye maruz kalmanın analiz yeteneğini zayıflatması:

Dijital çağda her gün birçok bilgiye maruz kalıyoruz. Ancak, bu bilginin büyük bir kısmı doğrulanmamış veya yanlış olabilir. Bilgi kirliliği, fazla bilgiye maruz kalmanın bir sonucudur ve bireylerin bilgiyi doğru bir şekilde analiz etme yeteneklerini zayıflatır. Sürekli bilgi akışı; bireylerin gerçek ve sahte bilgiyi ayırt etmesini zorlaştırır, bu da yanlış bilgilendirilme riskini artırır. Fazla bilgi yükü, zihinsel karmaşıklığa ve karar verme süreçlerinde yanılgılara neden olabilir.

3.2. Sosyal İlişkiler Üzerindeki Etkiler

Yüz Yüze İletişim Becerilerinin Zayıflaması

Sosyal medya ve mesajlaşma uygulamaları, iletişim kurmanın hızlı ve kolay yollarını sunmasına rağmen yüz yüze iletişim becerilerinin zayıflamasına yol açabilir. Dijital platformlar üzerinden yapılan kısa ve yüzeysel etkileşimler; insanların yüz yüze iletişimde geliştirdikleri tonlama, beden dili ve duygusal ifade gibi önemli sosyal becerilerin körelmesine neden olabilir. Dijital ortamdaki sohbetler, duygusal incelikleri ve karmaşık sosyal ipuçlarını taşımadığından kişiler arası ilişkilerde derin bağlar kurmak zorlaşabilir. Bu da bireylerin yüz yüze görüşmelerde kendilerini ifade etmekte zorlanmalarına ve sosyal ilişkilerde eksiklik hissetmelerine neden olabilir (Çelik ve Çelik, 2023).

Empati kurmanın ve sosyal becerilerin zayıflaması:

Sürekli çevrim içi olma ve dijital platformlar üzerinden iletişim kurma alışkanlığı, insanların başkalarıyla empati kurma yeteneğini zayıflatır. Sosyal medya ve mesajlaşma uygulamaları; kişiler arası iletişimde duygusal geri bildirim alma ve verme süreçlerini kısaltabilir, bu da empati becerisini olumsuz etkileyebilir. İnsanlar, yüz yüze iletişimdeki jest ve mimik gibi önemli sosyal ipuçlarını alamadıkları için karşılarındaki kişinin duygusal durumunu doğru bir şekilde anlamakta zorlanabilirler. Bu durum, zamanla sosyal becerilerin zayıflamasına ve kişiler arası ilişkilerde kopukluklara yol açabilir.

Siber Zorbalık

Çocuklar ve gençler arasında artan siber zorbalık vakaları ve etkileri:

Siber zorbalık; dijital platformlar aracılığıyla yapılan tehditler, hakaretler, dışlama veya aşağılayıcı mesajlar yazma gibi davranışları içerir. Sosyal medya, mesajlaşma uygulamaları ve çevrim içi oyunlar, özellikle çocuklar ve gençler arasında siber zorbalığın yayılmasına zemin hazırlamaktadır. Siber zorbalık, mağdurlar üzerinde ciddi duygusal ve psikolojik etkilere yol açabilir.

Zorbalığa maruz kalan bireyler; depresyon, kaygı, düşük öz güven, yalnızlık ve okul başarısızlığı gibi sorunlar yaşayabilir. Ayrıca, sürekli çevrim içi olma durumu zorbalıkla karşı karşıya kalma riskini artırır.



Siber zorbalıkla mücadele stratejileri:

Siber zorbalıkla başa çıkmak için öncelikle farkındalık ve eğitim önemlidir. Çocuklara ve gençlere siber zorbalık hakkında bilgi verilerek bu tür davranışların zararları anlatılmalıdır. Siber zorbalıkla mücadele stratejileri arasında:

- **Siber Zorbalık Durumunda Harekete Geçme:** Zorbalığa uğrayan bireylerin durumu saklamadan bir yetişkine, öğretmene veya güvenilir birine anlatmaları teşvik edilmelidir.
- **Zorbalık Yapan Kişiyi Engelleme ve Durumu Raporlama:** Sosyal medya platformlarında zorbalık yapan kişiyi engellemek ve durumu platforma bildirmek önemlidir. Çoğu platform, zorbalık içeren içerikleri kaldırma ve kullanıcıyı yasaklama gibi önlemler sunar.
- **Empati ve Sosyal Sorumluluk Eğitimleri:** Okullarda ve topluluklarda empati becerisi ve sosyal sorumluluk bilinci geliştirilerek çocukların ve gençlerin çevrim içi ortamda nasıl daha duyarlı bireyler olabilecekleri öğretilmelidir.



Etkinlik

Oyun: “Zorbalık Labirenti”

Amaç: Katılımcıların siber zorbalığın yol açtığı duygusal etkileri anlamalarını sağlamayı, zorbalık karşısında sergilenmesi gereken doğru ve destekleyici davranışları öğretmeyi amaçlar. Bu oyunda, katılımcılar zorbalık senaryolarıyla karşılaşırken empati kurmayı ve zorbalık mağdurlarına nasıl yardım edebileceklerini öğrenirler.

Gerekli Malzemeler:

Labirent Alanı: Bir büyük karton veya zemine bantlarla çizilmiş labirent (sınıf ortamına göre labirent şekli büyük veya küçük olabilir).

Görev Kartları: Her birinde siber zorbalık senaryoları olan kartlar.

Destek Kartları: Moral veren, güven sağlayan mesajlarla dolu kartlar.

Yol Belirleyiciler: Labirent boyunca hareket ettikçe her görev kartının tamamlandığını gösterecek işaretler (renkli kartlar veya küçük nesneler).

Katılımcıların geçeceği yollar ve görev durakları ile birlikte bir labirent çizilir. Bu labirent, sınıfta yer sorunu varsa büyük bir kâğıt veya karton üzerinde de yapılabilir.

Her bir durak noktasına bir görev kartı ve bir destek kartı yerleştirilir. Görev kartlarında zorbalık senaryoları bulunur, destek kartlarında ise olumlu ve cesaretlendirici mesajlar yazılır.

Örnek Destek Kartları:

“Bu zor bir durum ama yanındayız.”

“Yalnız değilsin, bu zorbalığın seni etkilemesine izin verme.”

“Kendine inan, zorbalığı doğru davranışlarla aşabilirsin.”

Katılımcılara oyunun amacı açıklanır. Her katılımcı sırayla labirente girer ve durak noktalarındaki görev kartlarını tamamlar. Her durakta, katılımcıya bir siber zorbalık senaryosu ve bir soru içeren kart verilir. Katılımcı, senaryoyu okuyup nasıl bir davranış sergilemesi gerektiğini düşünmelidir.

Örnek Görev Senaryoları:

“Birisi sana internette alaycı yorumlar yapıyor ve kötü lakaplar takıyor. Ne yapardın?”

“Sosyal medyada bir arkadaşın hakkında kötü bir dedikodu dolaşıyor. Arkadaşın senin desteğine ihtiyaç duyuyor. Ona nasıl yardım edersin?”

“Bir grup, çevrim içi bir oyun oynarken seni dışlayarak eğleniyor. Bu durumda nasıl davranırsın?”

Katılımcı, her senaryoya bir yanıt verdikten sonra bir destek kartı alır ve moral veren bir mesaj okur. Destek kartları, onlara bu tür zorbalıklara karşı güçlü durmaları gerektiğini hatırlatır. Katılımcılar her doğru veya destekleyici cevap verdiklerinde bir sonraki durak noktasına ilerler. Her doğru tepki veya çözüm önerisi sonrası ödül veya simge kartı alabilirler. Yanlış ya da zorbalığa cesaret veren bir yanıt verildiğinde, kısa bir açıklama yaparak neden bu davranışın yanlış olduğunu paylaşılır. Örneğin, “Bu tür bir yanıt karşı tarafı cesaretlendirebilir, destek almak veya görmezden gelmek daha iyi bir yol olabilir.”

Katılımcılar labirentin sonuna ulaştıklarında bir değerlendirme yapılır.

Tartışma Soruları:

“Siber zorbalık senaryoları ile karşılaşmak sana nasıl hissettirdi?”

“Bir arkadaşın zorbalığa uğradığında nasıl davranabileceğini fark ettin mi?”

“Bu oyundan çıkarabileceğin en önemli ders neydi?”

“Gerçek hayatta zorbalıkla karşılaştığında veya zorbalığa şahit olduğunda nasıl davranmayı düşünüyorsun?”

Bölüm 4: Dijital Sağlık ve Teknoloji Kullanımı Konusunda Çözümler ve Öneriler

4.1. Bağımlılığı Önleme

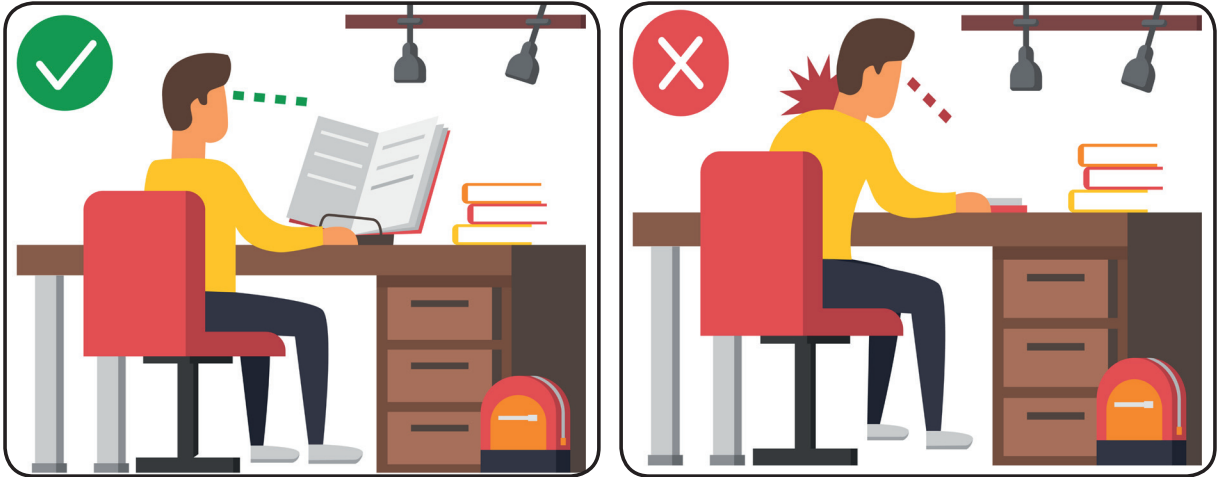
4.1.2. Bilinçli Kullanım

Teknoloji bağımlılığını önleme yöntemleri (ekran süresi yönetimi, bildirim ayarları vb.):

Teknoloji bağımlılığını önlemek için bilinçli kullanım stratejileri geliştirmek ve dijital cihazlarla sağlıklı bir denge kurmak önemlidir. Ekran süresi yönetimi, bu konuda atılabilecek en etkili adımlardan biridir. Dijital cihazların kullanım sürelerini sınırlandırmak, günlük ekran süresi hedefleri belirlemek ve bu hedeflere bağlı kalmak teknoloji kullanımını daha kontrollü hâle getirir. Bunun için birçok telefon ve bilgisayar, yerleşik ekran süresi izleme ve sınırlama özellikleri sunmaktadır. Aynı zamanda, uygulamalar için belirli kullanım süreleri ayarlanabilir ve bu süreler aşıldığında bildirim alınabilir.

Bildirim ayarlarını düzenlemek, teknolojinin sürekli dikkat dağıtıcı etkisini azaltmak için önemli bir adımdır. Sosyal medya, e-posta ve oyun gibi uygulamalardan gelen sürekli bildirimler; kullanıcının dijital cihazlara daha fazla vakit ayırmasına neden olabilir. Gereksiz bildirimleri kapatmak veya sadece belirli zaman dilimlerinde bildirim almak, teknoloji kullanımını daha verimli ve odaklı hâle getirir. Ayrıca, uygulamalara belirli saatlerde erişimi kısıtlamak veya “rahat-sız etmeyin” modu kullanarak belirli zaman dilimlerinde teknolojiye ara vermek de bağımlılıkla mücadelede etkili bir yöntemdir.

Bu yöntemlerin yanı sıra belirli zamanlarda dijital cihazlardan tamamen uzak durarak dijital detoks yapmak, zihin ve bedenin dinlenmesine yardımcı olur. Teknolojiyi amacına uygun ve sınırlı kullanmak, bağımlılık riskini azaltırken kullanıcıların dijital dünyada daha bilinçli ve dengeli bir yaşam sürmelerine olanak tanır.



4.2. Sağlıklı Dijital Alışkanlıklar

Dijital Detoks ve Ara Verme:

Sosyal medyadan belirli aralıklarla tamamen uzaklaşmak, zihni dinlendirmek ve dijital bağımlılığı azaltmak açısından etkili bir yöntemdir. Örneğin, haftada bir gün veya belirli saat dilimlerinde sosyal medya kullanımını tamamen durdurarak dijital detoks yapabiliriz.

Bilinçli Sosyal Medya Kullanımı:

Sosyal medyanın kontrollü kullanımı, faydaları ve riskleri:

Sosyal medya; bilgiye hızlı erişim, topluluk oluşturma ve eğlence gibi faydalar sunarken sosyal medyanın aşırı kullanımı anksiyete, depresyon, kıyaslama kültürü ve bağımlılık gibi riskler taşıyabilir. Bu nedenle; sosyal medyanın sağlığa zarar vermeyecek şekilde nasıl kullanılacağını öğrenmek, kullanıcıların psikolojik ve duygusal dengelerini korumalarına yardımcı olur. Sağlıklı sosyal medya alışkanlıkları, farkındalık ve sınır koyma becerileriyle geliştirilebilir (Çelik & Çelik 2023).

Ergonomik Çalışma ve Ekran Kullanımı:

4.2.1. Ergonomik Çalışma ve Ekran Kullanımı: Sağlıklı ve Verimli Bir Çalışma Alanı Nasıl Oluşturulur?

Ergonomik çalışma düzeni, hem sağlığı koruyan hem de verimliliği artıran bir ortam oluşturmayı amaçlar. Yanlış duruşlar ve uygun olmayan ekipmanlar zamanla boyun, sırt ve bilek ağrılarına, göz yorgunluğuna ve uzun vadeli ortopedik sorunlara yol açabilir. İşte ergonomik bir çalışma düzeni oluşturmak için izlenebilecek temel adımlar ve yapılabilecekler:

4.2.2. Doğru Oturma Pozisyonu

Ergonomik bir çalışma ortamı için oturma pozisyonu çok önemlidir. Sandalyeniz sırtınıza tam destek verecek şekilde ayarlanmalı ve ayaklarınız yere tam basmalıdır (Çalık vd,2013). Dizleriniz 90 derecelik bir açı yapmalı ve kalçalarınız diz seviyesinden biraz daha yukarıda olmalıdır. Sandalyenin sırt kısmı omurganızı desteklemeli ve bel bölgesine uygun eğime sahip olmalıdır.

Bu konuda ne yapabilirim:

- **Ayarlanabilir Ergonomik Sandalyeler:** Ergonomik sandalyeler, yükseklik ve sırt desteği ayarları ile farklı vücut tiplerine ve çalışma pozisyonlarına uyum sağlar.

4.2.3. Ekran Yüksekliği ve Konumu

Bilgisayar ekranınız göz hizasında ve yaklaşık 50-70 cm uzaklıkta olmalıdır. Ekranın çok aşağıda veya yukarıda olması boyun kaslarını zorlayabilir. Gözlerinizi yormamak için ekranı doğru dan karşınızda tutmalı ve ışığın yansımaları azaltmak için parlaklık ayarlarını düzenlemelisiniz.

Bu konuda ne yapabilirim:

- **Monitör Standları:** Ekran yüksekliğini doğru seviyeye getirmek için ayarlanabilir monitör standları kullanabilirsiniz. Bu, boyun ağrılarını ve duruş bozukluklarını önlemeye yardımcı olur.

4.2.4. Klavye ve Fare Yerleşimi

Klavye ve fare, dirseklerinizin yan tarafınızda ve 90-100 derece açıda duracağı şekilde yerleştirilmelidir. Bileklerinizi çok fazla bükmeden kullanabileceğiniz bir pozisyonda olmalı. Bileklerinizi dinlenmesi için uygun bir destek sağlayabilirsiniz.

Bu konuda ne yapabilirim:

- **Ergonomik Klavye ve Fare:** Bilek ve el kaslarına yüklenmeyi azaltan ergonomik klavyeler ve fareler kullanmak önemlidir. Dikey fareler bilek pozisyonunu doğal bir açıya getirir ve uzun süreli kullanımlarda rahatlık sağlar.

4.2.5. Ekran Işığının Kontrolü

Çalışma alanındaki aydınlatma, göz yorgunluğunu önlemek için yeterli ve doğru olmalıdır. Doğrudan ekrana gelen ışıklar yansımaya neden olabilir, bu yüzden ekranınızı ışık kaynağına dik açıyla yerleştirmek önemlidir. Mavi ışık filtresi kullanarak ekranlardan yayılan zararlı ışıkları azaltabilirsiniz.

Bu konuda ne yapabilirim:

- **Mavi Işık Filtresi ve Ekran Koruyucuları:** Ekran başında uzun süre çalışanlar için mavi ışık filtreli gözlükler, ekran koruyucuları veya ekran ışığı ile ilgili ayarlamalar yapmak göz yorgunluğunu azaltmada etkilidir.

4.2.6. Düzenli Molalar

Uzun süre aynı pozisyonda oturmak, kaslarda gerginlik ve yorgunluğa neden olabilir. Bu nedenle; her 30 dakikada bir kısa molalar vererek esneme hareketleri yapmak, kan dolaşımını artırır ve kas yorgunluğunu önler. “20-20-20” kuralı, ekran başında çalışanlar için ideal bir yöntemdir: Her 20 dakikada bir, 20 saniye boyunca 20 metre uzağa bakmak göz yorgunluğunu azaltır.

Bu konuda ne yapabilirim:

- **Zamanlayıcı Uygulamaları:** Zamanlama uygulamaları belirli aralıklarla mola vermenizi hatırlatarak sağlıklı bir çalışma rutini oluşturmaya yardımcı olabilir.

4.2.7. Ekipmanların Uygun Yükseklikte Ayarlanması

Çalışma alanınızın düzeni, tüm ekipmanların kolayca ulaşılabilir ve doğru yükseklikte olmasını sağlamalıdır. Masanızın yüksekliği omuzlarınızın rahat olmasını sağlayacak şekilde ayarlanmalı; klavye, fare ve diğer çalışma ekipmanlarınız da ellerinizin doğal bir şekilde durduğu konumda olmalıdır (Uluuysal & Kurt, 2011).

Bu konuda ne yapabilirim:

- **Ayarlanabilir Masalar:** Ayakta ve oturarak çalışma imkânı sağlayan ayarlanabilir masalar, çalışma süresince pozisyon değiştirme imkânı sunar. Bu, sırt ve boyun ağrılarını azaltırken verimliliği de artırır.



Etkinlik

Dijital Göz Koruma Hedefi

Amaç:

Katılımcıların dijital göz koruma yöntemlerini tanımasını ve uygulamasını sağlamayı amaçlamaktadır.

Hedef Kartları: Her biri farklı göz koruma ipuçlarını veya duruşları içeren kartlar (örneğin; “20-20-20 kuralı”, “doğru duruş”, “ekran mesafesi”, mavi ışık filtresi uygulamaları, göz muayeneleri, ekran parlaklığı, ortamın aydınlatılması gibi).

Atış Malzemeleri: Kâğıt topları, yumuşak toplar veya benzeri atış malzemeleri.

Hedef Panosu: Kartları yerleştirebileceğiniz bir pano veya duvarda bir alan.

Oyun Kuralları

Hedef kartları (her biri farklı bir göz koruma ipucu içeren) bir panoya veya duvara yerleştirilir. Katılımcılar 3-4 kişilik gruplara ayrılır. Her grup sırayla, atış malzemesini kullanarak hedef kartlarına atış yapar. Her atış için 1-2 dakika süre verilir. Her grup, kartlara attıkları atış sonrasında üzerlerinde yazılı ipuçlarını açıklamak zorundadır. Örneğin; “20-20-20 kuralı”na atış yaptıklarında, bu kuralın ne olduğunu ve nasıl uygulanması gerektiğini anlatırlar. Doğru açıklama yapan gruplara puan verilir. Atış başarı oranına göre ek puanlar da verilebilir. Her grup farklı kartlar üzerinde çalışarak hepsini açıklamaya çalışır.

Oyun sonunda en yüksek puanı toplayan grup, kazanan ilan edilir. Her grubun öğrendiklerini paylaşması için zaman ayrılır.



Etkinlik

Ergonomi ve Duruş Atölyesi (Duruş Yüzleşmesi)

Amaç:

Katılımcıların; ergonominin ve doğru vücut duruşunun önemini öğrenmesi, sağlıklı alışkanlıklar kazanması ve duruş bozukluklarını fark etmesi amaçlanmaktadır.

Gerekli Malzemeler:

- Masalar ve sandalyeler (sınıf içi veya dış mekân)
- Farklı yüksekliklerdeki sandalyeler
- Doğru duruşu gösteren posterler veya görseller

Etkinliğin başında ergonominin ne olduğu, doğru vücut duruşunun neden önemli olduğu ve duruş bozukluklarının etkileri anlatılır. Vücut duruşu bozukluklarının baş ağrısı, bel ağrısı ve diğer sağlık sorunlarına yol açabileceği vurgulanır. Katılımcılar, kendi çalışma alanlarını (masa ve sandalye) ergonomik hâle getirmeleri için gruplara ayrılır. Her grup, masanın ve sandalyenin doğru yüksekliklerini ayarlamak için birlikte çalışır.

Dikkat Edilecek Noktalar: Sandalyenin yüksekliği, sırt destekleri, ayakların yerde düz durması gibi konuları gözden geçirin.

Uygulama: Katılımcılara doğru oturuş ve duruş pozisyonları gösterilir. Doğru duruş için dikkat edilmesi gereken noktalar anlatılır (omuzların geri, belin düz, başın dik durması gibi).

Her katılımcı, ayna karşısında veya arkadaşlarının gözünde duruşunu kontrol eder.

**Etkinlik****Oyun - Duruş Yüzleşmesi:**

Katılımcıların doğru ve yanlış duruşları tanımasını ve doğru duruşları uygulamasını amaçlar.

Gerekli Malzemeler: Doğru ve yanlış duruşları gösteren resimler veya kartlar

Oyun Kuralları: Katılımcılar iki gruba ayrılır. Her grup, bir “doğru” ve bir “yanlış” duruş kartı alır. Eğitimci, her gruba sırayla duruş kartlarını gösterir. Kartta gösterilen duruşa göre gruplar “doğru” veya “yanlış” olarak cevap verir. Doğru cevabı veren grup, duruşu göstermelidir. Yanlış cevabı veren grup, duruşu düzeltmek için birlikte çalışır. Oyun sonunda, hangi duruşların doğru hangilerinin yanlış olduğu ve nedeni tartışılır.

KAYNAKÇA

- Bostancı, O. D. B. (2016). Dijital göz yorgunluğu sendromu ve kuru göz. MN Oftalmoloji, 23(1), 96-99.
- Çalık, B. B., Atalay, O. T., Başkan, E., & Gökçe, B. (2013). Bilgisayar kullanan masabaşı çalışanlarında kas iskelet sistemi rahatsızlıkları, işin engellenmesi ve risk faktörlerinin incelenmesi. Müsbed, 3(4), 208-214.
- Çelik, E., & Çelik, O. T. (2023). Çocuklarda dijital bağımlılığın öncülleri ve ardılları: Bir metasentez çalışması. Millî Eğitim Dergisi, 52(239), 1913-1944.
- Muslu, G. K., & Bolışık, B. (2009). Çocuk ve Gençlerde İnternet Kullanımı. TAF Preventive Medicine Bulletin, 8(5), 445-450.
- Uluuysal, B., & Kurt, A. A. (2011). İLKÖĞRETİM BİLGİSAYAR LABORATUARLARININ ERGONOMİK İLKELERE GÖRE İNCELENMESİ: ESKİŞEHİR İLİ ÖRNEĞİ. Ahi Evran Üniversitesi Kırşehir Eğitim Fakültesi Dergisi, 12(2), 271-285.
- Vural, Ö., Eler, S., & Güzel, N. A. (2010). Masa başı çalışanlarda fiziksel aktivite düzeyi ve yaşam kalitesi ilişkisi. Spormetre beden eğitimi ve spor bilimleri dergisi, 8(2), 69-75.

MODÜL 3

Dijital Eriřim



Modül Kapsamı

Dijital erişim, bireylerin eşit ve aktif bir şekilde dijital teknolojilere (bilgisayar, akıllı telefon, tablet vb.) ve internete ulaşabilme imkânını ifade eder. Dijital erişim yalnızca fiziksel bir internet bağlantısına sahip olmayı değil aynı zamanda bu bağlantının kalitesinin, hızının ve güvenliğinin bireyler açısından yeterli olmasını; bireylerin dijital teknolojileri kullanabilme yönündeki becerilerini de kapsar (Aldemir ve Avşar 2020). Bireylerin dijital dünyaya dâhil olmasını sağlayan dijital erişim, bireylerin dijital ortamlarda var olmalarına ve etkileşime girebilmelerine de olanak tanır.

Öğrenme Kazanımları

- Yerel kuruluşların dijital erişim ve kapsayıcılık alanındaki çalışmalarını tanımak.
- SWOT analizi ile kuruluşların güçlü ve zayıf yönlerini, fırsatlarını ve tehditlerini belirlemek.
- Dijital vatandaşlık bilinciyle topluma katkı sağlama becerisi kazanmak.

İçerik Ağacı

1. Dijital Dünyada Erişim ve Kapsayıcılık Ne Anlama Gelir?
2. Etkinlikler
 - 2.1. İlgili Kuruluşların Belirlenmesi
 - 2.2. SWOT Analizi Hazırlığı
 - 2.3. Dijital Erişimin Boyutları
 - 2.4. Tartışma Soruları
 - 2.5. Dijital Erişim Haritası Hazırlığı
 - 2.6. Dijital Erişim Anketi

Dijital Dünyada Eriřim ve Kapsayıcılık Ne Anlama Gelir?

Dijital bir vatandaş olmak için dijital teknolojiye erişim şarttır, ancak yeterli değildir. Çevrim içi dünya fırsatlarla dolu, uçsuz bucaksız, sınırsız bir alandır. Aynı zamanda pek çok açıdan çevrim dışı dünyadan daha zorludur, özellikle de kullanıcılara sağladığı hem görünür hem anonim olabilme fırsatı sayesinde katlanarak artan bir yayılma gücüne sahiptir (Tonta, 2002). Bu nedenle dijital erişim, yalnızca çevrim içi dünyanın sonsuz labirentlerinde etkin bir şekilde gezinmek için teknik becerileri değil aynı zamanda insan onuru ve insan haklarının temel değerlerine dayalı olarak başkalarına karşı sorumluluk ve saygı duygusunu da gerektirir.

Teknolojiye erişim; her şekil ve biçimde yeni öğrenme, iletişim, yaratıcı araçlar ve platformlar sunmaktadır. Bunlar arasında; kişisel veya dizüstü bilgisayar ve klavye, cep telefonları, tabletler ve oyun konsolları, uygulamalar ve günümüzde kullanılan robotlar, oyuncakların interneti ve nesnelerin interneti gibi pek çok şey yer almaktadır. Dijital vatandaşların sorumluluklarından biri, aktif olduğumuz her toplulukta olduğu gibi, bu dijital alanlarda azınlık gruplarına, daha az yetenekli kişilere ve hayatın her kesiminden insanların görüşlerine açıklık sağlamaktır. Bu, “kapsayıcılık” kavramının yalnızca bir yönüdür (Avrupa Konseyi, 2022).

İnternetin ortaya çıkışından çeyrek asır sonra bugün, Avrupa vatandaşlarının dörtte birinin internete erişimi olmadığı tahmin edilmektedir. Küresel nüfusa baktığımızda bu oran neredeyse her iki kişiden birinin internet erişimi olmadığını göstermektedir. Pek çok ülkede, çocukların var olan potansiyellerini gerçekleştirmelerini ve dijitalleşen dünyada aktif vatandaşlar olarak rol almalarını sağlayacak eşit fırsatları sunmak, okulların görevi olarak kabul edilmektedir. Ancak 2014 yılında OECD, üye ülkelerin sadece dörtte birinin eğitim sistemleri aracılığıyla eşit düzeyde erişim sağladığını bildirmiştir (Beaunoyer vd., 2020).

Teknoloji, büyük ölçüde temel müfredat derslerine bir eklenti olarak değerlendirilmekte ve okullardaki dijital vatandaşlık eğitimi amacına ulaşamamaktadır. Bazı ülkeler Kendi Cihazını Getir (BYOD) mekanizmasını denemekte ancak bu da eşitlik ve güvenlik sorunlarını gündeme getirmektedir. Kapsayıcılık önemli olsa da amacı iyi olmayan yazılımları ve meraklı gözleri etkisiz hâle getirmenin gün geçtikçe büyüyen bir zorluk olduğunun hızla farkına varılmaktadır.

Sınırlı eğitim fırsatları ve düşük gelir, dünya çapındaki ülkelerde erişim ve kapsayıcılığın önündeki en büyük engeller olarak ortaya çıkmaktadır (Choi, 2016). Bununla birlikte, teknolojinin satın alınabilirliği ve ulaşılabilirliği giderek artmaktadır. 2016 yılında aktif internet kullanıcı sayısında 2015 yılına göre %21’lik bir artış görülürken mobil kullanıcı sayısındaki artış şaşırtıcı bir şekilde %5’te kalmıştır.

Modüllerde birden fazla etkinlik seçeneği sunulmuştur, uygun bulduğunuz etkinliği kullanabilirsiniz.



Etkinlik

1. İlgili Kuruluşların Belirlenmesi

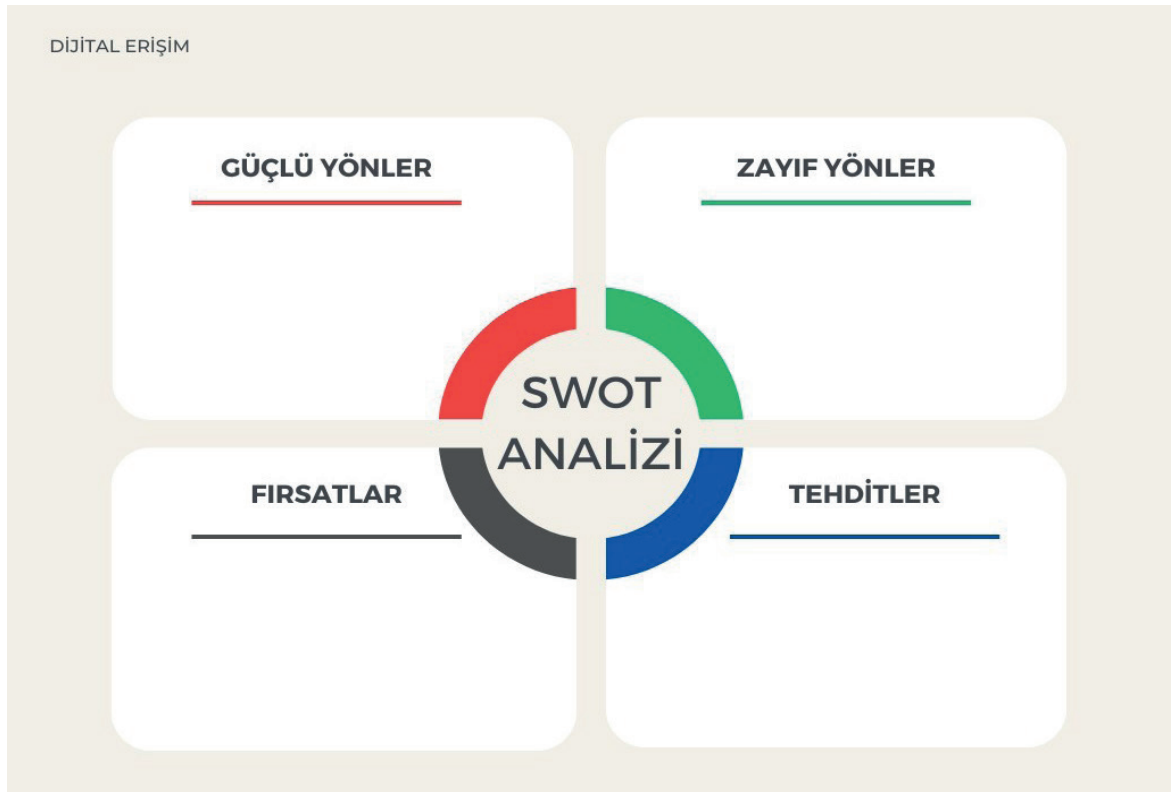
Görev: Öğrencilerle birlikte, topluluğunuzda dijital erişimi ve kapsayıcılığı sağlamaya çalışan ilgili kuruluşların bir listesini oluşturunuz. Bu kuruluşlar; dijital beceri geliştirme, internet erişimi sağlama ya da dijital içeriklere erişim konusunda yardım sunan kuruluşlar olabilir.

Amaç: Topluluğunuzda dijital erişimle ilgili hangi kuruluşların faaliyet gösterdiğini anlamak ve bu kuruluşların etkisini analiz etmek için bir temel oluşturmak.

2. SWOT Analizi Hazırlığı

Görev: Öğrenciler, belirledikleri yerel kuruluşların dijital kapsayıcılık çalışmalarını değerlendirmek amacıyla iki veya üç SWOT analizi yapacaktır. SWOT analizi; bu kuruluşların güçlü yönlerini, zayıf yönlerini, fırsatlarını ve karşı karşıya oldukları tehditleri değerlendirmeye olanak tanır. Bu süreçte, öğrencilerin kolayca kullanabileceği bir çevrim içi araç seçiniz.

Amaç: SWOT analizi yoluyla kuruluşların performansını değerlendirmek ve performanslarını iyileştirme fırsatlarını tespit etmek.



Tablo 2: SWOT Analizi Tablosu

Tablodan yararlanarak analiz yapabilirsiniz.

3. Dijital Erişimin Boyutları

Dijital erişim, bireylerin dijital teknolojilere ve internete erişim sağlama imkânını ifade eder. Dijital erişim yalnızca bir internet bağlantısına sahip olmayı değil aynı zamanda bu bağlantının kalitesini, hızını, cihazların uygunluğunu ve bireylerin dijital becerilere sahip olup olmamasını da kapsar.

	Fiziksel Erişim: Bireylerin internete bağlanabilmeleri için gerekli olan altyapının, cihazların ve internet hizmetlerinin mevcudiyeti.
	Ekonomik Erişim: Dijital cihazlara ve internete ulaşma maliyetlerinin düşük gelirli bireyler ve bölgeler için karşılanabilir olması.
	Sosyal ve Kültürel Erişim: Toplumun farklı kesimlerinin dijital erişimden nasıl faydalandıkları ve bu erişimin toplum üzerindeki etkileri. Dezavantajlı grupların dijital dünyaya dâhil edilmesi.
	Eğitimsel Erişim: Bireylerin dijital teknolojileri nasıl kullanacaklarını öğrenmeleri, dijital becerilere sahip olmaları ve bu becerileri sürekli olarak geliştirmeleri.

Tablo 3: Dijital Erişimin Farklı Boyutları



Etkinlik

4. Tartışma Soruları

- Dijital erişim kavramı sadece teknolojik cihazlara sahip olmakla mı sınırlıdır, bu kavramı sosyal ve ekonomik açıdan nasıl daha geniş bir perspektifte ele alabiliriz?
- Toplumda dijital erişimin eşit olmayışı, sosyal adalet ve ekonomik gelişim açısından hangi derin etkileri doğurur? Dijital uçurum kavramını, sadece bir erişim meselesi olarak değil; bir güç ve etki sorunu olarak nasıl inceleyebiliriz?

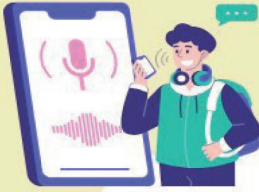
- Kendi topluluğunuzda dijital erişim eksiklerini ve potansiyel fırsatları değerlendirirken eksikleri gidermek ve fırsatları artırmak adına yaratıcı bir çözüm önerisi sunabilir misiniz? Özellikle, dijital okuryazarlığı ve teknolojiye erişimi artırmaya yönelik yenilikçi fikirler nasıl uygulanabilir?

ETKİNLİK ÖNERİLERİ

Dijital Görevler ve Yarışmalar:



Topluluk üyelerine belirli dijital görevler atanır. Örneğin e-devlet üzerinden bir hizmeti kullanma, çevrim içi güvenlik testini geçme, bir dijital beceri öğrenme (örneğin temel kodlama) gibi. Her görev tamamlandığında grup bir puan alır.



Dijital Yardım Görevi: DVE Gönüllüleri

Katılımcılar, dijital beceri konusunda zorlanan bir komşularına yardım ederek puan kazanırlar. Örneğin bir yaşlı bireyin akıllı telefon kullanmayı öğrenmesine yardımcı olabilirler, e-devlet sisteminde bir işlem yapmalarına destek olabilirler veya bir arkadaşlarına sosyal medya hesap güvenliği hakkında bilgi verebilirler.



Etkinlik

5. Dijital Eriřim Haritası Hazırlığı

- Kursiyerleri küçük gruplara ayırınız (3-4 kişilik gruplar).
- Her gruptan kendi il veya ilçelerinde dijital erişimin nasıl sağlandığını gösteren bir “Dijital Eriřim Haritası” oluřturmasını isteyiniz. Harita, ařağıdaki unsurları içermelidir:
 - o **Fiziksel erişim:** İnternet hizmeti sağlayıcıları, halka açık Wi-Fi noktaları, kütüphaneler, internet kafeler.
 - o **Ekonomik erişim:** Cihazlara ve internet hizmetine ulaşma maliyetleri, düşük gelirli aileler için sağlanan fırsatlar.
 - o **Eğitimsel erişim:** Dijital becerileri öğretmeye yönelik yerel programlar, okulların sunduğı dijital kaynaklar.
 - o **Engeller:** Topluluklarındaki dijital erişimi kısıtlayan fiziksel, ekonomik veya sosyal engeller (örneğin; altyapı eksiklikleri, yüksek maliyetler).

Gruplar haritalarını renkli kalemlemlerle çizebilir veya dijital araçlarla hazırlayabilir.



Etkinlik

6. Dijital Eriřim Anketi

Amaç: Bu anket, topluluğunuzdaki bireylerin dijital teknolojilere ve internete erişim durumunu değerlendirmek ve dijital erişimle ilgili mevcut sorunları tespit etmek için hazırlanmıştır.

1. Evde internet bağlantınız var mı?

- ☐ Evet
☐ Hayır

2. İnternet bağlantı hızınız nasıl?

- ☐ Çok yavaş
☐ Orta
☐ Hızlı
☐ Çok hızlı

3. Aşağıdaki dijital cihazlardan hangilerine erişiminiz var? (Birden fazla seçeneği işaretleyebilirsiniz.)

- ☐ Akıllı telefon
☐ Bilgisayar
☐ Tablet
☐ Akıllı televizyon

Diğer: _____

4. Dijital cihazlarınızı genellikle nerede kullanıyorsunuz?

- ☐ Evde
☐ İş yerinde
☐ Okulda
☐ Kütüphanede veya başka bir halka açık alanda
☐ İnternet kafede

Diğer: _____

5. Dijital teknolojileri ne sıklıkla kullanıyorsunuz?

- ☐ Her gün
- ☐ Haftada birkaç kez
- ☐ Haftada bir
- ☐ Nadiren
- ☐ Hiç

6. İnterneti en çok hangi amaçlarla kullanıyorsunuz? (Birden fazla seçeneği işaretleyebilirsiniz.)

- ☐ Sosyal medya
- ☐ İş ve iş başvuruları
- ☐ Eğitim ve araştırma
- ☐ Alışveriş
- ☐ Bankacılık işlemleri
- ☐ Eğlence (film, müzik, oyun)

Diğer: _____

7. Dijital becerilerinizi geliştirme konusunda fırsatlarınız var mı?

- ☐ Evet, dijital beceri geliştirme kurslarına katılıyorum.
- ☐ Hayır, fırsatım yok.
- ☐ Kendi kendime öğreniyorum.

8. Dijital cihaz ve internet kullanırken karşılaştığınız en büyük zorluk nedir?

- ☐ Düşük internet hızı
- ☐ Cihazların eski veya işlevsiz olması
- ☐ Dijital becerilerimin yetersiz olması
- ☐ Dijital kaynaklara erişimde sorun yaşamak
- ☐ Güvenlik ve gizlilik endişeleri

Diğer: _____

9. Dijital becerilerinizi geliştirmek veya internete erişiminizi iyileştirmek için herhangi bir öneriniz var mı?

KAYNAKÇA

Aldemir, C., & Avşar, M. N. (2020). Pandemi Döneminde Dijital Vatandaşlık Uygulamaları. *Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi*, 7(5), 148-169.

Avrupa Konseyi (2022). Dijital Vatandaşlık Eğitimi El Kitabı. Avrupa Konseyi Yayınları

Beaunoyer, E., Dupéré, S. ve Guitton, M. J. (2020). Covid-19 and digital inequalities: reciprocal impacts and mitigation strategies. *Computers in Human Behavior*, 111, 1-9.

Choi, M. (2016) A Concept Analysis of Digital Citizenship for Democratic Citizenship Education in the Internet Age, *Theory & Research in Social Education*, 44(4), 565-607, DOI:10.1080/00933104.2016.1210549

Tonta, Y. (2002). Dijital hizmetlere ve kaynaklara erişim. bildiri. PULMAN-XT Türkiye Ulusal Toplantısı, 16-19.

MODÜL 4

Dijital İletişim



Modül Kapsamı

Bu modül, günümüzün teknoloji odaklı dünyasında dijital iletişimin hem kişisel hem de profesyonel sosyal etkileşimler üzerindeki etkisini inceleyen kapsamlı bir rehber sunmaktadır. Anlık mesajlaşma, e-postalar, sosyal ağlar gibi çeşitli dijital iletişim araçlarını ve yöntemlerini inceleyerek her bir yöntemin geleneksel yüz yüze etkileşimden ne kadar farklı olduğunu vurgulamaktadır. Sözel olmayan ipuçlarının yokluğu ve çevrim içi alışverişlerin eş zamansız doğası gibi dijital iletişimin nüanslarını ele alan modül, kullanıcıların dikkatli ve etkili dijital uygulamaları benimsemeleri gerektiğini vurgulamaktadır. Ayrıca dijital vatandaşlığın kritik bileşenleri olarak çevrim içi kimliğin, gizliliğin ve dijital alanlara saygılı katılımın önemi vurgulanmaktadır.

Modül ayrıca; sosyal medyada sorumlu davranış, siber zorbalık ve gizlilik ihlalleri gibi çevrim içi risklerin farkındalığı da dâhil olmak üzere sağlıklı bir dijital varlığı teşvik etmek için gerekli etik hususları kapsamaktadır. Senaryolar ve aktiviteler aracılığıyla katılımcılar çatışma çözme stratejilerini uygulamaya ve çevrim içi etkileşimlerde empati geliştirmeye teşvik edilerek yanlış anlaşılmalara yapıcı bir şekilde ele alabilecekleri araçlarla donatılmaktadır. Modül; bu ilkeleri entegre ederek kullanıcıların çevrim içi eylemlerinin daha geniş etkilerinin farkında oldukları ve dijital alanlarda düşünceli bir şekilde etkileşimde bulunabildikleri, bağlanabilirliği etik sorumlulukla dengeledikleri bir dijital ekosistemi teşvik etmeyi amaçlamaktadır.

Öğrenme Kazanımları

Modülün sonuna kadar katılımcılar;

- Dijital iletişim araçlarını (e-posta, anlık mesajlaşma, sosyal medya, vb.) tanırlar ve Çevrim içi ve çevrim dışı iletişim arasındaki farkları kavrar.
- Çevrim içi ortamda etik ve saygılı bir dijital varlık oluşturma ve sürdürmenin önemini anlayarak dijital kimliklerini sorumlu bir şekilde yönetir.
- Dijital platformlarda gizlilik ve güvenliğin korunmasına yönelik stratejileri öğrenir ve kişisel bilgilerin korunmasının önemini fark eder.
- Etik kurallar doğrultusunda çevrim içi hareket etmenin gerekliliğini kavrar ve sosyal medya gibi dijital platformlarda uygun iletişim tekniklerini benimser.
- Çevrim içi yanlış anlamaları çözme, empati geliştirme ve saygılı iletişim kurma becerileri kazanarak dijital ortamlarda çatışma yönetimi yapar.
- Dijital içeriklerin ve çevrim içi davranışların etkilerini eleştirel bir bakış açısıyla değerlendirerek dikkatli ve sorumlu karar alma becerisi geliştirir.

İçerik Ağacı

1. Giriş
2. Dijital İletişim
3. Dijital İletişim ve İlişkiler
4. İletişimin Dijital Hâlinde Dikkat Edilmesi Gerekenler
5. Etkinlikler

1.Giriş

1.1. Dijital İletişim

Dijital iletişim, günümüzde hem kişisel hem de profesyonel bağlamlarda giderek daha önemli bir rol üstlenmiştir. Sözel olmayan ipuçlarının eksikliği ve zaman uyumsuzluğu gibi dijital iletişime özgü özellikler, bu iletişim biçimini geleneksel yüz yüze iletişimden belirgin şekilde ayırmaktadır. Bu farklılıklar, geleneksel iletişimle ilgili mevcut bulguların dijital bağlamda geçerliliği konusunda önemli soruları gündeme getirmekte ve dijital iletişim süreçlerinin özel niteliklerini anlamaya yönelik yeni araştırmaların gerekliliğini ortaya koymaktadır (Strauss, Harr ve Pieper, 2024).

İletişim teknolojisi, basitten karmaşığa doğru geniş bir araç yelpazesi sunmaktadır ve dijital medya iletişim yeteneklerimizi büyük ölçüde genişletmiştir. İletişim, yüz yüze ve çevrim dışı etkileşimlerin çok ötesine geçmiştir ve artık çevrim içi ortamlarda çeşitli biçimler ve yöntemler mevcuttur. Aşağıdakiler de dâhil olmak üzere çeşitli iletişim yöntemleri vardır:

- **Sohbet:** Çevrim içi bir ortamda özel bir tartışma kanalında etkileşimli iletişim için kullanılan gayri resmi bir terimdir.
- **Anlık mesajlaşma:** Anında mesaj alışverişine izin veren gerçek zamanlı bir metin iletişimi biçimidir.
- **SMS:** Cep telefonları aracılığıyla kısa metin mesajları göndermek için kullanılan kısa mesaj hizmetidir.
- **E-postalar:** Elektronik posta sistemleri aracılığıyla gönderilen dijital yazışmalardır.
- **VoIP (İnternet Protokolü Üzerinden Ses):** İnternet üzerinden sesli aramalar yoluyla yapılan iletişimdir.
- **Sosyal ağlar:** Kullanıcıların geniş kitlelerle iletişim kurmasını ve içerik paylaşmasını sağlayan platformlardır.
- **Podcastler:** Akış veya indirme için internet üzerinden paylaşılan önceden kaydedilmiş ses içerikleridir.
- **Sanal ve artırılmış gerçeklik ortamları:** Kullanıcıların simüle edilmiş veya geliştirilmiş gerçeklikler içinde iletişim kurmasına olanak tanıyan sürükleyici dijital alanlardır.
- **Oyun platformları:** Kullanıcıların video oyunları oynarken etkileşim ve iletişim kurduğu dijital ortamlardır (Council of Europe, 2022).

Teknoloji geliştikçe sanal gerçeklik (VR) ve artırılmış gerçeklik (AR) gibi yeni iletişim biçimleri ortaya çıkmaktadır. Sanal gerçeklik (VR) kullanıcıların, varlıklarının gerçek ya da hayali bir alanda simüle edildiği dijital bir ortamda etkileşime girmelerine olanak tanır. Buna karşılık artırılmış gerçeklik (AR); bilgisayar tarafından oluşturulan unsurları üst üste bindirerek mevcut fiziksel dünyayı geliştirir, deneyimi daha sürükleyici hâle getirir ve anlamlı etkileşime izin verir.

Hem VR hem de AR iletişim şeklimizi dönüştürme potansiyeline sahiptir. Bu teknolojiler tarafından sunulan sürükleyici deneyimler, her bireyin kendine özgü gerçeklik algısına göre uyarlanabilir ve sosyal etkileşimlerin kişiselleştirildiği iletişime yeni bir boyut kazandırır. Bu, iletişimin artık her bir katılımcı tarafından algılanan farklı gerçekliklere uyum sağlayan özelleştirilmiş bir sosyal karşılaşma olarak deneyimlenebileceği anlamına geliyor. Teknolojideki bu ilerlemeler; geleneksel iletişim biçimlerini dinamik, çok katmanlı deneyimlere dönüştürerek etkileşim olanaklarımızı genişletiyor.

1.2. Dijital İletişim ve İlişkiler

Günümüz dünyasında artan teknolojik imkânlar, insanların birbirleriyle nasıl iletişim kurduklarını önemli ölçüde etkilemiştir. Çevrim içi oyunlar ve sosyal medya gibi dijital platformlar, çeşitli eğlence seçenekleri sunarak ve sosyal etkileşimleri teşvik ederek boş zaman etkinliklerinin ayrılmaz bir parçası hâline gelmiştir. Bununla birlikte yüz yüze etkileşimlerin azalması, potansiyel teknoloji bağımlılığı ile ilgili endişeleri de beraberinde getirmektedir (Elnur, 2023).

İnternetin günlük hayatımızdaki varlığının giderek artması ile çevrim içi kimliklerimiz daha önemli hâle geldi. Dijital alanlarda birbirimizle etkileşim kurma şeklimiz hem olumlu hem de olumsuz etkilere sahip olabilir ve sadece kendimizi değil çevremizdekileri de etkileyebilir. Sorumlu bir şekilde ve başkalarının haklarını ihlâl etmeden iletişim kurarken sağlıklı bir dijital varlık oluşturmak ve sürdürmek, dijital vatandaşlık açısından çok önemlidir.

Dijital iletişim bağlamında çevrim içi kimliklerin artan önemi, bireylerin sanal etkileşimlerine özen ve iyi niyetle yaklaşmaları gerektiğinin altını çizmektedir. Fiziksel ve dijital dünyalar arasındaki sınırlar giderek daha fazla iç içe geçerken çevrim içi davranışlarımız genellikle kişisel değerlerimizin doğrudan bir yansımasıdır ve hem profesyonel hem de sosyal alanlarda nasıl algılandığımızı etkiler. Yüz yüze iletişimde olduğu gibi dijital etkileşimlerin de ilişkileri şekillendirme, itibar oluşturma ve başkalarını yapıcı ya da yıkıcı bir şekilde etkileme potansiyeli taşıdığını kabul etmek önemlidir.

Etkili dijital vatandaşlık, çevrim içi alanlara katılmanın getirdiği etik sorumlulukların anlaşılmasını içerir. Bireyler; saygılı iletişimi teşvik etme, kapsayıcılığı destekleme ve başkalarının haklarını koruma konusundaki rollerinin farkında olmalıdır. Bu; gizlilik, fikri mülkiyet ve ifade özgürlüğünün önemini kabul ederken bu hakları sorumlu iletişim ihtiyacıyla dengelemeyi de içerir. Bu bağlamda; çevrim içi iletişim her zaman dijital ekosisteme olumlu katkıda bulunmayı hedeflemeli, etkileşimlerin saygılı, düşünceli ve etik standartlarla uyumlu olmasını sağlamalıdır (Council of Europe, 2022).

Sorumlu bir e-varlık sürdürmek, yalnızca kişinin dijital faaliyetlerinin kişisel etkisinin farkında olmasını değil aynı zamanda toplum için daha geniş etkilerini anlamasını da içerir. Sosyal medya, çevrim içi forumlar ve dijital iş birliği araçlarının giderek yaygınlaşmasıyla birlikte bireyler sürekli olarak coğrafi sınırları aşan bir iletişim içerisine girmektedir. Dolayısıyla sağlıklı ve yapıcı bir dijital ortam yaratmak ortak bir sorumluluktur ve bireylerin dürüstlük, empati ve eylemlerinin sonuçlarının farkında olarak hareket etmelerini gerektirir.

İletişim uygulamalarınız; sanal sosyal alanlarda başkalarıyla paylaştığınız etkileşimleri, fikirleri, görüntüleri, videoları ve bilgi parçalarını kapsar. Doğal olarak, bu iletişimler hem çevrim içi hem de çevrim dışı olarak gerçekleşebilir ve genellikle iki alan arasında geçiş yapar. Dijital ortamlarda başlayan etkileşimler çevrim dışı alışverişleri etkileyebilir ve benzer şekilde, yüz yüze konuşmalar çevrim içi platformlara taşınabilir. Çevrim içi ve çevrim dışı iletişim arasındaki bu akışkanlık, sanal ve fiziksel dünya arasındaki sınırların giderek bulanıklaştığı modern etkileşimin birbirine bağlı doğasını vurgulamaktadır.

Tıpkı e-varlıkta olduğu gibi, iletişim uygulamaları da olumlu ya da olumsuz olabilir. Olumlu iletişimi teşvik etmek için gereken beceriler, bireyin bir mesaj oluşturmadaki sosyal ve bilişsel yetenekleriyle yakından bağlantılıdır. Etkileşimlerin izlenebildiği, paylaşılabildiği ve hızla yayılabildiği, genellikle popüler hâle gelebildiği çevrim içi iletişimin doğası göz önüne alındığında dijital iletişimin topluma ve çevrim içi topluluklara olumlu katkıda bulunması kritik önem taşımaktadır. Çevrim içi etkileşimlerin geniş kitlelere ulaşma ve uzun süreli etkilere sahip olma potansiyeli; dijital alanlarda kasıtlı, etik ve sosyal açıdan sorumlu olmanın önemini vurgulamaktadır.

1.3. İletişimin Dijital Hâlinde Dikkat Edilmesi Gerekenler

Dijital çağda; çevrim içi olarak yüklediğiniz, yayımladığınız veya kaydettiğiniz her şey, kumdaki ayak izlerine benzer bir dijital ayak izi bırakır. Bu dijital iz, çevrim içi faaliyetlerinizin kalıcı bir kaydı olarak hizmet eder ve sanal etkileşimlerde dikkatli katılımın önemini vurgular.

İçeriği ne olursa olsun, herhangi bir mesaj göndermeden önce dikkatlice düşünmek çok önemlidir. Olumlu bir katkı olarak algıladığınız şey başkaları tarafından yanlış yorumlanabilir ve istenmeyen sonuçlara yol açabilir. Bu nedenle, iletişiminizin potansiyel etkisinin kritik bir şekilde değerlendirilmesi son derece önemlidir.

Konumunuz veya cinsiyetiniz hakkında ipucu verebilecek görüntüler de dâhil olmak üzere kimliğinizin belirlenmesine yol açabilecek kişisel bilgilerin korunması da çok önemlidir. Dijital alanda gizliliğin korunması, kimliğinizin ve kişisel güvenliğinizin korunması için esastır.

Kullandığınız ekipmana saygı duymak hayati önem taşıdığı gibi, okulunuzun veya işvereninizin sunucuları üzerinden gerçekleştirilen iletişimlerin gizli kalmayabileceğinin farkında olmak da önemlidir. Bu durum, özellikle kurumsal bağlamlarda çevrim içi etkileşimlerde sağduyu ve profesyonellik ihtiyacını vurgulamaktadır.

Ayrıca, çevrim içi katkılarınızın görünürlüğünü kontrol etmenize olanak tanıyan seçenekleri araştırmak akıllıca olacaktır. On yaşındayken paylaşılan görüntülerin veya düşüncelerin on altı yaşında tekrar ziyaret edildiğinde pişmanlık uyandırabileceğini göz önünde bulundurmak gerekmektedir. Gizlilik ayarlarını anlamak ve bunlardan yararlanmak bu tür durumları hafifletmeye ve daha olumlu bir çevrim içi varlığa teşvik etmeye yardımcı olabilir.

Dijital dünyada olumlu iletişim uygulamalarının benimsenmesi, kişisel bütünlüğün korunması ve saygılı etkileşimlerin teşvik edilmesi için çok önemlidir. Dijital ayak izlerimize ve çevrim içi faaliyetlerimizin olası sonuçlarına dikkat ederek daha yapıcı ve destekleyici bir dijital ortama katkıda bulunabiliriz.

Günümüz dünyasında dijital iletişim, bireylerin yenilikçi yöntemlerle etkileşim kurmalarını sağlar. Ancak; teknolojik araçların sunduğu avantajlara rağmen, dikkatle değerlendirilmesi gereken önemli riskleri ve sonuçları da bulunmaktadır, örneğin;

- Kişisel e-posta hesaplarına yetkisiz erişim.
- Resim, sembol ve emojilerin kullanımı da dâhil olmak üzere yazılı mesajların yanlış yorumlanma potansiyeli.
- E-postanın kimlik avı, dolandırıcılık ve diğer suçlarla ilgili faaliyetler de dâhil olmak üzere siber suçlular tarafından bir iletişim yöntemi olarak yaygın bir şekilde kullanılması.
- Sohbet odalarının sorumlu bir şekilde kullanılmasını ve tartışmaların yaşa uygun konulara odaklanmasını sağlamanın önemi (Council of Europe, 2022).

Çevrim içi iletişimin istenmeyen yönleri açısından bakıldığında; dijital alanlarda siber zorbalık, çevrim içi taciz, kandırma, siber takip ve hatta kişiler arası iletişimden kaçınma gibi çeşitli olumsuz faaliyetler tespit edilebilir.

Bu zararlı uygulamaların yaygınlaşması, daha fazla farkındalık ve sorumlu çevrim içi davranış ihtiyacını vurgulamaktadır. Çevrim içi ortamlar anonimliği kolaylaştırabilir, bu da genellikle bireyleri yüz yüze etkileşimlerde üstlenmeyecekleri eylemleri çevrim içi ortamda uygulama

konusunda cesaretlendirir. Sonuç olarak, dijital iletişimin etik ve sosyal sonuçlarını anlamak kritik önem taşımaktadır. Kullanıcıları, özellikle de gençleri, potansiyel tehlikeler ve saygılı ve sorumlu çevrim içi etkileşimi teşvik etmenin önemi konusunda eğitmeye odaklanılmalıdır.

Olumlu bir çevrim içi varlık geliştirmek için özellikle dijital iletişim alanında çeşitli uygulamalar önerilebilir:

Farklı amaçlar için ayrı e-posta hesapları: Sosyal medya katılımı veya çevrim içi alışveriş gibi çeşitli faaliyetler için farklı e-posta hesapları oluşturulması tavsiye edilir. Bu ayrı hesaplar aldatıcı olmak için değil daha ziyade gizliliğinizi korumak için bir araç olarak hizmet eder. Bu uygulama, kişisel ve profesyonel iletişimin bölümlere ayrılmasını sağlayarak istenmeyen gizlilik ihlalleri olasılığını azaltır.

Çevrim içi görgü kurallarına bağlılık: Doğru “internet etiği” uygulamak, dijital alanlarda saygılı iletişimi teşvik etmek için çok önemlidir. İster e-postalar ister diğer çevrim içi platformlar aracılığıyla olsun, mesajlarınızın geniş bir kitleye ulaşabileceğini daima göz önünde bulundurmak gerekmektedir. Bu nedenle, iletişiminizin içeriği ve hacmi düşünceli ve özenli olmalıdır. Tıpkı yüz yüze etkileşimlerde olduğu gibi, çevrim içi iletişimin tonu ve resmiyeti profesyonelliği ve hedef kitleye saygıyı yansıtmalıdır.

Göndermeden önce düşünün: E-posta göndermeden veya çevrim içi içerik yayımlamadan önce, mesajın halka açık bir ortamda rahatça söyleyebileceğiniz bir şey olup olmadığını düşünmek çok önemlidir. Dijital iletişimin kalıcılığı, özel konuşmaların bile paylaşılabileceği ve incelenebileceği anlamına gelir; bu da çevrim içi alanlarda kasıtlı ve düşünceli iletişimin önemini vurgular (Council of Europe, 2022).

Çevrim içi etkileşimlerin iletişimsel doğasını anlayın: Çevrim içi oyunlar oynamak veya sosyal medya tartışmalarına katılmak gibi çeşitli internet platformlarında başkalarıyla etkileşime girerken bu etkileşimlerin bir dijital iletişim biçimi oluşturduğunu unutmayın. Bu sanal ortamlarda başkalarıyla nasıl etkileşim kurduğunuz, genel dijital varlığınız üzerinde önemli bir etkiye sahiptir. Bu etkileşimler sırasında saygılı, empatik ve düşünceli davranmak yalnızca olumlu bir kişisel imajı desteklemekle kalmaz, aynı zamanda daha sağlıklı bir çevrim içi topluluğa da katkıda bulunur.

Olumlu bir çevrim içi varlığın oluşturulması ve sürdürülmesi saygılı iletişime aktif katılımı, kişinin dijital eylemlerinin sonuçlarını anlamayı ve kişisel gizliliği korumayı gerektirir. Bu da bağlanabilirliğin faydaları ile etik çevrim içi davranış sorumluluğunun dengelenmesini gerektirir. Fiziksel ve dijital iletişim arasındaki sınırlar bulanıklaşmaya devam ettikçe yapıcı ve saygılı bir çevrim içi varlığı teşvik etmenin önemi, dijital alanlarda anlamlı ve olumlu etkileşimleri sürdürmek için daha da önemli hâle gelmektedir.

1.4. Etkinlikler

Modüllerde birden fazla etkinlik seçeneği sunulmuştur, uygun bulduğunuz etkinliği kullanabilirsiniz.



Etkinlik

1. Drama Senaryoları: “Dijital Çatışmaların Çözümü”

Genel Bakış:

Bu etkinlikte katılımcılar, yanlış anlamaları ve çatışmaları etkili bir şekilde çözme pratiği yapmak için çevrim içi konuşmaları simüle edecek ve rol oynayacaklar. Bu senaryolara katılarak niyetleri netleştirme ve saygılı iletişim tekniklerini uygulama becerilerini geliştireceklerdir.

Amaç:

Katılımcılar; yaygın çevrim içi yanlış anlamaları veya çatışmaları tasvir eden senaryoları canlandırmak ve analiz etmek için iş birliği içinde çalışacak, çatışma çözümü ve dijital iletişim becerilerini geliştireceklerdir.

Gerekli Materyaller:

- Senaryo kartları (çeşitli çatışma durumları ile önceden hazırlanmış kartlar)
- Beyaz tahta ve keçeli kalem

Uygulama:

1. Giriş: Çevrim içi çatışmaların çözümünde iletişim becerilerinin önemini açıklayarak başlayınız. Yanlış yorumlanan mesajlar veya ton gibi dijital konuşmalarda meydana gelen yaygın yanlış anlamaları tartışınız. Katılımcıları çevrim içi etkileşimlerin yüz yüze konuşmalardan ne kadar farklı olduğunu düşünmeye teşvik ediniz.

2. Grup Oluşturma: Katılımcıları 4-5 kişilik küçük gruplara ayırınız. Her grup, canlandırmaları ve çözmeleri için bir çatışma durumu sunan senaryo kartı üzerinde çalışacaktır.

3. Senaryo Ödevi: Her gruba belirli bir çatışmayı anlatan bir senaryo kartı veriniz (örneğin; yanlış anlaşılan bir mesaj, bir siber zorbalık örneği). Her grup kendilerine verilen senaryoyu okuyacak ve tartışacak, temel çatışmayı belirleyecek ve bunu nasıl etkili bir şekilde canlandıracaklarını planlayacaktır.

4. Rol Oynama: Gruplar sırayla senaryolarını sınıfın önünde canlandıracaktır. Çatışma durumunu canlandıracak, çatışmanın nasıl tırmandığını gösterecek ve ardından etkili iletişim stratejileriyle çatışmayı çözmek için birlikte çalışacaklardır. Katılımcıları; çatışmayı yaratıcı bir şekilde ele almaları ve tonu netleştirmeleri, özür dileme veya yeniden ifade etme gibi olumlu etkileşim teknikleri sergilemeleri için teşvik ediniz.

5. Sınıf Tartışması: Tüm gruplar performanslarını sergiledikten sonra, çatışmaları çözmek için kullanılan farklı stratejiler üzerine bir sınıf tartışması yönetiniz. Her senaryoda neyin işe yaradığını analiz ediniz, benzer durumlarla başa çıkmanın alternatif yollarını tartışın ve çevrim içi etkileşimlerde empatinin, açıklığın ve saygılı dilin önemini pekiştiriniz.

Değerlendirme:

Katılımcıların rol yapma oyununa katılımı; aktif katılımlarına, senaryoya bağlılıklarına ve tartışmaları çözmede sergiledikleri yaratıcılığa göre değerlendirilecektir.



Etkinlik

2. Sosyal Medya Etiği Tartışması

Amaç: Katılımcılar, gençler arasında sosyal medya kullanımının etik sonuçları hakkında bir tartışma yürüteceklerdir.

Materyaller:

- Araştırma materyalleri (makaleler, çalışmalar)
- Münazara formatı kılavuzu

Uygulama:

- 1. Giriş:** “Genç kullanıcıları korumak için sosyal medya platformları düzenlenmeli mi?” Tartışma konusunu tanıtınız. Münazaranın kurallarını ve formatını açıklayınız.
- 2. Araştırma Aşaması:** Katılımcılar iki takıma ayrılacak (lehte ve aleyhte) ve verilen materyalleri kullanarak argümanlarını araştırmaları için zaman verilecektir.
- 3. Münazara Hazırlığı:** Takımlar açılış konuşmalarını ve karşı argümanlarını hazırlayacaktır.
- 4. Münazaranın Yürütülmesi:** Her takım argümanlarını sunacak, ardından çürütmeler ve kapanış konuşmaları yapılacaktır. Saygılı söylemi ve aktif dinlemeyi teşvik ediniz.
- 5. Yansıtma:** Münazaradan sonra katılımcılar ne öğrendikleri ve görüşlerinin nasıl değişmiş olabileceği üzerine kısa bir değerlendirme yazacaklardır.

Değerlendirme:

Değerlendirme; sunulan argümanların kalitesine, karşı argümanlara yanıt verme becerisine ve münazaraya genel katılıma göre yapılacaktır.



Etkinlik

3. Dijital Vatandaşlık Atölyesi

Amaç: Katılımcılar dijital vatandaşlık ilkelerini öğrenecek ve sorumlu çevrim içi davranış için yönergeler oluşturacaklardır.

Materyaller:

- Dijital vatandaşlık kaynakları (makaleler, videolar)
- Grafik kâğıdı ve keçeli kalem

Uygulama:

- 1. Giriş:** Dijital vatandaşlık kavramını ve bu kavramın günümüz toplumundaki önemini tanıttınız. Sorumlu çevrim içi davranış hakkında kısa bir video gösteriniz.
- 2. Grup Araştırması:** Katılımcılar küçük gruplar hâlinde dijital vatandaşlığın farklı yönlerini araştıracaklardır (örneğin; gizlilik, iletişim, çevrim içi görgü kuralları).
- 3. Kılavuz Oluşturma:** Her grup araştırmalarına dayanarak bir dizi kılavuz oluşturacaktır. Bu yönergeleri grafik kâğıdında sunacaklardır.
- 4. Galeri Gezintisi:** Gruplar hazırladıkları kılavuzları sınıfta sergileyeceklerdir. Katılımcılar etrafta dolaşacak, her bir kılavuzu okuyacak ve geri bildirimde ya da önerilerde bulunacaklardır.

Değerlendirme:

- Oluşturulan kılavuzların kalitesine, sunumdaki yaratıcılığa ve galeri yürüyüşü sırasında aktif katılıma dayanacaktır.



Etkinlik

4. İş Birliğine Dayalı İnfografik Oluşturma: “Etkili Dijital İletişim”

Genel Bakış:

Bu etkinlikte katılımcılar, etkili dijital iletişim konusunda bilgilendirici infografikler oluşturmak için birlikte çalışacaklar. Saygılı ve etkili çevrim içi etkileşim için en iyi uygulamaları vurgulayan ilgi çekici bir kılavuzu araştırarak, tasarlayacak ve derleyeceklerdir. Bu kılavuz, olumlu

dijital etkileşimleri teşvik eden ve dijital bağlamda iletişim nüansları konusunda farkındalığı artıran bir ekran kaynağı olarak hizmet edecektir.

Amaç:

Katılımcılar; açıklığa, izleyici farkındalığına ve saygılı dile odaklanarak etkili dijital iletişim için temel ipuçlarını ve stratejileri sunan infografikleri araştırmak ve tasarlamak için iş birliği yapacaklardır.

Gerekli Materyaller:

- Tasarım yazılımı veya çevrim içi infografik araçları olan bilgisayarlar (ör. Canva)
- Araştırma materyallerine erişim (makaleler, dijital iletişim uygulamalarına ilişkin çevrim içi kaynaklar)

Uygulama:

1. Giriş: Dijital iletişimin önemini ve sosyal etkileşimler üzerindeki etkisini tartışarak başlayınız. Katılımcıların gruplar hâlinde çalışarak dijital ortamlarda nasıl etkili iletişim kurabilecekleri konusunda ekranlarına rehberlik edebilecek bir infografik oluşturacaklarını açıklayınız. Nihai ürünlerinin görsel olarak çekici, bilgilendirici ve anlaşılması kolay olması gerektiğini vurgulayınız.

2. Araştırma ve Planlama: Katılımcıları küçük gruplara ayırınız ve her birine dijital iletişimin farklı bir yönünü veriniz (örneğin; netlik, ton, izleyici farkındalığı, saygılı dil). Her grup, kısa ama etkili bir infografik bölümü oluşturmaya odaklanarak örnekler ve en iyi uygulamalar dâhil olmak üzere bilgi toplayacaktır.

3. Infografik Tasarımı: Katılımcılar tasarım araçlarını kullanarak infografik bölümlerini oluşturmaya başlarlar. Onları düzen, renk şemaları, simgeler ve okunabilirliği artıracak diğer görseller hakkında yaratıcı düşünmeye teşvik ediniz. Her bölüm pratik ipuçları, ilgili örnekler ve temel mesajları net bir şekilde yakalamak için metin ve görsel dengesi içermelidir.

4. Infografiklerin Derlenmesi: Gruplar kendi bölümlerini tamamladıktan sonra, infografikleri uyumlu bir dijital rehber hâline getirmek için bir araya geleceklerdir. Bir kapak sayfası, kısa bir giriş ve her grubun katkısını tanımak için kredi ekleyebilirler. Bu nihai ürün sınıf içinde paylaşılabilir veya dijital bir kaynak olarak kullanılabilir.

5. Sunum ve Yansıtma: Her grup kendi infografik bölümünü sunarak tasarım ve içerikte yaptıkları seçimleri açıklar. Sınıf olarak bu stratejilerin dijital etkileşimleri nasıl geliştirebileceğini tartışınız ve görsel araçların anlayış ve farkındalığı teşvik etmedeki değeri üzerine düşününüz.

Değerlendirme:

Grup İnfografiği Dereceli Puanlama Anahtarı:

- **İçerik Doğruluğu (%20):** Bilgiler; doğru, konuyla ilgili ve dijital iletişimde en iyi uygulamaları net bir şekilde sunuyor.
- **Tasarım ve Görsel Çekicilik (%20):** Infografik; renk, simge ve boşlukların dengeli kullanımı ile görsel olarak ilgi çekicidir.
- **Açıklık ve Okunabilirlik (%20):** Metin; özlü ve anlaşılması kolay, mantıksal akışı anlamayı kolaylaştırıyor.

- **Yaratıcılık (%20):** Grup, görsel tasarımlarında özgünlük sergiliyor ve infografiği akılda kalıcı kılan benzersiz unsurları bir araya getiriyor.
- **İş Birliği (%20):** Grup üyeleri, dengeli katılım ve paylaşılan sorumluluğun kanıtlarını göstererek birlikte etkili bir şekilde çalışmıştır.



Etkinlik

5. Ortak Hikâye Yazımı: “Dijital Dünyada Gezinmek”

Amaç: Katılımcılar; dijital iletişim, çevrim içi etkileşimler ve bunların kişisel ilişkiler üzerindeki etkilerini araştıran, anlatı yoluyla farkındalık ve eleştirel düşünme geliştiren bir hikâyeyi iş birliği içinde yazacaklardır.

Materyaller:

- İnteraktif tahta veya projektör
- Hikâye taslağı şablonları
- Düşünce günlükleri

Genel Bakış: Katılımcılar, dijital iletişim bağlamında iş birliğine dayalı bir hikâye oluşturmak için gruplar hâlinde çalışacaklardır. Her grup hikâyenin farklı bölümlerine katkıda bulunacak ve birlikte hem olumlu hem de olumsuz unsurlar dâhil olmak üzere çevrim içi etkileşimin çeşitli yönlerini vurgulayan bir anlatı oluşturacaklardır. Bu etkinlik yaratıcılığı, ekip çalışmasını ve dijital dünyanın karmaşıklığı üzerine düşünmeyi teşvik etmek için tasarlanmıştır.

Uygulama:

1. Giriş ve Tartışma: Katılımcılara aşağıdaki gibi sorular sorarak dijital iletişim üzerine bir sınıf tartışması ile başlayınız.

- “Çevrim içi iletişim kurmanın faydaları nelerdir?”
- “Çevrim içi iletişimde ne gibi zorluklar yaşadınız veya gözlemlediniz?”
- “Çevrim içi etkileşimler ilişkileri olumlu ya da olumsuz yönde nasıl etkileyebilir?”

Her öğrenci grubunun ortak bir anlatının farklı bölümlerini yazmaktan sorumlu olacağı iş birliğine dayalı bir hikâye fikrini tanıtınız.

2. Hikâye Planlama: Katılımcıları 3-4 kişilik küçük gruplara ayırınız. Sınıf, birlikte dijital iletişimin çeşitli yönlerini deneyimleyen bir grup karakter konseptine dayalı bir hikâye tasarlayacaktır (örneğin; çevrim içi arkadaşlıklar, kısa mesajlardaki yanlış anlamalar, sanal bir iş birliği projesi ve çevrim içi anlaşmazlıklarla başa çıkma). Tahtada hikâyeyi bölümlere ayırarak kaba bir taslak oluşturunuz.

Karakterler, dijital dünyada iletişime geçer ve birbirleriyle tanışarak etkileşimlerini geliştirir. Ancak yanlış anlaşılan bir mesaj veya siber zorbalık gibi bir çatışma ortaya çıkar ve

ilişkilerde gerginlik yaşanır. Olumlu iletişim stratejileri kullanarak bu çatışmayı çözerler ve dijital iletişimde daha bilinçli ve saygılı olmanın önemini kavrarlar. Bu deneyim, onların dijital etkileşimlerinde empati ve sağduyu geliştirmelerine katkı sağlar.

3. Gruplar Hâlinde Hikâye Yazımı: Her gruba ana hatları temel alarak hikâyenin bir bölümünü yazmalarını söyleyiniz. Hikâyeyi özgün kılmak için katılımcıları mesajlaşma, video görüşmeleri veya sosyal medya paylaşımları gibi gerçek hayattaki dijital iletişim yöntemlerini kullanmaya teşvik ediniz. Paylaşılan bir Google Docs veya benzer bir platform kullanarak gruplar kendi bölümleri üzerinde aynı anda çalışabilir, birbirlerinin katkılarını görebilir ve hikâyede süreklilik sağlayabilirler. Katılımcılar; yazarken karakterlerinin her durumda nasıl hissedebileceklerini, nasıl tepki verebileceklerini nasıl iletişim kurabileceklerini düşünmelidir.

4. Hikâye Derleme ve Düzenleme: Her grup kendi bölümünü tamamladıktan sonra, öyküyü tek bir belgede bir araya getiriniz. Sınıf olarak hikâyeyi okuyup akışı, tutarlılığı ve karakter gelişimindeki tutarlılığı kontrol ediniz. Gerekli düzenlemeleri yapın ve katılımcıları hikâyenin sorumlu dijital iletişimle ilgili mesajını iyileştirmek için değişiklikler veya eklemeler önermeye teşvik ediniz.

5. Sınıf Sunumu: Her grup; hikâyenin kendi yazdığı bölümünü sunacak ve karakter eylemleri, diyalog ve çözüm açısından yaptıkları seçimleri açıklayacaktır. Okumanın ardından, hikâyedeki karakterlerin deneyimlerinin gerçek hayattaki durumları nasıl yansıttığı ve öğrendikleri dersleri kendi çevrim içi etkileşimlerine nasıl uygulayabilecekleri üzerine bir sınıf tartışması başlatınız.

6. Yansıtma ve Geri Bildirim: Katılımcılar günlüklerine iş birlikçi öykü yazma deneyiminden neler öğrendiklerine dair kısa bir değerlendirme yazacaklardır. Yönlendirici sorular aşağıdaki örnekleri içerebilir.

- “Karakterlerin çevrim içi etkileşimlerinde sizi şaşırtan ne oldu?”
- “Benzer bir dijital durumda neyi farklı yapardınız?”
- “Bunun gibi hikâyeler kendi dijital iletişimimizi anlamamıza ve geliştirmemize nasıl yardımcı olabilir?”

Değerlendirme:

Hikâye İçeriği: Hikâyenin bütünlüğünü, yaratıcılığını ve dijital iletişim temalarının tasvirini değerlendiriniz.

İş Birliği: Süreç boyunca katılımcıların iş birliği, iletişim ve ekip çalışmasını gözlemleyiniz.

Yansıtma Günlükleri: Öğrenci yansımalarının derinliğini ve hikâyedeki olayları dijital etkileşimlerle ilgili kişisel iç görüşlerle ilişkilendirme becerilerini değerlendiriniz.

KAYNAKÇA

Council of Europe. (2022). Digital citizenship education handbook.

Elnur, A. (2023). İletişim süreçlerinin dijitalleşmesi bağlamında boş zaman sosyolojisinin dönüşümü. Akademik Hassasiyetler, 10(23), 287-311.

Strauss, C., Harr, M. D., & Pieper, T. M. (2024). Analyzing digital communication: a comprehensive literature review. Management Review Quarterly, 1-39.

MODÜL 5

Dijital Ticaret



Modül Kapsamı

Bu modül, dijital ticaret konusunda bilgi ve beceri kazandırmayı hedefleyen bir eğitim programıdır. Modül; dijital ticaret, dijital ticaretin potansiyeli, dijital ticaretin faydaları ve riskleri, dijital tüketiciler konularını kapsar. Çevrim içi platformların büyümesi, yeni teknolojilerin üretilmesi, hizmetlerin üretilmesi, malzemelerin ve hizmetlerin tedarik edilme şekli ve teslimat biçimleri, ticari faaliyetlerin değişimi, yeni zorluklar ve fırsatları ortaya çıkarma durumları günümüzde yapılan ticarete önemlidir.

Öğrenme Kazanımları

- Dijital ticareti kavramsal olarak tanımak.
- Dünyadaki ve ülkemizdeki dijital ticaretin büyüme oranını karşılaştırmak.
- Dijital ticaretin faydaları konusunda bilinç düzeyini arttırmak.
- Dijital ticaretin risklerini fark etmek ve alınacak önlemleri öğrenmek.
- Dijital tüketici kavramını öğrenmek.
- Bilinçli tüketici olmak için yapılması gerekenleri fark etmek.

İçerik Ağacı

1. Dijital Ticaret
2. Dijital Ticaretin Potansiyeli
3. Dijital Ticaretin Faydaları ve Riskleri
4. Dijital Tüketiciler

Dijital Ticaret

4.3. Modülden Beklentiler:

- Bu modülden ne öğrenmeyi bekliyorsunuz?
- Beklentilerinizi bir not kâğıdına yazınız, yönergesi katılımcılara bildirilir ve katılımcılara not kâğıdı verilerek beklentilerini yazmaları istenir.
- Kâğıtlar panoya herkesin göreceği şekilde asılır.

4.4. Tanışma:

Adının Dans Hareketleri

- Katılımcılar bir daire içinde durur.
- İlk katılımcı, adındaki her heceyi bir hareketle ilişkilendirir (el veya bacak hareketleri, adımlar, piruetler, kafa hareketleri vb.).
- Bir sonraki katılımcı, ilk kişinin hareketlerini isim ile tekrarlar ve kendi hareketlerini ekler.
- Grup hareketleri ve isimleri birlikte tekrarlar.
- Oyun son kişiye kadar bu şekilde devam eder.

1. Dijital Ticaret

İletişim teknolojilerinin ve internetin hızlı gelişimiyle birlikte yeni ve farklı bir ekonomik düzen ortaya çıkmıştır. Bu değişikliklerle birlikte coğrafi sınırlar kalkmış, pazarlar farklı bir boyut kazanmış ve satıcılar tüm dünyayı potansiyel müşteri olarak görüp ticari faaliyetlerini web tabanlı sistemlere taşımışlardır (Civan ve Bal, 2002). Dijital ağlar, özellikle ticaret alanına yeni bir boyut kazandırmıştır. Bu ağlar, alıcılar ve satıcıların daha hızlı ve kolay bir şekilde bağlantı kurmasını sağlayarak arama maliyetlerini düşürür. Ayrıca iletişim ve koordinasyon maliyetlerinde de azalma sağlanabilir, bu da nakliye maliyetlerinin düşmesine katkıda bulunur (Abeliansky ve Hilbert, 2017). Dijital ticaret; ürünlerin ve hizmetlerin internet üzerinden alım, satım ve sipariş işlemlerini kapsayan geniş bir alanı ifade eder. Dünya Ticaret Örgütüne göre dijital ticaret; mal ve hizmetlerin elektronik yollarla üretilmesi, dağıtılması, pazarlanması, satılması veya alıcılara teslim edilmesidir. Bu kapsamda; dijital ticaret yalnızca alışveriş işlemlerini değil, aynı zamanda pazarlama, müşteri desteği ve ticari iletişim gibi süreçleri de içerir. Bilgisayar ağları aracılığıyla gerçekleştirilen bu faaliyetler; küresel ölçekte ticaretin daha hızlı, etkili ve kapsamlı bir şekilde yapılmasına olanak tanır (Civan ve Bal, 2002).

1.2. Dijital Ticaretin Kapsamı

İnternet aracılığıyla ticari işlemler (alışveriş) anlamındaki e-ticaretin genel olarak kapsamı kâr amaçlı olsun veya olmasın tüm kuruluşları içine almaktadır. Bu açıdan bakıldığında e-ticaretin genel çerçevesi aşağıdaki şekilde yapılabilir (Elibol ve Kesici, 2004, s. 306).



- Dijital içeriklerin veya fiziksel malların alım ve satımı.
- Herhangi bir aracı kullanmadan ürünlerin tüketiciye pazarlanması.
- Tanıtım, reklam ve bilgilendirme faaliyetleri.
- Ticari kurumlar arası işlemler ve sözleşmeler.
- Satış sonrası destek ve elektronik ortamda ihalelerin yapılması.
- Elektronik banka işlemlerinin yapılması.
- Ortak tasarım ve üretim projeleri.
- Ticari kayıtların tutulması ve izlenmesi.
- Dijital içeriklerin sevkiyatının yapılması.
- Kamu ve özel sektör hizmetlerinin kullanılması.

Ancak, e-ticareti kapsamı yalnızca internet aracılığıyla yapılan alışverişle sınırlı değildir. Genel anlamda; e-ticaret bilgisayar ağları aracılığıyla ürünlerin üretilmesi, satılması, reklamının yapılması, satış sonrası teknik destek sağlanması ve ödemelerin gerçekleştirilmesi gibi faaliyetleri içerir (Kaya, 2002; Akt: Özel, 2013, s. 2). Bucaklı (2007) tarafından e-ticareti kapsamı aşağıdaki şekilde sıralamaktadır:

- Mal ve hizmetlerin dijital alışverişi.
- Üretim planlaması, organizasyonu ve tedarik zinciri oluşturma.
- Tanıtım, reklam ve bilgilendirme faaliyetleri.
- Sipariş oluşturma işlemleri.
- Anlaşmalar yapma süreci.

- Elektronik banka işlemleri ve fon transferleri.
- Elektronik konşimento gönderimi.
- Gümrükleme işlemleri.
- Elektronik ortamda kamu alımları.
- Elektronik posta ile yapılan işlemler.
- Elektronik hisse alışverişi ve borsa işlemleri.
- Ticari kayıtların tutulması ve izlenmesi.
- Doğrudan tüketiciye pazarlama faaliyetleri.
- Dijital imza, elektronik noter gibi işlemler.
- Dijital içeriğin anında dağıtımı.
- Anında bilgi oluşturma ve aktarma.
- Elektronik ortamda vergilendirme.
- Fikri mülkiyet haklarının transferi.
- Dijital ortamda üretim izleme.
- Dijital ortamda sevkiyat izleme.

1.3. Dijital Ticaret Araçları

Genel olarak ticari faaliyetlerde bulunan tarafların işlemlerini kolaylaştıran her türlü teknoloji ve teknoloji ürünü, elektronik ticaret aracı olarak tanımlanabilir. Bu araçlar arasında internet, bilgisayar, tablet, faks, telefon, elektronik veri değişim (EDI) sistemleri ve elektronik ödeme sistemleri yer almaktadır. En yaygın kullanılan e-ticaret araçları ise, elektronik veri değişim sistemleri, internet ağları ve elektronik ödeme sistemleridir (Arpacı ve Uluçay, 2012; Akt: Akçi ve Göv, 2015, s. 415).

1.3. Dijital Ticaret Türleri

E-ticaret; genel olarak doğrudan ve dolaylı e-ticaret olarak iki sınıflamaya tabi tutulmaktadır. Dolaylı e-ticarete; satıcıların ürünlerin reklamını yapması, malların müşteriler tarafından incelenmesi, siparişin oluşturulması elektronik olarak gerçekleştirilir ancak fiziksel teslimat posta hizmeti veya ticari kuryeler aracılığıyla geleneksel yollarla yapılır. Doğrudan e-ticaret ise sipariş, ödeme ve teslimat süreçlerinin tamamen dijital ortamda gerçekleştirildiği bilgisayar programları, eğlence ve kültürel içerikli görsel ve işitsel mal ve hizmetleri kapsar (Özel, 2013, s. 4).

2. Dijital Ticaretin Potansiyeli

Günümüzde Bilgi Çağı olarak adlandırılan dönemde, bilgisayar ve internetin hızla yaygınlaşması ticareti derinden etkilemiş ve geleneksel ticaret anlayışına alternatif ve yenilikçi olarak e-ticaretin ortaya çıkmasına neden olmuştur. Bu bağlamda, e-ticaret küreselleşme süreciyle ilişkilendirilen yeni bir ticaret modeli olarak görülebilir (Özdemir, Törenli ve Kıyan, 2010). E-ticareti geleneksel ticaretten ayıran en önemli yeniliklerinden biri, ticari faaliyetlerin mekân ve zaman

kısıtlamalarını ortadan kaldırarak herhangi bir yer ve zamanda alışveriş yapılabilmesini sağlamasıdır (Akçi ve Gv, 2015, s. 412). Bu sayede geleneksel srelerde yz yze gerekleen mal ve hizmet alım-satım ilemlerini kolaylatıran e-ticaret, zellikle internet teknolojisindeki ilerlemelerle birlikte giderek daha yaygın hle gelmitir (Kayahan ve Hepaktan, 2016, s. 160).



Dijital Ticaretin Byklğ

- Katılımcılar iki gruba ayrılır.
- Birinci grup 2014 ile 2024 yılları arasında dnyadaki dijital ticaretin byklğn dijital aralar kullanarak aratırır, rapor hazırlar ve sunum yapar.
- İkinci grup 2014 ile 2024 yılları arasında Trkiye'deki dijital ticaretin byklğn dijital aralar kullanarak aratırır, rapor hazırlar ve sunum yapar.

2.1. Dnyada Dijital Ticaret

Dijital ticaret, gnmzde dı ticaretin yeni bir trendi olarak ne ıkmakta ve zellikle ABD gibi lkelerde nemli kazanımlar saėlamaktadır. Aratırmalar, internetin 1990'lı yılların sonlarından itibaren dı ticaret zerinde byk etkisi olduėunu gstermektedir (Artan ve Kalaycı, 2009, s. 181). Gnmzde ortaya konan ekonomik veriler, e-ticaret hacminin toplam ticaret hacmi ierisindeki payının gn getike arttıėını ortaya koymaktadır (Yenieri, 2008). E-ticaret hem satıcılara hem de alıcılara zaman ve maliyet tasarrufu saėlamakta ve ayrıca verimlilik artıı gibi avantajlar saėlamaktadır. Bunun yanında, firmalara (kurululara veya iletmelere) kresel lekte (tm dnya kapsamında) i yapabilme olanaėı sunmaktadır (Artan ve Kalaycı, 2009, s. 176). İnternet sayesinde firmalar, daha dk maliyetle ve pazara giri engelleriyle karılamaksızın dnya genelinde faaliyet gsterebilmekte, tketiciler ise aracılara ihtiya duymadan daha eitli mal ve hizmetlere eriim imknı bulmaktadır (zel, 2013, s. 2). İnternet zerinde faaliyet gsteren bir firmanın byklğ ne olursa olsun, artık faaliyet alanı tm dnyadır (Elibol ve Kesici, 2004, s. 204-304).

Dnyada e-ticaret, pandemi srecinin balamasıyla birlikte hızlı bir byme ve gelime srecine girmitir. Kresel e-ticaret hacmi 2022 yılında yaklaşık 5,5 trilyon dolarken, 2023'te %25'ten fazla byyerek yaklaşık 7 trilyon dolara ulamıtır.

2.2. Türkiye’de Dijital Ticaret

Günümüzde Türkiye’de hem kamu hem de özel sektörün internet üzerinden hizmet verme konusunda önemli ilerlemeler kaydettiği görülmektedir. 2005’te %80,4 olan internet erişimine sahip işletme oranı, 2010’da %90,9’a yükselmiştir, bu da girişimcilerin internete hızlı adaptasyon gösterdiğinin bir göstergesidir (Özel, 2013, s. 13-14). Bu durum, e-ticaret hacminin her yıl katlanarak büyüdüğünü işaret etmektedir. Ekonomik birimler için internet, artık bir tercih veya teknolojiye uyum sağlamaktan ziyade bir zorunluluk hâline gelmiştir (Kayahan ve Hepaktan, 2016, s. 185-186). Buna rağmen, Türkiye’de internet kullanımı e-ticareten daha hızlı ilerlemekte ve e-ticaretin henüz Türkiye’de beklenen düzeye ulaşmadığı bilinmektedir. Şu an hâlihazırda Türkiye’de 12.000 civarında e-ticaret sitesi faaliyetine devam etmektedir. E-ticaret hacmi Türkiye’de 2022 yılında 600 milyar Türk lirası iken 2023 yılında 850 milyar Türk lirasını geçmiştir. Küresel e-ticaretin toplam perakende satışlardaki payının %21’i geçtiği ve bu oranın birkaç yıl içerisinde %25’i geçeceği ve gelecek 5-10 yıl içerisinde %50’yi bulabileceği düşünülmektedir (Ticaret Bakanlığı, 2022).

İnternet üzerinden hizmet sunan bankalar sitelerini her geçen gün geliştirerek bu alanda öncülük yapmaktadır (Küçükyılmazlar, 2006, s. 35-37). Bununla birlikte; e-ticaretin Türkiye’de gelişmesinde kitapçılar, CD satıcıları, elektronik ve bilgisayar parçaları satıcıları ile oyuncakçılar da öncü rol oynamaktadır. E-ticaret sayesinde gelişim gösteren bir dijital alan ise firmaların bilet alım satımıdır. Günümüzde, çeşitli amaçlarla kullanılan bilet alım satım işlemlerinin %70’inden fazlası sanal ortamda gerçekleştirilmektedir (Arslandere, 2010, s. 53-54). Türkiye’de, telekomünikasyon yapısının e-ticaret çerçevesinde yeniden yapılandırılmasına yönelik yasal altyapının güçlendirilmesiyle e-ticaretin daha da genişleyeceği öngörülmektedir. E-ticaret konusunda yapılan ilk kapsamlı çalışma, 1998 yılında Elektronik Ticaret Koordinasyon Kurulu’nun (ETTK) oluşturulmasıdır. Daha sonra bu kurul, e-Ticaret Kurulu (ETİK) olarak adlandırılmıştır. 2003 yılında Dış Ticarete e-Belge ile e-Finansal Hizmetler grubu kurulmuş ve “İnternet Üst Kurul” da bu kapsamda sayılabilir (Küçükyılmazlar, 2006, s. 35-37).

Deloitte raporuna göre 2014 – 2019 yılları arasında dünya çapındaki perakende e-ticaret satış rakamları şöyledir:

- 2014 yılında 1.336 trilyon dolar,
- 2015 yılında 1.548 trilyon dolar,
- 2016 yılında 1.845 trilyon dolar,
- 2017 yılında 2.382 trilyon dolar,
- 2018 yılında 2.982 trilyon dolar,
- 2019 yılında 3.535 trilyon dolar,



Sembolünü Seç

- Katılımcılara internet üzerinden ticaret yapan bir satıcı oldukları söylenir. Satışlarını arttırmak için bilgisayar üzerinde firmalarının sembollerini oluşturmaları istenir. Semboller grupla tartışılır.

- 1.Semboller firmaların değerlerini temsil ediyor mu?
- 2.Müşteride alışveriş yapma duygusu oluşturuyor mu?
3. Güven veriyor mu?
4. Firmanın satışını yaptığı ürün/hizmet hakkında bilgi veriyor mu?

3. Dijital Ticaretin Faydaları ve Riskleri





Tartışma Programı

- Katılımcılar iki gruba ayrılır.
- Televizyonda tartışma programına davet edildikleri söylenir.
- Gruplara konular verilir.
- Birinci grup dijital ticaretin/alışverişin faydalarını savunuyor.
- İkinci grup dijital ticaretin/alışverişin risklerini ve geleneksel ticareti/alışverişi savunuyor.
- Grupların hazırlanması için 5 dk. verilir.
- Gönüllü bir katılımcı tartışma programının sunuculuğunu üstlenir.

3.1. Dijital Ticaretin Faydaları

İnternet sayesinde tüketiciler, yılın her günü ve günün yirmi dört saati alışveriş yapabilme olanağına sahip olurlar. Ayrıca daha düşük fiyatlarla mal ve hizmet satın alma, yazılım gibi dijital ürünlere daha kolay erişme ve dünya çapında kendi aralarında takas yapabilme imkânına kavuşurlar. Tüketiciler açısından e-ticaretin yararları aşağıdaki şekilde sıralanabilir (Doğaner, 2007, s. 35-36)

- Evden çıkmadan ürünleri görme, inceleme alışveriş yapma imkânı sunar.
- Ulaşım masraflarını azaltır.
- Ürün çeşitliliğini daha rahat görme olanağı sağlar.
- Çevrim içi perakendecilikte, etkili ürün sunumu web sayfasının çekiciliğini artırarak tüketicilerin karar verme süreçlerini kolaylaştırır (Yoo ve Kim, 2014; Algharabat, 2014; Ozok ve Komlodi, 2009; Algharabat vd., 2017).

Ürünler hakkında bilgi edinme sürecinde ürünleri 360° görüntüleme imkânı ve sanal deneme yapma gibi uygulamaların tüketicilerin satın alma kararları üzerinde önemli bir etkisi bulunmaktadır (Markopoulos vd., 2006; Beck ve Cri , 2016).

3.3. Dijital Ticaretin Riskleri

- Kimlik Hırsızlığı

Bu durum genellikle siber suçluların e-ticaret web sitelerine sızarak kullanıcıların oturum açmalarını veya kredi kartı bilgilerini çalmalarını içerir. Böylece, siber suçlular kullanıcıların kimliklerini kullanarak dolandırıcılık amaçlı satın almalar yapabilir veya kişisel bilgilerini çevrim içi olarak diğer suçlulara satabilirler.

- Sahte Çevrim İçi Mağazalar

Tüm e-ticaret siteleri güvenilir değildir. Dolandırıcılar, gerçek satıcılar gibi görünmek için sahte web siteleri oluşturabilirler. Tasarım ve düzeni kopyalayıp logoları çalarak kullanıcıları güvenilir bir sitede olduklarına inandırırılar. Popüler giyim markalarını, mücevherleri ve elektronik ürünleri düşük fiyatlarla sunarak dikkat çekerler. Bazen kullanıcıların parasını ödeyip satın aldıkları ürünler ellerine ulaşır. Bazı zamanlarda ise kullanıcıların satın aldıkları ürünler hiçbir şekilde ellerine ulaşmaz.

- Şifrelenmemiş Veriler

Bazı web siteleri verileri şifrelemez. Güncel ve korunaklı bir SSL sertifikasına sahip olmayan saldırılara karşı daha savunmasız olurlar. URL'si HTTPS yerine HTTP ile başlayan web siteleri güvenli değildir; bu durum, kredi kartı bilgileri ve diğer hassas bilgileri bu sitelerle paylaşarak alışveriş yapanlar için risk oluşturur.

- Veri İhlalleri

Çevrim içi alışveriş yaptığınızda banka veya kredi kartı bilgileri, iletişim ve adres bilgileri gibi özel verileri satıcılarla paylaşmış olursunuz. Eğer bilgisayar korsanları bir e-ticaret web sitesine yetkisiz erişim sağlarsa, bir veri ihlâli durumunda bu bilgilerinizin açığa çıkma riski bulunmaktadır.

- Sahte Yorumlar

Çevrim içi alışveriş yapan birçok kişi, ürünü satın almadan önce yorumları inceler. Ancak, tüm çevrim içi yorumların gerçek olmayabileceğini unutmayın. Belirli bir satıcı için gerçek olamayacak kadar iyi görünen veya yeterince ayrıntı içermeyen incelemeler varsa, kaynağı kontrol etmeye ve içgüdülerinize güvenmeye özen gösterin.

- Sahte Uygulamalar

Gerçek çevrim içi satıcıların çoğu, özel uygulamalara sahiptir. Ancak siber suçlular, bu uygulamaların sahte sürümlerini oluşturarak kullanıcıları kandırmaya çalışabilirler. Amaçları, banka veya kredi kartı bilgileri ile kullanıcı adları ve parolaları gibi kişisel bilgileri ele geçirmektir.

- Güvenli Olmayan Wi-Fi

Halka açık yerlerde güvenli olmayan kablosuz internet ağları, ciddi güvenlik riskleri taşıyabilir. Bu risklerden biri, bilgisayar korsanlarının siz ve bağlantı noktası arasında konumlanarak veri aktarımını izleyebilmesidir. Güvenli olmayan bir Wi-Fi ağı üzerinden çevrim içi alışveriş yaptığınızda, bilgisayar korsanları kredi kartı bilgileri ve iletişim bilgileri gibi kişisel verilerinize erişim sağlayabilirler.

- Reklam Yazılımları

Reklam yazılımları, internette gezinirken ekranda beliren istenmeyen reklamlardır. Adware, “reklam yazılımı”nın kısaltmasıdır ve genellikle sahibine gelir sağlamak amacıyla kullanılır. Bu yazılımlar meşru olabilir ancak siber suçlular tarafından da kötü niyetle kullanılabilirler. Örneğin, sizi kişisel bilgilerinizi ele geçirmeye çalışan zararlı web sitelerine yönlendirebilirler. Hatta bazen, açılır pencere reklamını kapatmak için “X” sembolüne tıklamak bile sorun yaratabilir.

- Kimlik Avı Saldırıları

Bu, gerçek bir satıcıdan geliyormuş gibi görünen sahte e-postalar gönderen dolandırıcıları içerir. E-postalar, genellikle alıcıyı tıklamaya ikna etmek için tasarlanmış ekler veya bağlantılar içerir ve bu bağlantıların tıklanması durumunda kötü amaçlı yazılım bulaşmasına yol açabilir.



Nasıl Bir Tüketiciyim?

Bu aktiviteye katılımcılar oturur pozisyondayken başlanır. Katılımcıların takip etmesi istenen talimatlar verilir:

- Sık alışveriş yapıyorsan, ayağa kalk.
- Süpermarketlerden alışveriş yapıyorsan otur.
- İnternette sipariş veriyorsan, ayağa kalk.
- İnternette satış yapıyorsan, otur.
- İnternetteki ticareti kolay buluyorsan ayağa kalk.
- Reklam pazarından etkileniyorsan otur.
- İnternette siparişlerinde kandırıldıysan, ayağa kalk.



Alışveriş Potansiyelim

Katılımcılar dört gruba ayrılır. Gruplardan; yiyecek, giyim, tatil, beyaz eşya, araba vb. konulardan birini seçip dijital ortamda tüketiciler için reklam afişi tasarlamaları istenir. Katılımcılar afişleri inceler ve alışveriş isteğini arttıran afişi seçerler. Katılımcıların alışveriş yapma isteklerini arttıran etmenler hakkında tartışılır.

- Afişte ne görüyorsun?
- Afiş ne içeriyor?
- Afişte hangi detay senin için en önemlidir? Neden?
- Neden alışveriş yapmayı düşünüyorsun?
- Bu alışveriş yaptıktan sonra bunun hangi ihtiyacını gidereceğini düşünüyorsun?
- Afişte ne eksik?
- Afişe ne eklemek istersin?
- Bu görüntüyü beğendin mi beğenmedin mi? Neden?
- Bu afiş sende hangi duyguları, hisleri, hatıraları uyandırıyor?

4. Dijital Tüketiciler

Teknolojinin ilerlemesiyle birlikte mobil cihazlar ve internet kullanımının artması, insanların yaşam biçimlerini ve alışveriş alışkanlıklarını dönüştürmüştür (Ryan, 2016). Bu önemli ve olumlu gelişmeler, işletmelerin dijital medya ve benzeri yeni kanallar aracılığıyla hedef kitleleriyle iletişim kurmasını sağlamaktadır. Tüketicilerin bu değişimlere olumlu yanıt vermesiyle dijital pazarlamanın kullanımı artmış ve bu pazarlama biçimi işletmeler için kritik bir önem kazanmıştır. Artık işletmelerin karşısında “dijital tüketiciler” bulunmaktadır ve bu yeni nesil tüketicilerin ihtiyaçlarını, alışkanlıklarını ve davranışlarını anlamak büyük önem taşımaktadır. Ancak, bu sürecin zorluklarla dolu olduğu da göz ardı edilmemelidir (Alan, Kabadayı ve Erişke, 2018; 493).

E-tüketicilerin internetten alışveriş yapma nedenleri:

- Hızlı erişim
- Evden, işten kazanma
- Prestij kazanma
- Konfor
- Çevrim içi olma

İnternette alışveriş yapılırken dikkat edilecek hususlar:

- 3D secure sistemi olan siteleri tercih edin.
- Satıcı güvenliğine dikkat edin: Sanal POS kullanmalı.
- SSL sertifikasını mutlaka kontrol edin.
- Sanal kart ile alışveriş yapın.
- Güvenli şifreler belirleyin.
- Çok ucuz fiyatlara dikkat edin.
- Ödemeyi mutlaka kendi bilgisayarınızdan yapın.
- Sitenin adres ve telefonunu kontrol edin.



Etkinlik:

Bilinçli Tüketici

- Katılımcılardan üç farklı gönüllü grup oluşturulur.
- Gönüllü katılımcılar arasında durum kartları kullanılarak canlandırma süreci paylaştırılır.
- Birinci grup durum kartı: Bir genç, ailesinden bilgisayarını yenileyeceği için destek ister. Ailesi de kredi kartı bilgilerini ve şifreyi verir. Ailesi gence; siteleri incelemesini, ucuz fiyatlara dikkat etmesini, sitelerin adres ve telefonlarını kontrol etmesini hatırlatır. Genç, iş yerinin bilgisayarından ailesinin kredi kartı bilgilerini girerek alışveriş yapar. Birkaç gün sonra gencin eline bilgisayar yerine saç kurutma makinesi, babasının kredi kartına da bir sürü borç gelir... Bundan sonraki gelişmeler grup tarafından canlandırılır. Grubun sunumu için birkaç dakika hazırlık fırsatı verilir. Canlandırma sonrası internetten alışveriş yapılırken nelere dikkat edileceği hakkında katılımcılarla birlikte dijital araçlar aracılığı ile bilinçli tüketici yönergesi yazılır.
- İkinci grup durum kartı: Adam, karısını tatile götürmek için sanal ortamda rezervasyon yaptırır ve ödemeyi gerçekleştirir. Eşinin sürprizi kadını mutlu eder. Tatil için otele gittiklerinde böyle bir rezervasyonun ve otelin olmadığını görürler... Bundan sonraki gelişmeler grup tarafından canlandırılır. İkinci grubun canlandırması sonrası dijital ortamda yaşanmış olumsuz alışveriş deneyimleri ilgili haberler araştırılır, paylaşılır ve nedenleri hakkında tartışılır.
- Üçüncü grup durum kartı: Bir kadın, kolay ulaşılabilir olması nedeni ile internetten ihtiyacı olsun olmasın sürekli alışveriş yapar. Kadın bilinçsiz bir tüketici, kocası durumdan çok muzdarip ve evin ekonomisi zor durumda... Bundan sonraki gelişmeler grup tarafından canlandırılır. Üçüncü grubun canlandırması sonrası bilinçli tüketici olma konusunda internet sitesine girerek her katılımcı kendi karbon ayak izi ölçer.

Sürdürülebilirliği Düşünen Tüketiciler İçin Öneriler

Katılımcılar üç gruba ayrılır; gıda, giyim ve eşya konularından birini seçip internetten araştırma yaparak sürdürülebilirliği olan uygulamaların listesini çıkarıp gruba sunum yaparlar.



Alışveriş Kimliğim

1. Alışveriş yapmayı sevenler?
1.....
2.....
3.....
4.....
2. Yüz yüze alışveriş yapanlar?
1.....
2.....
3.....
4.....
3. İnternette alışveriş yapanlar?
1.....
2.....
3.....
4.....
4. İhtiyaca göre alışveriş yapanlar?
1.....
2.....
3.....
4.....
5. İhtiyaç dışında alışveriş yapanlar?
1.....
2.....
3.....
4.....
6. Fiyata dikkat edenler
1.....
2.....
3.....
4.....

Katılımcılara “Alışveriş Kimliğim” kâğıtları ve kalem verilir. Katılımcıların on dakika içinde “Alışveriş Kimliğim” kâğıtlarında bulunan soruları birbirlerini sormaları, verilen cevapları yazmaları istenir. Her sorunun altındaki cevaba dört tane katılımcı ismini ilk yazan oyunu kazanır. Katılımcılarla çember oluşturulur ve sorular ekiple tartışılır (Örneğin; ihtiyaca göre alışveriş yapanların bunu nasıl başardığı, neden internette alışveriş yaptığı vb.).

Modülden Öğrendiklerim/Bulduklarım

- Bu modülden ne öğrendiniz ne buldunuz?
- Öğrendiklerinizi ve bulduklarınızı bir not kâğıdına yazınız, yönergesi katılımcılara söylenir.
- Katılımcılara not kâğıdı verilerek yazmaları istenir.
- Kâğıtlar panoya herkesin göreceği şekilde asılır.
- Modülün başında katılımcılar tarafından yazılan beklentiler ile modül sonunda katılımcıların öğrendikleri/buldukları karşılaştırılır.

KAYNAKÇA

- Abeliansky, A. L. ve Hilbert, M. (2017). Digital technology and international trade: Is it the quantity of subscriptions or the quality of data speed that matters? *Telecommunications Policy* (41), 35-48.
- Akçi, Y. ve Göv, S. A. (2015). "Tüketicilerin E-Ticaret Algılarının İncelenmesi (Gaziantep ve Adıyaman Örneği)". *Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 7(13), 412-415.
- Alan, A. K., Kabadayı E. T. ve Erişke, T. (2018). İletişimin Yeni Yüzü: Dijital Pazarlama ve Sosyal Medya Pazarlaması, *Electronic Journal of Social Sciences*, 17(66).
- Algharabat, Raed S. (2014). "Conceptualising and modelling virtual product experience for online retailers". *International Journal of Internet Marketing and Advertising*, 8(4), 300-319.
- Algharabat, Raed, Ali Abdallah Alalwan, Niripendra P. Rana ve Yogesh K. Dwivedi (2017). "Three-dimensional product presentation quality antecedents and their consequences for online retailers: The moderating role of virtual product experience". *Journal of Retailing and Consumer Services*, 36 (Mayıs), 203-217
- Arslandere, M. (2010). Elektronik Ticaret ve Karaman'daki Kobi'ler Üzerine Bir Araştırma. (Yayımlanmamış Yüksek Lisans Tezi), Karamanoğlu Mehmet Bey Üniversitesi Sosyal Bilimler Enstitüsü.
- Artan, S. ve Kalaycı, C. (2009). "İnternetin Uluslararası Ticaret Üzerindeki Etkileri: OECD Ülkeleri Örneği". *Doğuş Üniversitesi Dergisi*, 10 (2), 176-181.
- Beck, Marie, ve Dominique Crié. (2016). "I virtually try it... I want it! Virtual Fitting Room: A tool to increase on-line and off-line exploratory behavior, patronage and purchase intentions". *Journal of Retailing and Consumer Services*, 40(Ocak), 279- 286.
- Bucaklı, A. T. (2007). Elektronik Ticaret. (Yayımlanmamış Yüksek Lisans Tezi), İstanbul: Kadir Has Üniversitesi Sosyal Bilimler Enstitüsü İşletme Bölümü.
- Civan, M. ve BAL, V. (2002). "E-Ticaret ve KOBİ'lerin Geleceği", Kocaeli Üniversitesi İİBF İktisat ve İşletme Bölümü, I. Ulusal Bilgi, Ekonomi ve Yönetim Kongresi / Bildiriler Kitabı, 1011 Mayıs 2002 Hereke- Kocaeli.
- Doğaner, M. (2007). Elektronik ticaret Türkiye'de elektronik ticaretin gelişimi ve işletmeden tüketiciye elektronik ticaret üzerine bir araştırma, Selçuk Üniversitesi, Yayınlanmamış Yüksek Lisans Tezi, Sosyal Bilimler Enstitüsü, Konya.
- Elibol, H. ve Kesici, B. (2004). "Çağdaş işletmecilik açısından elektronik ticaret". *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 11, 304-329.
- Kayahan, L. ve Hepaktan, C. E. (2016). "Türkiye'de elektronik ticaret hacmini etkileyen faktörlere ilişkin var analizi". *Ardahan Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 4, 159-190.
- Küçükylmazlar, A. (2006). Elektronik Ticaret Rehberi. İstanbul: İstanbul Ticaret Odası Yayınları, Yayın no: 2006-3.
- Markopoulos, Panos M., Ravi Aron ve Lyle H. Ungar (2016). "Product information websites: are they good for consumers?". *Journal of Management Information Systems*, 33(3), 624-651.
- Özdemir, F.B., Törenli, N. ve Kıyan, Z. (2010). "Türkiye-Avrupa birliği dış ticaret ilişkileri açısından e-ticaret modeli ve düzenleyici rejim-yapı". *Ankara Avrupa Çalışmaları Dergisi*, 9 (2), 117-143.

Özel, H. A. (2013). "E-ticaret ve Türkiye'nin Bilgi Toplumundaki Yeri". Akademik Bakış Dergisi, 38, 1-14.

Ryan, D. (2016). Understanding digital marketing: marketing strategies for engaging the digital generation. Kogan Page Publishers.

Ticaret Bakanlığı. (2022). 2022 yılı E-Ticaret bülteni.

<https://www.eticaret.gov.tr/dnnqthgzvawtdxraybsaacxtymawm/content/FileManager/Dosyalar/2022%20Yılı%20E-Ticaret%20Bülteni%20v2.pdf>

Yeniçeri, T. (2008). "KOBİ'lerin elektronik ticareti kullanma eğilimi üzerinde etkili olan faktörlerin yapısal eşitlik modeli ile incelenmesi". Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 31, 145-163.

Yoo, Jungmin, ve Minjeong Kim (2014). "The effects of online product presentation on consumer responses: A mental imagery perspective". Journal of Business Research, 67(11), 2464-2472.

MODÜL 6

Dijital Güvenlik



Modül Kapsamı

Bu modül, dijital güvenlik konusunda eğitimcilerle bilgi ve beceri kazandırmayı hedefleyen bir eğitim programıdır. Dijital dünyada kişisel veri güvenliği, özellikle sosyal ağlarda güvenli kullanım bireylerin ve kurumların karşılaştığı en kritik konulardan biridir. Eğitimcilerin dijital güvenlik konusunda bilinçli olması bu bilgileri öğrencilere aktarmada büyük bir öneme sahiptir. Bu modül; kişisel veri koruma, güvenlik önlemleri, sosyal medya kullanımı ve dijital tehditlerle mücadele konularını kapsar. Dijital güvenlik hem akademik çalışmalarda hem de günlük yaşamda karşılaşılan dijital tehditlerin artmasıyla daha da önemli hâle gelmiştir.

Öğrenme Kazanımları

- Kişisel verilerin ne olduğu ve nasıl korunması gerektiği konusunda farkındalık kazandırmak.
- Kişisel verilerin hangi yöntemlerle elde edilebileceğini ve bu verilerin korunması için alınacak önlemleri öğretmek.
- Sosyal ağ uygulamalarında güvenli kullanım yöntemlerini öğretmek.
- Dijital dünyada karşılaşılan tehditlere karşı bireylerin bilinçli ve güvenli davranışlar sergilemelerini sağlamak.

İçerik Ağacı

Dijital Güvenlik

- Kişisel Veri Nedir?
 - Dijital Ayak İzimi Takip Ediyorum
- Kişisel Verileri Elde Etme Yöntemleri
 - Veri Avcıları
- Kişisel Verilerin Korunmasında Alınabilecek Önlemler
 - Siber Güvenlik Simülasyonu
- Sosyal Ağ Uygulamalarında Güvenlik
 - Güvenli Sosyal Medya Profili Oluşturma

Dijital Güvenlik

1. Kişisel Veri Nedir?

Kişisel veri, bir bireyi doğrudan ya da dolaylı olarak tanımlayabilecek her türlü bilgiyi ifade eder. Bu kapsamda ad-soyad, T.C. kimlik numarası, e-posta adresi, IP adresi gibi bilgiler kişisel veri olarak kabul edilir. Kişisel verilerin korunması, dijital çağda bireysel mahremiyetin korunmasının temel taşlarından biridir. Kişisel verilerin korunması üzerine yapılan çalışmalar, verilerin kontrol edilmesinin ve üçüncü şahıslarla paylaşılmadan önce onay alınmasının önemini vurgulamaktadır. Özkaya ve Toprak (2022) tarafından yapılan çalışmada, Türkiye’de güvenlik faaliyetleri kapsamında kişisel verilerin işlenmesi incelenmiştir. Araştırmacılar, özellikle kişisel verilerin hukuki boyutunu derinlemesine analiz etmişlerdir. Çalışmada, kişisel verilerin işlenmesi sürecinde yaşanan sorunlar ve bu sorunlara çözüm önerileri sunulmuştur. Kişisel veri güvenliği konusunda yapılan farkındalık çalışmaları artırılmalıdır. Türkiye’de yaşanan çeşitli veri ihlalleri ve KVKK’nin (Kişisel Verilerin Korunması Kanunu) gündeme gelmesi, bireylerin kişisel verilerinin korunması konusundaki farkındalığını artırmıştır. Özellikle bankacılık ve telekom sektörlerinde yaşanan veri sızıntıları, bu konudaki hassasiyetleri artırmıştır.





1.1. Dijital Ayak İzimi Takip Ediyorum

1. Kişisel Veri Tarama: Katılımcılar kendi isimlerini veya kullanıcı adlarını Google’da aratarak dijital ortamda kendileri hakkında hangi bilgilere ulaşılabildiğini keşfederler. Her öğretmen, bulgularını grubuyla paylaşır.

2. Grup Çalışması: Öğretmenler 3-4 kişilik gruplara ayrılır. Her grup, internet üzerinde yaygın kullanılan bir sosyal medya platformu (Facebook, Instagram, LinkedIn gibi) hakkında araştırma yapar ve bu platformların kullanıcılardan hangi kişisel verileri topladığını belirler. Elde ettikleri verileri kâğıda veya dijital bir not aracına kaydederler.

3. Tartışma ve Sonuç: Her iki etkinlik sonucunda ulaşılan bilgilerin güvenli olup olmadığı, bu bilgilerin dijital güvenlik açısından nasıl bir risk oluşturabileceği tartışılır. Son olarak, kişisel veri paylaşımı konusunda alınması gereken önlemler konuşulur ve eğitmen tartışmaya rehberlik eder.

2. Kişisel Verileri Elde Etme Yöntemleri

Kişisel veriler, dijital dünyada farklı yöntemlerle elde edilebilir. İnternet siteleri üzerinden yapılan alışverişler, sosyal medya paylaşımları, çevrim içi anketler ve çerez (cookie) kullanımı gibi dijital izler, kötü niyetli kişiler tarafından izinsiz toplanabilir. Kimlik avı (phishing) ve sosyal mühendislik gibi dolandırıcılık yöntemleriyle de bireylerin bilinçsizce kişisel bilgilerini paylaşması sağlanabilir.

Dijital olmayan yöntemler de veri elde etmek için kullanılır. Örneğin, kişisel/kurumsal çöplerin karıştırılması (dumpster diving) veya mobil cihazların fiziksel olarak ele geçirilmesi yoluyla kişisel bilgilere erişilebilir. Kamuya açık Wi-Fi ağları da şifrelenmemiş verilerin çalınmasını kolaylaştırdığı için risklidir.

Dijital dünyada kötü amaçlı yazılımlar (malware), casus yazılımlar (spyware) ve keylogger kullanılarak cihazlardaki veriler izinsiz toplanabilir. Sosyal medya platformları; özellikle güvenlik ayarlarının zayıf olduğu durumlarda büyük risk taşır, çünkü kişisel bilgiler kolayca toplanabilir ve izinsiz kullanılabilir. Altıntaş ve Barkuş (2023), dijital gelişmelerin yoğun olarak yaşandığı ve yaşanmaya devam edeceği bu dönemde kişisel verilerimizin güvenliğinin her geçen gün daha da önemli hâle geldiğini ifade eder. Bu nedenle dijital ortamlarda kişisel veri güvenliğini tehdit eden ve güvenliği korumak için alınan önlemlere yönelik farkındalığa sahip olunması büyük önem taşımaktadır.



2.1. Veri Avcıları

Senaryo Tabanlı Oyun: Katılımcılar iki gruba ayrılır:

Grup 1: “Veri Avcıları” rolünü üstlenir. Onlara, kurgusal sosyal medya platformu veya e-ticaret sitesi gibi çeşitli çevrim içi araçlarla insanların kişisel verilerini toplama görevi verilir. Bunun için uygulamalarda izin isteme ekranları, cazip kampanya teklifleri veya çevrim içi testler hazırlayarak kullanıcıları veri paylaşmaya ikna etmeye çalışırlar.

Grup 2: “Veri Koruyucuları” olarak, kişisel bilgilerini kısıtlı şekilde paylaşarak grup1 tarafından oluşturulan çevrim içi senaryolardan geçmeye çalışırlar.

Değerlendirme ve Geri Bildirim: Etkinlik tamamlandıktan sonra her iki grup da deneyimlerini paylaşır. Veri avcıları; hangi yöntemlerin daha etkili olduğunu anlatır, veri koruyucuları ise hangi noktalarda zorlandıklarını ve veri sızdırma tuzaklarına nasıl düştüklerini düştüklerini paylaşırlar. Eğitmen, bu süreçte hangi veri toplama yöntemlerinin yaygın olduğunu ve buna karşı hangi stratejilerin kullanılabileceğini vurgular.

3. Kişisel Verilerin Korunmasında Alınabilecek Önlemler

Kişisel verilerin korunmasında birkaç temel önlem alınabilir: (National Cyber Security Centre, 2024)

- Güçlü ve benzersiz şifreler kullanmak (Örneğin Eskişehir_83 yerine €5k1\$eH1r_BE).
- İki faktörlü kimlik doğrulama (2FA) kullanarak hesap güvenliğini artırmak. Bir hesabın güvenliğini artırmak için ek bir doğrulama yöntemiyle kimlik doğrulaması yapılmasını sağlar. Örneğin bir e-posta hesabına giriş yaparken önce şifrenizi girersiniz (ilk faktör). Ardından, telefonunuza bir SMS veya bildirim ile gönderilen tek kullanımlık doğrulama kodunu girmeniz istenir (ikinci faktör). Bu iki aşamalı süreç, sadece şifreyi bilen birinin değil aynı zamanda telefonunuza da erişimi olan birinin hesaba girebilmesini sağlar, böylece hesabınız daha güvenli hâle gelir.
- Tanınmayan veya güvensiz kaynaklardan gelen e-postalara ya da dosyalara dikkat etmek.
- Düzenli olarak yazılım ve işletim sistemi güncellemelerini yapmak.
- Çevrim içi platformlarda kişisel bilgilerin paylaşılmasını sınırlandırmak.

3.1. Siber Güvenlik Simülasyonu

Uygulama

- Katılımcılar, küçük gruplara ayrılır ve her grup için farklı bir senaryo verilir. Senaryolarda, bir veri ihlâli veya siber saldırı tehdidi ile karşı karşıya kalan birey ya da kurumun durumu anlatılır. Örneğin:
 - Grup 1: Bir sosyal medya hesabının ele geçirilmesi.
 - Grup 2: E-posta kimlik avı (phishing) saldırısı.
 - Grup 3: Bir uygulamanın izinsiz veri toplaması.
- Her grup, senaryodaki güvenlik açığını tespit etmeli ve verilen bilgileri kullanarak bu duruma karşı hangi önlemleri almaları gerektiğini tartışmalı ve bir çözüm planı oluşturmalıdır.

Sunum ve Tartışma: Her grup, senaryosunu ve geliştirdikleri çözüm planını diğer gruplara sunar. Diğer katılımcılar da çözüm önerileri üzerinde geri bildirimde bulunur ve konu birlikte tartışılır. Eğitimci, bu süreçte her çözümün doğruluğunu değerlendirir ve ek bilgiler sunar.

1.4. Sosyal Ağ Uygulamalarında Güvenlik

Sosyal medya platformları, kullanıcıların büyük bir kısmının kişisel bilgilerini paylaştığı alanlardır. Kullanıcıların farkında olmadan çok fazla bilgi paylaşması, kötü niyetli kişilerin bu bilgileri kullanarak kimlik avı saldırıları düzenlemesine veya hesap ele geçirme gibi güvenlik ihlâllerine yol açabilir. Paylaşılan kişisel bilgilerin platformlar tarafından üçüncü şahıslara veya reklamcılara izinsiz bir şekilde aktarılması, kullanıcıların mahremiyetinin ihlâl edilmesine neden olabilir. Bu platformlarda güvenlik açığı yaşamamak için şu önlemler alınabilir:



- Profil bilgilerini sadece tanıdığınız kişilerle paylaşmak.
- Güvenlik ayarlarını düzenleyerek kimlerin bilgilerinize erişebileceğini sınırlandırmak.
- Şüpheli bağlantılara tıklamamak ve tanınmayan kişilerden gelen mesajlara dikkat etmek.
- Sosyal medya hesaplarının şifrelerini düzenli aralıklarla değiştirmek.

Ceyhan ve Demiryürek (2015), Türkiye’de sosyal medya kullanıcılarının kişisel verilerini nasıl paylaştıklarını ve bu paylaşım sırasında ne tür güvenlik önlemleri aldıklarını incelemiştir. Araştırma, kullanıcıların büyük bir kısmının gizlilik ayarlarına dikkat etmediğini ortaya koymuştur. Son yıllarda Türkiye’deki bazı ünlü isimlerin sosyal medya hesaplarının hacklenmesi, bu platformlarda güvenlik önlemlerinin artırılması gerektiğini gözler önüne sermiştir. “The Social Dilemma” belgeseli, sosyal medyanın kişisel veri güvenliği üzerindeki etkilerini sorgulayan önemli bir yapım olarak dikkat çekmiştir.



3.2. Güvenli Sosyal Medya Profili Oluşturma

Profil Analizi ve Güvenlik Ayarları:

- a. Katılımcılar, ellerindeki mevcut sosyal medya hesaplarından (Facebook, Instagram, Twitter gibi) birini seçer.
- b. Eğitimci eşliğinde, katılımcılar seçtikleri platformun güvenlik ayarlarını gözden geçirir ve düzenler. Hangi bilgilerin herkese açık, hangi bilgilerin sadece arkadaşlarına ya da kendilerine görünür olduğunu kontrol ederler. Eğitimci, bu süreçte kritik noktalara dikkat çeker.
- c. Sosyal medya hesaplarına yönelik güvenlik açıklarını kapatmak için şifre güçlendirme, iki faktörlü kimlik doğrulama ekleme, sosyal medya uygulama izinlerini gözden geçirme gibi ek güvenlik önlemleri uygulamalı olarak gösterilir.

Grup Çalışması: Sosyal Mühendislik Simülasyonu:

- a. Katılımcılar 4-5 kişilik gruplara ayrılır. Her grup, sosyal mühendislik temelli bir senaryo üzerinde çalışır. Örneğin:
 - i. Bir arkadaşın hacklenmiş hesabından gelen şüpheli bir mesaj.
 - ii. Kimlik avı (phishing) içeren bir e-posta ya da DM (direkt mesaj).
- b. Gruplar, bu tür saldırılara karşı hangi güvenlik önlemlerinin alınması gerektiğini belirler ve bir çözüm stratejisi oluşturur.

Sunum ve Değerlendirme: Her grup, karşılaştıkları senaryoya karşı geliştirdikleri çözüm önerilerini diğer gruplarla paylaşır. Eğitimci, bu önerileri değerlendirir ve daha güvenli sosyal medya kullanımı için önerilerde bulunur.

5. EKLER

6. “Siber Güvenlik Simülasyonu” Etkinliği Senaryo Örnekleri

6.1. Grup 1: Sosyal Medya Hesabının Ele Geçirilmesi

Bir öğretmenin sosyal medya hesabı ele geçirilmiş ve hesabından izinsiz olarak uygunsuz

içerikler paylaşılmaya başlanmıştır. Hesap sahibi, bu durumun farkına varmış ancak hesabına giriş yapamamaktadır. Öğretmen, hesabı kurtarmak ve bu tür bir durumu tekrar yaşamamak için hangi adımları atmalıdır?

6.2.Çözüm Önerileri:

- **Hesap kurtarma işlemi:** Hesap sahibinin, sosyal medya platformunun hesap kurtarma araçlarını (şifre sıfırlama veya kimlik doğrulama) kullanarak hesabını geri alması.
- **İki faktörlü kimlik doğrulamanın (2FA) aktif edilmesi:** Hesaba girişlerde ek bir doğrulama yöntemi kullanılması (SMS, e-posta doğrulaması veya kimlik doğrulama uygulamaları).
- **Güçlü şifre kullanımı:** Daha karmaşık ve tahmin edilmesi zor bir şifre belirlemek, aynı şifreyi farklı hesaplarda kullanmaktan kaçınmak.
- **Şüpheli aktiviteleri izlemek:** Hesapta şüpheli bir oturum açılma veya etkinlik fark edilirse, hemen sosyal medya platformuyla veya destekle iletişime geçilmesi.
- **Güvenlik ayarlarının gözden geçirilmesi:** Hesap gizlilik ve güvenlik ayarlarının sıkılaştırılması ve yalnızca güvenilir cihazlardan giriş yapılması.

6.3.Grup 2: E-posta Kimlik Avı (Phishing) Saldırısı

Bir öğretmen, okul yönetimi tarafından gönderilmiş gibi görünen bir e-posta alır. E-posta, güncelleme yapılması gereken bir sistem bağlantısı içerir. Öğretmen bağlantıya tıklar ve kişisel bilgilerini (şifre, kimlik numarası) girer. Kısa bir süre sonra e-posta hesabına giriş yapamadığını fark eder. Öğretmenin bu saldırıyı fark ettiğinde yapması gerekenler nelerdir ve bu tür saldırılardan korunmak için ne gibi önlemler almalıdır?

6.4.Çözüm Önerileri:

- **Derhal şifreyi değiştirmek:** Kimlik avına maruz kalındığını fark eden kişi, hemen şifrelerini değiştirmelidir (e-posta, sosyal medya, banka gibi hesaplar dâhil).
- **Güvenlik yazılımları kullanmak:** Antivirüs veya anti-phishing yazılımlarını kullanarak sistemde olası kötü amaçlı yazılımların tespiti ve temizliği yapılmalıdır.
- **İki faktörlü kimlik doğrulama (2FA) etkinleştirilmesi:** Hesapları daha güvenli hâle getirmek için ek doğrulama yöntemleri uygulanmalıdır.
- **Gelen e-postaların doğruluğunu kontrol etmek:** Kurumlardan veya bankalardan gelen e-postalardaki bağlantılara tıklamadan önce, gönderenin resmi olup olmadığını kontrol etmek. Şüpheli e-postalar doğrudan silinmeli veya rapor edilmelidir.
- **Kişisel bilgilere dikkat etmek:** Hiçbir zaman e-posta aracılığıyla hassas bilgiler (şifreler, T.C. kimlik numarası) paylaşılmamalıdır.

6.5.Grup 3: Uygulamanın İzinsiz Veri Toplaması

Bir öğretmen, öğrencileriyle iletişim kurmak için popüler bir mesajlaşma uygulaması kullanmaktadır. Uygulamanın, kullanıcı bilgilerini izinsiz olarak topladığına ve üçüncü şahıslara sattığına dair haberler yayılmaya başlar. Öğretmen, bu durumu nasıl değerlendirmeli, öğrencilerinin güvenliğini sağlamak için ne gibi önlemler almalıdır?

6.6.Çözüm Önerileri:

- **Alternatif güvenli uygulamalar bulmak:** Güvenliği ihlâl edilen veya kişisel veri topladığı bilinen uygulamalar yerine güvenilir ve mahremiyete saygı gösteren alternatif uygulamalar tercih edilmelidir.
- **Uygulama izinlerini gözden geçirmek:** Uygulamanın hangi verilere eriştiğini gözden geçirmek ve gerekmediği halde kişisel verilere erişim iznini sınırlamak.
- **Kullanıcı sözleşmesini incelemek:** Uygulamanın gizlilik politikasını detaylıca okuyarak hangi verilerin toplandığını öğrenmek ve bunu kullanıcılarla paylaşmak.
- **Güvenlik yazılımlarından faydalanmak:** Mobil cihazlara güvenlik yazılımları yükleyerek kötü niyetli uygulamaların ve veri ihlallerinin önüne geçmek.
- **Öğrenciler ve velileri bilgilendirmek:** Öğrencileri ve velileri veri güvenliği hakkında bilgilendirmek, daha güvenli dijital araçlar kullanmaları konusunda farkındalık oluşturmak. (Schneier, B. (2015).

7. “Güvenli Sosyal Medya Profili Oluşturma” Etkinliği Senaryo Örnekler

7.1.Senaryo 1: Hacklenmiş Hesaptan Gelen Şüpheli Mesaj

Bir öğretmen, sosyal medya hesabında bir arkadaşından gelen garip bir mesaj alır. Mesajda, bir linke tıklaması ve kişisel bilgilerini paylaşması istenmektedir. Ancak mesaj, arkadaşının tipik yazım tarzına benzememektedir ve şüphe uyandırır. Bu durumda öğretmen, hesabın ele geçirilmiş olabileceğini düşünerek nasıl bir yol izlemelidir?

7.3.Çözüm Önerileri:

Mesaja yanıt vermemek ve linke tıklamamak: Öncelikle, şüpheli mesajlara yanıt verilmemeli ve gönderilen linklere tıklamaktan kaçınılmalıdır.

Arkadaşla farklı bir kanaldan iletişime geçmek: Hesabın sahibi olduğunu düşündüğü arkadaşına farklı bir iletişim yolu (telefon, e-posta) kullanarak ulaşip mesajın gerçekten ondan gelip gelmediğini doğrulamalıdır.

İki faktörlü kimlik doğrulama (2FA) kullanımı: Hesabın ele geçirilmemesi için öğretmen, kendi sosyal medya hesaplarında iki faktörlü kimlik doğrulamayı aktif hâle getirmeli ve güvenlik ayarlarını düzenlemelidir.

Şifrenin değiştirilmesi ve güvenlik kontrolleri: Eğer mesaj gönderen kişinin hesabı hacklenmişse, arkadaşının şifresini değiştirmesi ve sosyal medya platformunun güvenlik kontrollerinden geçmesi önerilmelidir.

7.4.Senaryo 2: Kimlik Avı (Phishing) İçeren E-posta

Bir öğretmen, bankasından geldiği iddia edilen bir e-posta alır. E-posta, öğretmenin hesap bilgilerini güncellemesi gerektiğini belirten bir link içerir. Link, bankanın resmi web sitesine çok benzeyen sahte bir siteye yönlendirme yapmaktadır. Öğretmen, bu e-postanın sahte olabileceğinden şüphelenir bu durumda nasıl bir çözüm stratejisi geliştirmelidir?

7.5.Çözüm Önerileri:

E-postanın kimliğini doğrulamak: E-posta adresini dikkatle incelemek ve resmi bir kaynaktan gelip gelmediğini kontrol etmek (örneğin bankanın resmi web sitesi üzerinden iletişim bilgilerini bulmak).

Linke tıklamamak: Şüpheli linklere tıklamamak ve hassas bilgileri doğrudan bu tür e-postalar aracılığıyla paylaşmamak önemlidir.

Bankayla doğrudan iletişime geçmek: Eğer mesaj bir bankayla ilgiliyse, bankanın resmi telefon numarası veya web sitesinden doğrudan iletişime geçerek e-postanın doğruluğunu sorgulamak.

Phishing raporlama: Öğretmen, bu tür kimlik avı e-postalarını ilgili bankaya veya platforma bildirmeli ve e-posta sağlayıcısına phishing olarak işaretlemelidir.

7.6.Senaryo 3: Kimlik Avı (Phishing) İçeren Direkt Mesaj

Bir öğretmen, sosyal medya platformunda bir arkadaşından gelen özel bir mesaj alır. Mesajda, öğretmenin bir çekilişi kazandığı belirtilmiş ve ödülü alabilmesi için kişisel bilgilerini paylaşması istenmiştir. Mesaj, şüpheli bir link ve hızlıca yanıt vermesini isteyen bir içerik barındırmaktadır. Bu durumda öğretmenin nasıl bir önlem alması ve bu saldırıdan korunmak için ne yapması gerektiğini belirlemesi istenir.

7.7.Çözüm Önerileri:

Mesajı dikkatlice incelemek: Mesajdaki hızlı tepki verme baskısı, ödül vaadi ve linkler gibi kimlik avı göstergelerini analiz etmek.

Linke tıklamamak: Mesajdaki linke tıklamak yerine, resmi bir kaynak üzerinden bilgilerin doğruluğunu araştırmak.

Arkadaşla farklı bir kanaldan iletişime geçmek: Mesajın gerçekten arkadaştan gelip gelmediğini kontrol etmek için telefon ya da başka bir sosyal medya hesabı gibi alternatif yollarla iletişim kurmak.

Sosyal medya hesap güvenliğini artırmak: Sosyal medya hesaplarında güvenlik ayarlarını kontrol etmek, iki faktörlü kimlik doğrulamayı (2FA) aktif hâle getirmek ve şifreleri düzenli olarak değiştirmek.

Kaynakça

- Altıntaş, S., & Barkuş, F. (2023). Dijital ortamlarda kişisel veri güvenliği kavramı üzerine bir derleme çalışması. Meslek Yüksekokulları Elektronik Dergisi, 13(2), 46-69. <https://dergipark.org.tr/en/download/article-file/3194391>
- E. B. Ceyhan, E. Demiryürek, ve B. Kandemir, "Sosyal Ağlarda Güncel Güvenlik Riskleri ve Korunma Yöntemleri", UBGMD, c. 1, sy. 1, ss. 1–10, 2015. <https://dergipark.org.tr/tr/pub/ubgmd/issue/18272/192646>
- National Cyber Security Centre. (2024, 20 Kasım). 10 steps to cyber security. <https://www.ncsc.gov.uk>
- Özkaya, E., & Toprak, B. (2022). Türkiye’de Güvenlik Faaliyetleri Kapsamında Kişisel Verilerin İşlenmesi. DergiPark, 11(2), 79-95. <https://dergipark.org.tr/en/download/article-file/2351149>
- Schneier, B. (2015). Data and Goliath: The hidden battles to collect your data and control your world. New York: W.W. Norton & Company.

MODÜL 7

Dijital Etik



Modül Kapsamı

Bu modül, dijital dünyada karşılaşılan etik sorunlara yönelik eğitimcilerin bilgi ve farkındalık düzeylerini artırmayı amaçlamaktadır. Dijital etik; dijital ortamlarda bireylerin ve kurumların sorumluluklarını, haklarını ve sınırlarını belirleyen bir kavramdır. Dijital çağda etik davranışlar; çevrim içi ortamlarda bilgilerin doğruluğu, kişisel veri ihlalleri ve dijital mülkiyet gibi konuların üzerinde durulması gereken önemli alanları kapsar. Eğitimcilerin bu alanlarda bilinçli davranışlar sergilemesi, öğrencilere de aynı bilinci kazandırmaları açısından kritik öneme sahiptir.

Öğrenme Kazanımları

- Dijital ortamda etik kavramını ve önemini tanımlama.
- Dijital içeriklerin ve kişisel verilerin korunmasına yönelik farkındalık geliştirme.
- Dijital mülkiyet ve akademik etik ihlallerini tanıma ve bunlara karşı bilinçli tavırlar sergileme.
- Dijital platformlarda ifade özgürlüğünün sınırlarını ve sorumluluklarını değerlendirme.

İçerik Ağacı

Dijital Etik

1. Etik ve Ahlâk Kavramları
 - 1.1. Etik İkilemler Atölyesi
2. Kişisel Verilerin İhlâli
 - 2.1. Kritik Durum Kartları ile Farkındalık
3. Bilginin Doğruluğu
 - 3.1. Doğru Bilgiyi Bulma Yarışı
4. Dijital Mülkiyet
 - 4.1. Hak ve Sorumluluk Tiyatrosu
5. Akademik Usulsüzlük
 - 5.1. İntihal Dedektifiği Çalışması
6. İfade Özgürlüğü
 - 6.1. Sorumlu Paylaşım Atölyesi

Dijital Etik

1. Etik ve Ahlâk Kavramları

Etik, dijital ortamlarda bireylerin doğru ve yanlış davranışlarını belirleyen kurallardır. Ahlâk ise bireylerin kendi değer yargıları doğrultusunda şekillenen davranışlardır. Dijital dünyada etik kurallarının önemi giderek artmaktadır. Çünkü çevrim içi ortamda anonimlik, bireylerin sınırları aşmasına neden olabilir.



1.1. Etik İkilemler Atölyesi

Vaka Sunumu: Katılımcılara kısa ve düşündürücü bir vaka sunulur. Örneğin, bir öğretmenin öğrenci bilgilerini paylaşırken farkında olmadan kişisel veri ihlâli yapması veya bir sosyal medya platformunda etik olmayan davranış sergilemesi.

Grup Çalışması: Katılımcılar 4-5 kişilik gruplara ayrılır ve her grup; vakayı etik açıdan tartışarak çözüm önerileri geliştirir.

Sonuç Paylaşımı: Her grup, çözüm önerilerini tüm sınıfla paylaşır. Diğer grupların önerilerini değerlendirir ve etik açıdan doğru yaklaşım tartışılır.

Sonuç ve Geri Bildirim: Eğitimci, etkinliğin sonunda etik ve ahlâka dair genel bir değerlendirme yaparak katılımcıların bu kavramları ne şekilde daha etkili kullanabileceğine dair geri bildirim verir.

2. Kişisel Verilerin İhlâli

Kişisel verilerin korunması, dijital dünyada en çok dikkat edilmesi gereken etik sorunlardan biridir. Türkiye’de KVKK (Kişisel Verileri Koruma Kanunu) ile kişisel veri ihlâlleri kontrol altına alınmaya çalışılsa da bu konudaki farkındalık artırılmalıdır. Kişisel Verilerin Korunması Kanunu kapsamında yapılması planlanan değişikliklerin zaman kaybetmeden gerçekleştirilmesi ve özellikle yapılacak değişikliklerin Avrupa Birliği düzenlemeleriyle eş değer boyutta olması gerekmektedir (Türkiye Barolar Birliği, 2022).



2.1. Kritik Durum Kartları ile Farkındalık

Hazırlık ve Bilgilendirme: Katılımcılar sınıfa girdiğinde, eğitimci kendilerine ait birkaç veriyi (örneğin ad-soyad, e-posta adresi) bir kâğıda/dijital forma yazmalarını ister.

Kimlik Avı Simülasyonu: Eğitmen, katılımcılara <https://www.proxynova.com/tools/send-anonymous-email/> adresi üzerinden kurumsal gibi görünen sahte bir e-posta gönderir. Bu e-posta, onlardan bir linke tıklamalarını ya da bir dosya indirmelerini ister. Bazı katılımcılar bu durumu fark etmeden linke tıklayıp sahte sayfada kişisel bilgilerini paylaşabilir.

Kimlik İhlâli Sürprizi: Etkinlik sırasında eğitmen, gizlice belirli katılımcıların adlarına sahte sosyal medya profilleri ya da e-postalar oluşturur ve grup içinde “kimlik ihlâli gerçekleşti” diyerek bu kişilerin dijital kimliklerinin çalındığını açıklar. Bu noktada katılımcılar, sahte kimliklerin nasıl kolayca oluşturulduğunu ve kötü niyetli kişilerin bu bilgileri nasıl manipüle edebileceğini görürler.

Sonuçları Tartışma: Eğitmen, katılımcılara ihlâl edilen kimlik bilgileri üzerinden oluşabilecek sonuçları belirtir:

- Kredi kartı dolandırıcılığı,
- Sosyal medyada sahte hesaplardan yapılan paylaşımlar,
- İş veya sosyal ilişkilerde güvensizlik yaratılması,
- Güvenlik açığı yaşayan kişilerin hissettikleri korku ve stres.

Çözüm Yolları ve Toplu Tartışma: Katılımcılar, bu tür ihlâlleri önlemek için hangi güvenlik önlemlerini alabilecekleri üzerine beyin fırtınası yapar. İki faktörlü kimlik doğrulama, güçlü şifreler kullanma, e-posta güvenliği, kişisel verilerin sınırlı paylaşımı gibi konular tartışılır.

3. Bilginin Doğruluğu

Dijital ortamda doğru bilginin ayırt edilmesi, özellikle sosyal medya ve diğer bilgi platformlarında yaygınlaşan yanlış bilgiler karşısında hayati bir öneme sahiptir.



3.1. Doğru Bilgiyi Bulma Yarışı

Bilgi Kartları Dağıtımı: Katılımcılar 4-5 kişilik gruplara ayrılır ve her gruba 5-6 tane haber başlığı içeren kartlar verilir. Bu kartlarda bazı haberler gerçek, bazıları ise uydurma ya da yanlış bilgilerden oluşmaktadır. Her grup; kendilerine verilen haberlerin hangisinin gerçek, hangisinin sahte olduğunu tartışarak belirlemeye çalışır. Bu aşamada kaynak kontrolü yapmalarına izin verilir.

Tartışma ve Sunum: Gruplar, buldukları sonuçları sunar ve her grubun haberlerin doğruluğunu nasıl tespit ettiğine dair kısa bir açıklama yapması istenir. Her haberin doğruluğu veya yanlışlığı eğitmen tarafından açıklanır ve haber kaynaklarının güvenilirliği üzerine grupça tartışma yapılır.

Değerlendirme ve Öneriler: Eğitmen; sahte bilgiye karşı alınabilecek önlemler, güvenilir kaynakların nasıl ayırt edileceği ve doğru bilginin nasıl yayılması gerektiği konusunda geri bildirimde bulunur. Ayrıca katılımcılara, dijital ortamlarda bilgi doğrulama araçları (Fact-Checking siteleri) hakkında bilgi verilir.

1.5 Dijital Mülkiyet

Fikri mülkiyet meselesi çağdaş bir sorundur ve bu çağdaş sorun hakkında birçok farklı görüş bulunmasına rağmen temel tartışmalar iki bakış açısı altında şekillenmektedir. Dijital dünyada fikri mülkiyeti savunanlar ve ona karşı çıkanlar. Her iki grubun anlaştığı noktalar mevcuttur. Fikri mülkiyetin yenilikleri teşvik ettiği ve eser üreticilerinin emeklerinin karşılığını almaları için bir miktar korumaya ihtiyaç olduğu konusunda genel bir mutabakat söz konusudur. Anlaşamadıkları nokta ise fikri hakların ölçüsünün ne olacağı ve bu sınırlamanın nereye kadar uzanacağıdır (Medin, B. (2017).



3.2. Hak ve Sorumluluk Tiyatrosu

Vaka Çalışmaları: Katılımcılar küçük gruplara ayrılır ve her gruba dijital mülkiyet ihlâliyle ilgili bir senaryo verilir. Örneğin:

- **Grup 1:** Bir öğretmenin çevrim içi bir blogdan aldığı makaleyi izinsiz şekilde ders materyali olarak kullanması.
- **Grup 2:** Bir öğrencinin sosyal medya üzerinde başka birine ait bir fotoğrafı sahibinden izin almadan paylaşması.
- **Grup 3:** Bir yazılımın illegal yollarla indirilip bir okulda kullanılması.

Her grup; senaryosundaki mülkiyet ihlâlini analiz eder, durumun neden bir ihlâl olduğunu tartışır ve çözüm önerileri sunar.

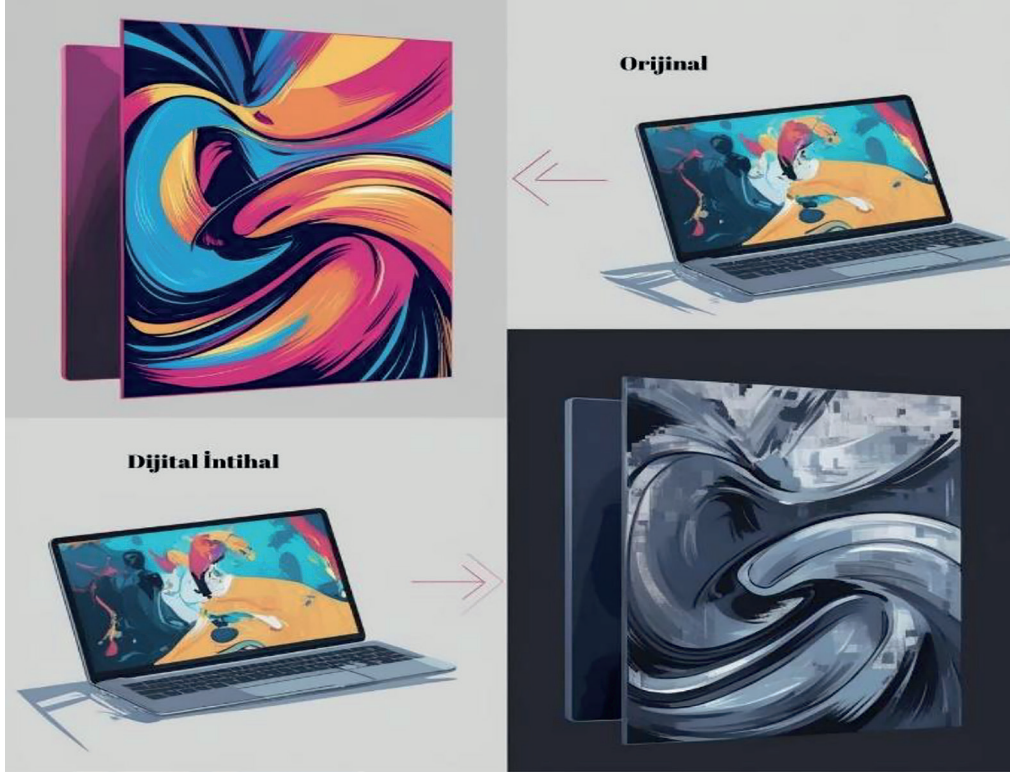
Sunum ve Tartışma: Gruplar, senaryolarını ve çözüm önerilerini diğer katılımcılara sunar. Her grup; telif hakları, adil kullanım (fair use) ve lisanslı içerik kullanımı hakkında öğrendikleri bilgileri sunum yaparak paylaşır. Eğitmen, bu noktada yanlış anlaşılımların önüne geçmek için geri bildirimde bulunur.

Değerlendirme ve Kapanış: Son olarak, dijital mülkiyetin ihlâl edilmemesi için içerik üretiminde dikkat edilmesi gereken hukuki ve etik kurallar tartışılır. Katılımcılar, dijital ortamda ürettikleri ve paylaştıkları içeriklerin telif haklarına nasıl uyabilecekleri konusunda farkındalık kazanır.

4. Akademik Usulsüzlük

Dijital çağda, akademik etik de büyük bir dönüşüm geçirmiştir. Özellikle çevrim içi kaynaklara erişim kolaylaştıkça intihal gibi etik ihlâllerin önüne geçmek daha zor hâle gelmiştir. Öğretmen adaylarının akademik usulsüzlüğe ilişkin görüşlerini, akademik usulsüzlük içeren davranışları sergileme düzeylerini ve bu davranışları yapma nedenlerini bütünsel olarak belirlemeyi amaçlayan bir araştırma akademik usulsüzlük için alınabilecek önlemlere ilişkin önemli sonuçlar ortaya koymuştur. Bu kapsamda öncelikle öğretmen adaylarının yarıdan fazlasının akademik usulsüzlüğün etik olmayan bir davranış olduğunu (%59.2), önlenmesine dönük uy-

gulamaların yaşama geçirilmesi gerektiğini (%60.2) düşündükleri ve bu yönde bir davranış sergilediklerinde suçluluk hissettikleri (%53.5) belirlenmiştir. Buna karşın %50.3'ünün akademik usulsüzlük olarak nitelendirilebilecek bir davranışta bulunduklarını beyan ettikleri görülmüştür (Özden, M., Özdemir Özden, D. ve Biçer, B. 2015).



4.1. İntihal Dedektifiği Çalışması

Vaka Çalışması: “Akademik Dedektifler”: Katılımcılar gruplara ayrılır ve her gruba bir vaka çalışması verilir. Örneğin:

- **Grup 1:** Bir öğretmenin makaleyi kaynak göstermeden kullanarak sunum hazırlaması.
- **Grup 2:** Bir öğrencinin, başka bir öğrencinin araştırma verilerini kendi çalışması gibi göstermesi.
- **Grup 3:** Bir öğretim görevlisinin, internetten aldığı bir kaynağı intihal ederek ders materyali hâline getirmesi.
- Gruplar, ellerindeki vaka örneğini inceleyerek akademik usulsüzlük olup olmadığını tartışır ve çözüm önerileri sunar. Her grup, çözüm yolunu önerirken etik ilkeleri göz önünde bulundurarak hangi adımların atılması gerektiğini tartışır.

Sunum ve Tartışma: Gruplar senaryolarını ve önerdikleri çözüm yollarını diğer katılımcılara sunar. Eğitimci, akademik usulsüzlüğün eğitimin kalitesine olan etkisine ve bu ihlallerin önlenmesine dair ek bilgi verir.

Değerlendirme ve Kapanış: Her grup, akademik dürüstlük ilkelerinin korunması için nelere dikkat etmeleri gerektiği konusunda geri bildirim alır. Katılımcılar, akademik dürüstlük hakkında daha derin bir anlayış geliştirir ve eğitim ortamında etik ilkelere nasıl uyacakları hakkında bilgi edinir.

1.6. İfade Özgürlüğü

İletişim teknolojilerindeki gelişmeler ve artan dijitalleşme, dezenformasyonun günümüz modern dünyasındaki etkisini ve gücünü arttırmıştır. Dezenformasyon; değişen yapısı ile farklı hak ve özgürlükleri tehdit edebilmekte, çözüm önerilerinin odak noktası ise toplumların yapıları ve hassasiyetleri doğrultusunda değişebilmektedir (Şahin, Z. B. (2023)).



4.2. Sorumlu Paylaşım Atölyesi

Münazara Hazırlığı: Katılımcılar iki gruba ayrılır. Her bir grup, “İfade özgürlüğü her koşulda sınırsız olmalıdır.” başlığı altında bir münazara gerçekleştirecek şekilde pozisyon alır. Bir grup ifade özgürlüğünün sınırsız olması gerektiğini savunurken diğer grup bu özgürlüğün sınırlandırılması gerektiğini savunur. Gruplar, savunacakları argümanlar üzerinde çalışır ve diğer gruba karşı nasıl savunma yapacaklarını planlarlar.

Münazara: Her grup sırayla argümanlarını sunar, karşı grup ise argümanlara yanıt verir. Bu bölümde özellikle öğretmenlerin, sınıflarında ifade özgürlüğüyle ilgili nasıl bir ortam oluşturabileceklerini ve bu özgürlüğü etik bir çerçevede nasıl yönetebileceklerini düşünmeleri teşvik edilir.

Değerlendirme ve Kapanış: Münazara tamamlandıktan sonra, tüm katılımcılarla birlikte tartışma yapılır. İfade özgürlüğünün eğitimde ve toplumda nasıl ele alınması gerektiği, öğretmenlerin bu konuda karşılaşılabilecekleri zorluklar ve çözüm yolları üzerinde durulur. Eğitimci, ifade özgürlüğünün sınırlarının etik çerçevede nasıl çizileceği konusunda önerilerde bulunur.

Kaynakça

- Medin, B. (2017). DİJİTALLEŞEN DÜNYADA FİKRİ HAKLAR SORUNU. Kırıkkale Üniversitesi Sosyal Bilimler Dergisi, 7(2), 51-68. <https://dergipark.org.tr/tr/download/article-file/335522>
- Özden, M., Özdemir Özden, D., & Biçer, B. (2015). Mersin Üniversitesi Eğitim Fakültesi Dergisi, 11(2), 505-525. <https://dergipark.org.tr/tr/download/article-file/161127>
- Şahin, Z. B. (2023). Dezenformasyonla Mücadelede İfade Özgürlüğü: İçeriğin Korunması ve 29. Madde. Yeni Medya(15), 282-299. <https://doi.org/10.55609/yenimedya.1339504>
- Türkiye Barolar Birliği. (2022). Dijital Dönüşüm ve Hukuk: Dijitalleşmenin Hukuk Üzerindeki Etkileri. Türkiye Barolar Birliği Dergisi, 2022(163), 2083. <https://tbbdergisi.barobirlik.org.tr/m2022-163-2083>.

MODÜL 8

Dijital Hukuk



Modül Kapsamı

Bu modül öğretmenlerin dijital hukuk konusunda yetkinlik kazanmalarını hedefler. Dijital okuryazarlık, dijital sağlık, dijital erişim, dijital iletişim, dijital ticaret, dijital güvenlik, dijital etik ile dijital hak ve sorumluluklar başlıkları içerik ağacını oluşturmaktadır. Her başlık dijital dünyada karşılaşılan hukuki durumlar hakkında bilgi ve etkinlikler içerir. Öğretmenler bu modülle birlikte dijital ortamda karşılaşılan hukuki meseleler hakkında farkındalık geliştirir ve bu konuları öğrencilerine doğru şekilde aktarabilme becerisi kazanır. İçerik ağacı, hukuki bilincin artırılması ve dijital dünyada etik davranışların teşvik edilmesini amaçlar. Eğitim, dijital çağın gereksinimlerine uygun olarak farkındalıklarımızı geliştirmeyi ve bu konularda çevremize ve öğrencilerimize örnek olabilmeyi hedefler.

Öğrenme Kazanımları

Modülün sonuna kadar katılımcılar;

- Dijital hukuk kavramını tanımlar.
- Dijital hukukun diğer vatandaşlık boyutlarıyla ilişkisini açıklar.
- Dijital okuryazarlığın bileşenlerini tanımlayarak hukuki çerçevesini anlar.
- Dijital sağlık hizmetlerinde karşılaşılan hukuki sorunları ve bu sorunların çözümlerini öğrenir.
- Dijital erişim ve hukuki düzenlemelerin önemini vurgular.
- Dijital iletişimde etik ve hukuki düzenlemeleri anlar ve uygular.
- Dijital ticaret işlemlerinde hukuki düzenlemeleri ve uygulamaları öğrenir.
- Dijital güvenlik ve hukuki çerçeveyi anlar.
- Dijital etik ve hukuki düzenlemelerin ilişkisini anlar.
- Dijital haklar ve sorumlulukların hukuki boyutunu kavrar.

İçerik Ağacı

1. Giriş
2. Dijital Okuryazarlık
 - 2.1 Kavram Haritası ve Tartışma
 - 2.2 Anahtar Kelimeler ve Kavramlar
3. Dijital Sağlık
 - 3.1 Vaka Analizi
 - 3.2 Elektronik Sağlık Kayıtları ve Gizlilik
4. Dijital Erişim
 - 4.1 Düşün-Eşleş-Paylaş
 - 4.2 Dijital Erişim Zorlukları
5. Dijital İletişim
 - 5.1 Kalem Konuşur
 - 5.2 Dijital İletişimde Etik ve Hukuk

6. Dijital Ticaret
 - 6.1 Sokratik Diyalog
 - 6.2 E-Ticaret Düzenlemeleri
7. Dijital Güvenlik
 - 7.1 Beyin Fırtınası
 - 7.2 Dijital Güvenlik Tehditleri
8. Dijital Etik
 - 8.1 Değerler Çizelgesi
 - 8.2 Dijital Etik Değerleri
9. Dijital Hak ve Sorumluluklar
 - 9.1 Grup Tartışması
 - 9.2 Dijital Haklar ve Sorumluluklar

1. Giriş

Dijital hukuk, internet ve dijital teknolojiler bağlamında yasal düzenlemeleri içeren dinamik bir alandır. Hem Türkiye’de hem de uluslararası alanda, dijital hukuk alanında önemli düzenlemeler ve yasalar bulunmaktadır.

Örneğin, Türkiye’de Kişisel Verileri Koruma Kanunu (KVKK), bireylerin kişisel verilerinin korunmasını sağlamak amacıyla yürürlüğe girmiştir (Kişisel Verileri Koruma Kurumu, 2020). KVKK; kişisel verilerin işlenmesi, saklanması ve üçüncü taraflara aktarılması gibi konularda sıkı düzenlemeler getirmektedir. Bu kanun, Avrupa Birliği Genel Veri Koruma Yönetmeliği’ne (GDPR) benzerlik göstermektedir.

Uluslararası alanda ise GDPR, dünya genelinde dijital veri koruma standartlarının yükselmesine katkı sağlamıştır. GDPR, AB sınırları içerisindeki bireylerin kişisel verilerinin korunmasını amaçlar ve bu konuda sıkı kurallar getirir.

Fikri mülkiyet hakları da dijital hukuk alanında önemli bir yer tutar. Türkiye’de Fikir ve Sanat Eserleri Kanunu, dijital ortamdaki yaratıcı eserlerin korunmasını sağlar (Ateş, 2012). Bu kanun, dijital içeriklerin izinsiz kopyalanmasını ve dağıtılmasını engellemeye yöneliktir. Uluslararası alanda ise Dünya Fikrî Mülkiyet Örgütü (WIPO), fikri mülkiyet haklarının korunması konusunda küresel standartlar belirlemektedir.

Siber suçlar, dijital hukuk kapsamında ele alınan bir diğer önemli konudur. Türkiye’de Türk Ceza Kanunu’nun 243. ve 244. maddeleri, siber suçlarla mücadeleyi düzenler (Türk Ceza Kanunu, 2020). Uluslararası düzeyde ise Birleşmiş Milletler, siber suçlarla mücadele konusunda çeşitli anlaşmalar ve protokoller oluşturmuştur.

E-ticaret düzenlemeleri de dijital hukuk içinde önemli bir yer tutar. Türkiye’de Elektronik Ticaretin Düzenlenmesi Hakkında Kanun, e-ticaret işlemlerinin güvenli ve adil bir şekilde gerçekleşmesini sağlamayı amaçlar (Elektronik Ticaretin Düzenlenmesi Hakkında Kanun, RG. 05.11.2014/29166). Uluslararası alanda ise OECD, e-ticaretin düzenlenmesi ve tüketici haklarının korunması konusunda önemli rol oynamaktadır (OECD).

2. Dijital Okuryazarlıkla İlişkisi

Dijital okuryazarlık; bireylerin dijital ortamlarda bilgi arama, kullanma ve üretme yeteneklerini içerir. Dijital hukuk bilgisi, bu yeteneklerin yasal sınırlar ve sorumluluklar çerçevesinde kullanılmasını sağlar. Özellikle gizlilik ayarlarının yönetimi, telif haklarının korunması ve yasal içerik paylaşımı dijital okuryazarlığın önemli bileşenleridir (Ateş, 2012). Dijital okuryazarlık, dijital hukuk bilgi ve becerilerini içerdiğinde daha etkili ve güvenli hâle gelir. Bu nedenle dijital hukukun anlaşılması, dijital okuryazarlığın ayrılmaz bir parçasıdır. Eğitim programları ve farkındalık kampanyaları, dijital okuryazarlığın artırılmasında önemli rol oynar (Bradford, 2020).

2.1. Kavram Haritası

Dijital hukukun dijital okuryazarlıkla ilişkisine dair düşüncelerinizi kavram haritası şeklinde belirtiniz. Belirlediğiniz kavramları ve ilişkiyi diğer katılımcılarla tartışınız.

Kavramlar

Dijital Okuryazarlık: Dijital teknolojileri etkin ve güvenli bir şekilde kullanma becerisi.

Veri Koruma: Kişisel bilgilerin gizliliğini sağlama.

Telif Hakları: Dijital içeriklerin yasal olarak korunması.

Çevrim İçi Güvenlik: İnternet ve dijital ortamda güvenliği sağlama.

Dijital Etik: Dijital dünyada sorumlu ve bilinçli davranış.

Bilgi Erişimi: Dijital kaynaklara ve bilgilere ulaşma becerisi.

Medya Okuryazarlığı: Dijital ve geleneksel medyayı eleştirel olarak anlama.

Siber Zorbalık: Çevrim içi ortamda yapılan zorbalık ve taciz.

Dijital Ayak İzi: İnternette bırakılan kişisel veri izleri.

Çevrim İçi Kimlik: Dijital dünyada bireyin kimliği ve kişisel bilgileri.

İnternet Etiği: İnternet kullanımı sırasında uyulması gereken etik kurallar.

İlişkiler

Dijital Okuryazarlık ve Veri Koruma: Dijital okuryazarlık, bireylerin kişisel verilerini koruma konusunda bilinçlenmesini sağlar.

Telif Hakları & Dijital Etik: Dijital içeriklerin telif haklarına saygı göstermek, dijital etik kurallarının bir parçasıdır.

Çevrim İçi Güvenlik & Bilgi Erişimi: Güvenli internet kullanımı, doğru ve güvenilir bilgilere erişimi artırır.

Medya Okuryazarlığı & Dijital Ayak İzi: Medya okuryazarlığı, dijital ayak izinin farkında olarak bilinçli medya tüketimini sağlar.

Siber Zorbalık & Çevrim İçi Kimlik: Çevrim içi kimlik bilgileri, siber zorbalığa karşı korunmalıdır.

İnternet Etiği & Çevrim İçi Güvenlik: İnternet etiği kurallarına uymak, çevrim içi güvenliği artırır.

3. Dijital Sağlıkla İlişkisi

Dijital sağlık, sağlık hizmetlerinin dijital teknolojilerle sunulmasını içerir. Dijital hukuk, sağlık bilgileri ve kayıtlarının korunmasını sağlar. Özellikle elektronik sağlık kayıtları ve mobil sağlık uygulamaları, kişisel verilerin korunması ve gizlilik düzenlemelerine tabidir (European Union). Türkiye’de Kişisel Verileri Koruma Kanunu (KVKK), sağlık bilgilerinin güvenli bir şekilde saklanması ve iletilmesini garanti eder (Kişisel Verileri Koruma Kurumu, 2020). Dijital sağlık hizmetlerinin etik kullanımı ve hastaların haklarının korunması da dijital hukuk çerçevesinde düzenlenir. Bu düzenlemeler, dijital sağlık uygulamalarının güvenli ve etkili olmasını sağlar.

3.1. Vaka Analizi

Modüllerde birden fazla etkinlik seçeneği sunulmuştur, uygun bulunan etkinlik kullanılabilir.



Etkinlik

Katılımcılar dörder veya beşer kişilik gruplara ayrılır. Dijital hukukun dijital sağlıkla ilişkisine dair hazırlanan vaka senaryoları her bir gruba verilir (EK1). Katılımcılar grupça verilen senaryodaki “Olası Hukuki Sorun ve Çözüm Önerilerini” belirler. (5’) Gruplar senaryolarını diğer katılımcılarla paylaşır. (5’)

Vaka 1: Elektronik Sağlık Kayıtlarının İhlâli

Senaryo: Bir hastane, elektronik sağlık kayıtları sisteminde veri ihlâli yaşar ve hastaların kişisel sağlık bilgileri izinsiz olarak üçüncü şahısların eline geçer.

Olası Hukuki Sorunlar: Kişisel verilerin izinsiz paylaşımı, hasta gizliliğinin ihlâli.

Çözüm Önerileri: Hastane; KVKK ve GDPR gibi veri koruma yasalarına uygun olarak acil durum protokollerini uygulamalı, etkilenen hastaları bilgilendirmeli ve veri güvenliğini artırıcı önlemler almalıdır.

Vaka 2: Sağlık Uygulamalarının Veri Toplaması

Senaryo: Bir mobil sağlık uygulaması, kullanıcıların sağlık verilerini izinsiz olarak toplar ve ticari amaçlarla kullanır.

Olası Hukuki Sorunlar: Gizlilik ihlâli, veri koruma yasalarının ihlâli.

Çözüm Önerileri: Uygulama geliştiricileri, veri koruma yasalarına uygun olarak kullanıcı verilerini toplamalı ve veri işleme süreçlerini şeffaf hâle getirmelidir. Kullanıcı onay süreçleri güçlendirilmelidir.

Vaka 3: Dijital Sağlık Sistemlerine Yönelik Siber Saldırıları

Senaryo: Bir hastane, siber saldırıya uğrar ve hasta bilgilerinin bir kısmı fidye yazılımı tarafından ele geçirilir.

Olası Hukuki Sorunlar: Veri güvenliği ihlâli, siber suçlar.

Çözüm Önerileri: Hastane; acil durum protokollerini devreye sokmalı, saldırıyı yetkili mercilere bildirmeli ve veri güvenliğini artırmak için siber güvenlik önlemlerini gözden geçirmelidir. Hukuki olarak siber saldırılara karşı daha etkili koruma ve yaptırım mekanizmaları geliştirilmelidir.

Vaka 4: Uygulama Hatası Nedeniyle Yanlış Tedavi

Senaryo: Bir hastane, hastaların tedavi sürecini takip etmek için dijital bir uygulama kullanmaktadır. Ancak uygulamada yaşanan bir hata nedeniyle bazı hastalar yanlış tedavi almaktadır.

Olası Hukuki Sorunlar: Tıbbi ihmaller, hatalı yazılım kullanımı.

Çözüm Önerileri: Uygulama geliştiricileri ve hastane yönetimi, yazılımın güvenilirliğini ve doğruluğunu artırmak için düzenli kontroller ve güncellemeler yapmalıdır. Hastaların zarar görmemesi için hızlı düzeltme yapılmalı ve iletişim süreçleri oluşturulmalıdır.

Vaka 5: Sağlık Bilgilerinin İşverenle Paylaşılması

Senaryo: Bir sağlık sigortası şirketi, müşterilerinin sağlık bilgilerini işverenlerle paylaşarak iş başvurusunda bulunan adayların sağlığını değerlendirir.

Olası Hukuki Sorunlar: Gizlilik ihlâli, adil olmayan iş değerlendirmesi.

Çözüm Önerileri: Sağlık sigortası şirketleri, kullanıcı verilerini sadece kullanıcı onayı ile gerekli gizlilik anlaşmalarına uygun olarak paylaşmalıdır. Bu tür bilgilerin izinsiz paylaşılması yasaklanmalıdır.

Vaka 6: Yanıltıcı Dijital Sağlık Reklamları

Senaryo: Bir sağlık ürünü, dijital platformlarda yanıltıcı reklamlarla tanıtılır ve bu ürünün sağlık üzerindeki etkileri abartılarak gösterilir.

Olası Hukuki Sorunlar: Yanıltıcı reklam, tüketici haklarının ihlâli.

Çözüm Önerileri: Reklam verenler; ürünlerinin sağlık üzerindeki etkilerini doğru ve dürüst bir şekilde tanıtmalı, yanıltıcı bilgilerin yer aldığı reklamlar yasal olarak denetlenmeli ve yaptırımlar uygulanmalıdır.

Vaka 7: Çevrim İçi Sağlık Danışmanlığında Gizlilik İhlâli

Senaryo: Bir çevrim içi sağlık danışmanlığı hizmeti, kullanıcıların sağlık bilgilerini izinsiz olarak üçüncü şahıslarla paylaşmaktadır.

Olası Hukuki Sorunlar: Kişisel veri ihlâli, gizlilik ihlâli.

Çözüm Önerileri: Çevrim içi sağlık danışmanlığı hizmetleri, veri koruma yasalarına uygun olarak kullanıcı bilgilerini işlemeli ve bu bilgilerin izinsiz paylaşımını engellemek için gerekli güvenlik önlemlerini almalıdır.

Vaka 8: Dijital Sağlık Verilerinin Yanlış Kullanımı

Senaryo: Bir araştırma merkezi, hastaların dijital sağlık verilerini izinsiz kullanarak ticari bir ürün geliştirir.

Olası Hukuki Sorunlar: Kişisel veri ihlâli, etik ihlâller.

Çözüm Önerileri: Araştırma merkezleri; veri kullanım izinlerini açık ve şeffaf bir şekilde almalı, veri sahiplerine veri kullanım amacı hakkında tam bilgi vermelidir. Etik kurallar ve veri koruma yasalarına sıkı bir şekilde uyulmalıdır.

4. Dijital Erişimle İlişkisi

Dijital erişim, bireylerin bilgi ve hizmetlere dijital platformlar üzerinden eşit ve adil bir şekilde ulaşabilmelerini ifade eder. Dijital hukuk, dijital erişimin sağlanmasında kritik bir rol oynar. Özellikle engelli bireylerin dijital platformlara erişimini sağlamak amacıyla yasal düzenlemeler yapılmaktadır (Gökçen, 2018). Ayrıca, dijital eşitsizliklerin giderilmesi ve herkesin dijital kaynaklara erişebilmesi için devletler ve uluslararası kuruluşlar çeşitli politikalar ve programlar geliştirmektedir (OECD). Dijital hukuk, dijital erişim haklarının korunması ve geliştirilmesi için temel bir yapı sağlar. Bu düzenlemeler, dijital kaynakların herkes için erişilebilir olmasını amaçlar.

4.1. Düşün-Eşleş-Paylaş



Etkinlik

Katılımcılara, bilgi ve hizmetlere dijital platformlar üzerinden eşit ve adil bir şekilde ulaşabilmenin ne ifade ettiği ve bu konuda özellikle engelli bireylerin ne gibi sorunlar yaşayabileceği sorulur. 1 dakika boyunca bireysel düşünen katılımcılar yanlarındaki katılımcıyla eşleşerek düşüncelerini birbirleriyle paylaşır. (3') Gönüllü katılımcılardan konu ile ilgili düşüncelerini tüm grupta paylaşması istenir. (5')

5. Dijital İletişimle İlişkisi

Dijital iletişim, internet ve diğer dijital platformlar aracılığıyla bilgi ve mesajların iletilmesini içerir. Dijital hukuk, bu iletişimin yasal çerçevede gerçekleşmesini sağlar. Özellikle sosyal medya kullanımı, çevrim içi taciz, nefret söylemi ve yanlış bilgilendirme gibi konular dijital hukuk kapsamında ele alınır (Ersoy, 2021). Dijital hukuk, dijital iletişimde gizlilik ve veri koruma standartlarını belirler ve bu standartların ihlâl edilmesi durumunda yasal yaptırımlar uygular (Cini ve Czulno, 2022). Böylece, dijital iletişimin güvenli ve etik bir şekilde gerçekleşmesi sağlanır.

5.1. Kalem Konuşur

Aşağıdaki konu başlıkları yazılı, önceden hazırlanmış beş farklı flipchart sınıfın (uygun olmadığı durumda koridorun) duvarlarına asılır. Katılımcılar beş gruba ayrılır. Katılımcıların eline birer kalem alması istenir. Etkinliğin adından da anlaşılacağı üzere bu dakikadan itibaren sadece kalemlerin konuşacağı bilgisi verilir. Her bir grup bir flipchartın önüne yönlendirilir. Herkesin bir dakika içinde önünde yer alan kavramla ilgili akıllarına gelen sorun ve çözümleri bireysel olarak yazmaları istenir. Bir dakika sonunda gruplar saat yönünde dönerek bir sonraki kavramla ilgili sorun ve çözüm önerilerini bireysel olarak yazarlar. Tüm flipchartlara yazıldıktan sonra katılımcılar yerlerine davet edilir. Beş gönüllü katılımcıdan flipchartlarda yazılanları tüm katılımcılarla paylaşması istenir.

Konu Başlıkları

Sosyal Medyada Nefret Söylemi
Çevrim İçi Taciz ve Siber Zorbalık
Kişisel Verilerin İzinsiz Paylaşımı
Telif Haklarının İhlâli
Dijital İçerik Manipülasyonu

Örnek Sorunlar ve Çözüm Önerileri

Sosyal Medyada Nefret Söylemi:

Sorun: Sosyal medyada nefret söylemi ve yanlış bilginin yayılması.

Çözüm: Hukuki düzenlemeler ve platform denetimleri artırılmalı, kullanıcı eğitimleri sağlanmalı.

Çevrim İçi Taciz ve Siber Zorbalık:

Sorun: Çevrim içi ortamda taciz ve zorbalık vakalarının artması.

Çözüm: Çevrim içi taciz ve zorbalığa karşı yasal önlemler alınmalı, kurban destek hizmetleri güçlendirilmeli.

Kişisel Verilerin İzinsiz Paylaşımı:

Sorun: Dijital platformlarda kişisel verilerin izinsiz paylaşılması.

Çözüm: Veri koruma yasalarına uyum sağlanmalı, kullanıcı gizlilik ayarları güçlendirilmeli.

Telif Haklarının İhlâli:

Sorun: Dijital içeriklerin izinsiz kopyalanması ve dağıtılması.

Çözüm: Telif hakları yasaları daha sıkı uygulanmalı, eğitim ve farkındalık kampanyaları düzenlenmeli.

Dijital İçerik Manipülasyonu:

Sorun: Dijital içeriklerin manipüle edilerek yanlış bilgilerin yayılması.

Çözüm: İçerik doğrulama mekanizmaları geliştirilmeli, yanlış bilgi yayanlara yaptırımlar uygulanmalıdır.

6. Dijital Ticaretle İlişkisi

Dijital ticaret, mal ve hizmetlerin dijital platformlar üzerinden satışını ve satın alınmasını içerir. Dijital hukuk, dijital ticaret işlemlerinin güvenli ve adil bir şekilde gerçekleşmesini sağlar. E-ticaret düzenlemeleri, tüketici haklarının korunması, elektronik sözleşmelerin geçerliliği ve dijital ödeme sistemlerinin güvenliği gibi konuları kapsar (Elektronik Ticaretin Düzenlenmesi Hakkında Kanun, 2014). Ayrıca dijital hukuk, dijital platformlarda rekabetin adil bir şekilde sürdürülmesini ve haksız rekabetin önlenmesini amaçlar (Bradford, 2020). Bu sayede, dijital ticaretin sağlıklı bir şekilde işlemesi sağlanır.

6.1. Sokratik Diyalog

Sokratik diyalog karşılıklı sorular sorarak ve cevaplar vererek konunun derinlemesine analiz edildiği bir tekniktir.

Eğitmen, katılımcılara aşağıdaki soruları sorarak katılımcıların eleştirel düşünme becerilerini geliştirirken katılımcılarla dijital ticaretin hukuki yönleri de tartışılır.

Soru 1: Dijital Ticarete Tüketici Hakları Neden Önemlidir?

Amaç: Tüketici haklarının korunmasının dijital ticaretteki önemini anlamak.

Tartışma: Katılımcılar, tüketici haklarının ihlâl edilmesi durumunda ortaya çıkabilecek sonuçları tartışır.

Tüketici haklarının ihlâl edilmesi, çeşitli ciddi sonuçlara yol açabilir.

Maddi Kayıplar: Tüketici, satın aldığı malın veya hizmetin eksik veya hatalı olması nedeniyle parasını kaybedebilir. İadeler kabul edilmez veya tazminat ödenmezse tüketici mağdur olur.

Güven Erozyonu: Tüketici, dijital platformlara ve e-ticaret sitelerine olan güvenini kaybeder. Bu durum, platformların itibarını zedeler ve müşteri kaybına neden olur.

Yasal Süreçler: Tüketiciler, haklarını aramak için yasal yollara başvurabilirler. Bu durum, uzun ve maliyetli dava süreçlerine yol açabilir.

Kişisel Bilgi Güvenliği: Tüketici verilerinin izinsiz kullanımı veya paylaşımı, kişisel veri ihlâli anlamına gelir. Bu, tüketicinin kimlik hırsızlığı ve dolandırıcılık gibi suçlarla karşı karşıya kalmasına neden olabilir.

Sağlık ve Güvenlik: Tüketici, güvenlik standartlarına uymayan bir ürün veya hizmet nedeniyle sağlık ve güvenlik riskleriyle karşı karşıya kalabilir. Bu, fiziksel zararlara veya ciddi sağlık sorunlarına yol açabilir.

Soru 2: Dijital Ödeme Sistemlerinde Veri Güvenliği Nasıl Sağlanır?

Amaç: Dijital ödeme sistemlerinde veri güvenliğinin sağlanma yollarını analiz etmek.

Tartışma: Katılımcılar, GDPR ve KVKK gibi veri koruma düzenlemelerinin rolünü tartışır.

GDPR (General Data Protection Regulation) ve KVKK (Kişisel Verilerin Korunması Kanunu), kişisel verilerin korunması ve gizliliğin sağlanması amacıyla oluşturulmuş yasal düzenlemelerdir.

GDPR Avrupa Birliđi (AB) genelinde geerlidir ve tm AB yesi lkelerde kiřisel verilerin korunmasını amalar. GDPR, veri iřleyen kuruluřların sıkı gvenlik nlemleri almasını ve veri sahiplerine eřitli haklar tanınmasını zorunlu kılar. rneđin; bireylerin verilerine eriřme verilerinin silinmesini talep etme ve verilerinin nasıl kullanıldıđına dair bilgilendirilme hakları vardır.

KVKK ise Trkiye’de yrrlkte olup benzer amalarla bireylerin kiřisel verilerini korumayı hedefler. KVKK; veri iřleyenlerin, veri sahiplerinin aık rızasını almalarını ve kiřisel verileri hukuka ve drstlk kurallarına uygun olarak iřlemelerini zorunlu kılar.

Bu dzenlemeler, bireylerin mahremiyetini koruyarak veri ihlllerine karřı gvenli bir dijital ortam yaratmayı amalar. Ayrıca, veri ihllleri durumunda ađır yaptırımlar ngrerek veri iřleyen kuruluřları caydırıcı řekilde etkiler.

Kısaca; GDPR ve KVKK, bireylerin dijital dnyadaki haklarını koruyan ve veri gvenliđini sađlayan temel yasal dzenlemelerdir.

Dijital deme sistemlerinde veri gvenliđi, eřitli yntemlerle sađlanır:

řifreleme (Encryption): Verilerin gizliliđini korumak iin iletilen veriler řifrelenir. Bu sayede, veriler izinsiz eriřimlere karřı korunur.

İki Faktrl Kimlik Dođrulama (2FA): Kullanıcıların hesaplarına ek gvenlik katmanı ekler. Giriř yapmak iin kullanıcı adı ve řifre dıřında bir ek dođrulama yntemi gerektirir.

Gvenli Soket Katmanı (SSL) ve Tařıma Katmanı Gvenliđi (TLS): deme iřlemlerinin gvenli bir řekilde gerekleřmesi iin SSL/TLS sertifikaları kullanılır. Bu, verilerin gvenli bir bađlantı zerinden iletilmesini sađlar.

Tokenizasyon: Kredi kartı bilgileri gibi hassas veriler, tek seferlik kullanılabilen token’ler ile deđiřtirilir. Bu, verilerin alınması durumunda bile gvenliđin korunmasını sađlar.

PCI DSS Uyumluluđu: deme kartı endstrisi veri gvenliđi standartlarına (PCI DSS) uyum, veri gvenliđi iin nemli bir adımdır. Bu standartlar, deme iřlemlerinde veri gvenliđinin sađlanması iin gereklilikler belirler.

Gncel Gvenlik Yazılımları: Antivirs ve anti-malware yazılımları kullanarak sistemleri ve verileri zararlı yazılımlara karřı korur. Ayrıca, gvenlik yamalarının dzenli olarak gncellenmesi nemlidir.

Bu yntemler, dijital deme sistemlerinde veri gvenliđini artırarak kullanıcıların gvenli ve sorunsuz bir řekilde deme yapmalarını sađlar.

Soru 3: E-ticarete Telif Hakları Nasıl Korunur?

Ama: Dijital ticarete telif haklarının korunmasının yollarını keřfetmek.

Tartıřma: Katılımcılar, dijital ieriklerin izinsiz kullanımını ve bunun hukuki sonularını tartıřır.

Hukuki Sonular:

Tazminat Talepleri: Telif hakkı sahibinin, izinsiz kullanım nedeniyle maddi zarara uğradıđını kanıtlaması durumunda mahkemeler tazminat denmesine karar verebilir.

Cezai Yaptırımlar: Birok lkede, telif hakkı ihlli cezai bir su olarak kabul edilir ve para cezası veya hapis cezası gibi yaptırımlar uygulanabilir.

İhtar ve İptal: Telif hakkı sahipleri, ihll edici ieriđin kaldırılması veya kullanımına son verilmesi iin ihtarname gnderebilir. İhtara uyulmaması durumunda hukuki sre bařlatılabilir.

İtibar Kaybı: Kurumlar veya bireyler, telif hakkı ihlalleri nedeniyle itibarlarını kaybedebilir ve güvenilirliklerini yitirebilirler.

Lisans Ücretleri: Telif hakkı sahipleri, izinsiz kullanımdan sonra içeriklerini kullanmak isteyenlerden lisans ücretleri talep edebilir.

Çözüm Önerileri:

Lisanslama: Dijital içerikleri kullanmadan önce yasal lisanslar alarak izinsiz kullanım riskini ortadan kaldırmak.

Kredi Verme: İçerik sahiplerine uygun şekilde atıfta bulunarak orijinal eser sahiplerinin haklarına saygı göstermek.

Eğitim ve Farkındalık: Telif hakkı ve dijital içeriklerin yasal kullanımı konusunda farkındalık artırıcı eğitimler düzenlemek.

Yasal Danışmanlık: Hukuki süreçler ve telif hakları konusunda profesyonel danışmanlık almak. Bu yasal önlemler ve farkındalık çalışmaları, dijital içeriklerin izinsiz kullanımını engellemeye yardımcı olur.

Soru 4: Dijital Platformlarda Satıcı ve Alıcı Arasındaki Hukuki Sorumluluklar Nelerdir?

Amaç: Dijital ticaret platformlarında tarafların hukuki sorumluluklarını incelemek.

Tartışma: Katılımcılar, sözleşme hukuku ve tüketici hakları açısından tarafların sorumluluklarını tartışır. Sözleşme hukuku ve tüketici hakları, tarafların hak ve sorumluluklarını düzenleyerek güvenli ve adil bir ticaret ortamı sağlar.

Sözleşme Hukuku Açısından:

Satıcı Tarafından:

Mal veya Hizmetin Teslimi: Sözleşmede belirtilen malı veya hizmeti zamanında ve tanımlandığı şekilde teslim etmek.

Bilgilendirme: Ürün veya hizmet hakkında doğru ve eksiksiz bilgi sağlamak.

Garanti ve İade: Ürün veya hizmetin garanti süresine ve iade koşullarına uygun olmasını sağlamak.

Alıcı Tarafından:

Ödeme Yükümlülüğü: Sözleşmede belirtilen bedeli, belirlenen zaman ve şekilde ödemek.

Ürünün Kabulü: Teslim edilen malın veya hizmetin kontrolünü yaparak onaylamak veya kusurları bildirmek.

Sözleşme Koşullarına Uyum: Sözleşmede belirtilen diğer şartlara uygun hareket etmek.

Tüketici Hakları Açısından:

Tüketici Hakları:

Bilgilendirilme Hakkı: Ürün veya hizmet hakkında tam ve doğru bilgiye sahip olma hakkı.

Güvenli Ürün Kullanma Hakkı: Sağlık ve güvenliği tehlikeye atmayacak ürün veya hizmet talep etme hakkı.

İade ve Garanti Hakkı: Ürün veya hizmetin iade edilmesi veya garanti kapsamında onarılması hakkı.

Hak Arama Hakkı: Şikâyetlerde ve uyuşmazlıklarda yasal yollara başvurma hakkı.

Satıcı Yükümlülükleri:

Açık ve Şeffaf Bilgilendirme: Tüketicilere ürün veya hizmet hakkında şeffaf bilgi sağlamak.

Kaliteli Hizmet Sağlama: Satılan ürün veya hizmetin kalitesini ve güvenliğini sağlamak.

Garanti ve İade Koşullarına Uyum: Tüketici haklarını gözeterek garanti ve iade süreçlerini yönetmek.

Yasal Düzenlemelere Uyum: Tüketici koruma yasalarına ve yönetmeliklerine uygun hareket etmek. Bu sorumluluklar, tüketici ve satıcı arasındaki ticari ilişkilerin adil ve güvenilir bir şekilde yürütülmesini sağlar.

Soru 5: Lojistik ve Teslimat Sürecinde Karşılaşılan Hukuki Sorunlar ve Bu Sorunların Çözümleri Nelerdir?

Amaç: Dijital ticarette lojistik ve teslimat sürecinde yaşanan hukuki sorunları ve çözüm yollarını analiz etmek.

Tartışma: Katılımcılar, hasarlı veya gecikmiş teslimatlarda tarafların sorumluluklarını tartışır.

Dijital ticarette lojistik ve teslimat süreçlerinde yaşanan hukuki sorunlar genellikle şunlardır:

Sipariş ve Teslimat Sorunları: Siparişlerin zamanında ve doğru şekilde teslim edilmesi konusunda yaşanabilecek hukuki sorunlar vardır. Örneğin, tedarik zinciri boyunca yaşanabilecek gecikmeler veya teslimat hatası gibi durumlar.

Veri Gizliliği ve Güvenliği: Müşteri verilerinin korunması ve güvenliği konusunda hukuki sorunlar yaşanabilir. Kişisel verilerin yanlışlıkla paylaşılabilmesi veya siber saldırılara maruz kalabileceği durumlar bu kapsamda yer alır.

Kargo ve Lojistik Hizmetleri: Kargo şirketleri ile olan sözleşmelerde yaşanabilecek hukuki sorunlar, kargo maliyetlerinin belirsizliği, kargo kayıpları veya kargoların zamanında teslim edilmemesi gibi konuları içerir.

Rekabet Hukuku: Dijital pazarlarda rekabet kurallarına uygun olmayan davranışlar, örneğin fiyat manipülasyonu veya telif hakları ihlâli gibi konular da hukuki sorunlardan biridir.

Çözüm yolları ise şunlardır:

Dijital Dönüşüm ve Teknoloji Kullanımı: Veri analitiği, yapay zekâ ve blockchain gibi teknolojilerin kullanımı lojistik ve teslimat süreçlerini daha verimli ve güvenli hâle getirir.

Hukuki Düzenlemeler ve Uyum: Dijital ticaretin hukuki düzenlemelerine uygun davranmak, özellikle veri gizliliği ve güvenliği konularında dikkatli olmak gereklidir.

Müşteri İletişimi ve Destek: Müşteri memnuniyetini artırmak için etkileşimli ve hızlı destek hizmetleri sunmak, sorunları hızlı bir şekilde çözmenin önemli bir yolu olabilir.

Rekabet Hukuku Uyumları: Dijital pazarlarda rekabet kurallarına uygun davranılmalı, fiyatlar ve hizmetlerin adil ve rekabetçi bir şekilde sunulması sağlanmalıdır.

Hasarlı veya gecikmiş teslimatlarda tarafların sorumlulukları, genellikle satış sözleşmesi ve yürürlükteki tüketici koruma yasalarına göre belirlenir.

Satıcı Tarafından:

Teslimat Sorumluluğu: Satıcı, ürünü zamanında ve hasarsız teslim etmekle yükümlüdür. Ürün hasarlı veya geç teslim edilirse satıcı ürünün yenisiyle değiştirilmesini veya iade kabulünü sağlamak zorundadır.

Güvence: Ürün teslimat sürecinde zarar görürse satıcı sorumluluk üstlenir ve zarar gören ürünü onarmak veya yenisiyle değiştirmek durumundadır.

Bilgilendirme: Müşteriyi gecikmeler ve olası sorunlar hakkında zamanında bilgilendirmek satıcının sorumluluğundadır.

Alıcı Tarafından:

Kontrol ve Bildirim: Ürünü teslim aldıktan sonra hemen kontrol edip herhangi bir hasar veya eksiklik varsa satıcıya bildirmek alıcının sorumluluğundadır.

Belgeler: Alıcı, hasarlı teslimat durumunda gerekli belgeleri (teslimat fişi, hasar raporu) sunmalı ve ürünün fotoğrafını çekerek durumu belgelemelidir.

Lojistik Şirketi:

Hasar ve Zarar Tazmini: Taşıma sırasında ürüne zarar verdiyse, lojistik şirketi zararı tazmin etmekle yükümlüdür.

Sigorta: Taşıma sigortası, hasar durumunda alıcıya veya satıcıya ödeme yaparak zararın tazmin edilmesini sağlar.

Bu sorumluluklar, tarafların hak ve yükümlülüklerini netleştirerek adil bir ticaret sürecinin sağlanmasına yardımcı olur.

7. Dijital Güvenlikle İlişkisi

Dijital güvenlik, dijital ortamda bilgi ve sistemlerin korunmasını ifade eder. Dijital hukuk, dijital güvenliğin sağlanmasında önemli bir rol oynar. Siber suçlarla mücadele, kişisel verilerin korunması ve veri ihlallerinin önlenmesi gibi konular dijital hukuk kapsamında düzenlenir (Türk Ceza Kanunu, 2020). Devletler ve uluslararası kuruluşlar, siber güvenlik standartlarını belirler ve bu standartların ihlâl edilmesi durumunda yasal yaptırımlar uygular (United Nations Office on Drugs and Crime). Böylece dijital ortamlarda güvenliğin sağlanması ve siber tehditlerin önlenmesi amaçlanır.

7.1. Beyin Fırtınası



Etkinlik

Katılımcılar beş gruba ayrılır. Gruplardan dijital güvenlik tehditlerini belirleyerek liste oluşturmaları istenir. (3') Gruplar oluşturdukları listelerdeki tehditlere yönelik hukuki çözüm önerileri geliştirirler. (3') Listeler ve çözüm önerileri diğer gruplarla paylaşılır. (3')

Yaygın dijital güvenlik tehditleri şunlardır:

Kimlik Hırsızlığı: Kişisel bilgilerinizi ele geçirerek sahte hesaplar açabilir veya finansal verilerinizi kullanabilirler.

Kötü Amaçlı Yazılımlar: Virüsler, trojanlar, casus yazılımlar gibi kötü amaçlı yazılımlar cihazınıza zarar verebilir veya bilgilerinizi çalabilir.

Siber Saldırıları: Büyük ölçekli saldırılar; hükümetler, şirketler veya bireyler üzerinde ciddi zararlar bırakabilir.

Veri Sızıntıları: Hassas verilerin sızdırılması, kişisel veya kurumsal bilgilerin tehlikeye girmesine neden olabilir.

Phishing Saldırıları: Sahte web siteleri veya e-postalar kullanarak kişisel bilgilerinizi ele geçirmeye çalışır.

Sosyal Mühendislik: İnsanları yanıltarak kişisel bilgileri veya gizli bilgileri elde etmeye çalışır.

İnsan Hataları: Yetersiz güvenlik bilincine sahip çalışanların yanlış davranışları, siber güvenliği tehdit edebilir.

Güvenlik Açıkları: Yazılım veya donanımın güvenlik açıkları, saldırganların cihazlarına erişim sağlamalarına olanak tanır.

Ransomware: Bilgilerinizi veya sistemlerinizi kilitler ve ödeme talep eder.

Wi-Fi Tehditleri: Gelişmiş Wi-Fi tehlikeleri gizliliği ihlâl edebilir.

Dijital güvenlik tehditlerine karşı alınabilecek bazı etkili çözüm önerileri şunlardır:

Kimlik Hırsızlığı:

Güçlü ve benzersiz şifreler kullanın.

İki faktörlü kimlik doğrulamayı etkinleştirin.

Kimlik bilgilerinizi düzenli olarak kontrol edin ve olası ihlalleri raporlayın.

Kötü Amaçlı Yazılımlar:

Antivirüs ve anti-malware yazılımları kullanın ve bu yazılımları güncel tutun.

Bilinmeyen kaynaklardan gelen e-posta eklerini açmayın ve dosyaları indirmeyin.

Yazılım ve işletim sistemlerinizi düzenli olarak güncelleyin.

Siber Saldırıları:

Güçlü güvenlik duvarları ve ağ izleme sistemleri kullanın.

Siber güvenlik konusunda eğitim alın.

Yedekleme stratejileri geliştirerek verilerinizi düzenli olarak yedekleyin.

Veri Sızıntıları:

Veri şifreleme tekniklerini kullanın.

Sıkı erişim kontrol politikaları belirleyin ve yalnızca gerekli kişilere erişim izni verin.

Veri izleme araçları kullanarak şüpheli aktiviteleri tespit edin.

Phishing Saldırıları:

Şüpheli e-postalar ve web siteleri konusunda dikkatli olun.

Phishing farkındalık eğitimleri düzenleyin ve çalışanları bilgilendirin.

Güvenilir e-posta filtreleme yazılımları kullanın.

Sosyal Mühendislik:

Sosyal mühendislik saldırılarına karşı eğitim alın.

Hassas bilgileri paylaşmadan önce kimlik doğrulaması yapın.

Güvenli bilgi paylaşım yöntemleri kullanın.

İnsan Hataları:

Güvenlik politikalarını netleştirin ve sıkılaştırın.

Düzenli olarak güvenlik eğitimleri düzenleyin.

Çalışanların farkında olmadan yapabilecekleri hataları en aza indirmek için teknolojik çözümler kullanın.

Güvenlik Açıkları:

Yazılım ve donanım güncellemelerini düzenli olarak yapın.

Güvenlik açıklarını tespit etmek için güvenlik testleri (penetrasyon testleri) uygulayın.

Açık kaynaklı yazılımlar kullanıyorsanız, topluluk güncellemelerini takip edin.

Ransomware:

Önemli verilerinizi düzenli olarak yedekleyin ve bu yedeklemeleri çevrim dışı olarak saklayın.

Bilinmeyen e-posta eklerini ve bağlantılarını açmaktan kaçının.

Sistemlerinizi düzenli olarak güncelleyin ve güvenlik yazılımları kullanın.

Wi-Fi Tehditleri:

Güçlü ve karmaşık Wi-Fi şifreleri kullanın.

WPA3 gibi güvenli şifreleme protokollerini tercih edin.

Şüpheli cihazları ve aktiviteleri izlemek için ağ izleme yazılımları kullanın.

8. Dijital Etik İlişkisi

Dijital etik, dijital teknolojilerin ve platformların etik kullanımıyla ilgilenir. Dijital hukuk, dijital etik konularında yasal çerçeve sağlar. Özellikle dijital platformlarda kullanıcı verilerinin etik kullanımı, yapay zekâ algoritmalarının şeffaflığı ve dijital içeriklerin etik paylaşımı gibi konular dijital hukuk kapsamında ele alınır (Güneş, 2019). Dijital etik ve dijital hukuk, dijital dünyada sorumlu ve bilinçli bir davranış kültürü oluşturmayı amaçlar. Bu sayede, dijital platformlarda etik ve yasal standartların korunması sağlanır (Kaya, 2021).

8.1. Değerler Çizelgesi



Etkinlik

Katılımcılar dijital etik değerlerin listesini oluştururlar. (2') Gönüllü katılımcılardan belirledikleri değerleri paylaşımları istenir. Belirlenen değerlerin hukuki yansımaları tartışılır. (8')

Olası değer ve hukuki yansımaları:

Gizlilik: Kişisel verilerin gizliliğine saygı göstermek ve koruma sağlamak.

Şeffaflık: Bilgi paylaşımında ve veri işleme süreçlerinde açık ve dürüst olmak.

Güvenlik: Dijital sistemlerin ve verilerin korunmasını sağlamak.

Adalet: Dijital hizmetlerde ve algoritmalarda ayrımcılığın önlenmesi ve eşitlik sağlanması.

Doğruluk: Bilginin doğru, eksiksiz ve güvenilir olmasını sağlamak.

Sorumluluk: Dijital ürün ve hizmetlerin kullanımında etik kurallara uyma yükümlülüğü.

Saygı: Kullanıcıların haklarına ve dijital ortamdaki davranışlarına saygı göstermek.

Gizlilik: Bireylerin çevrim içi ve çevrim dışı mahremiyetine saygı duymak.

İzin: Verilerin işlenmesi ve paylaşılması için kullanıcıların açık rızasını almak.

Erişilebilirlik: Dijital platformların herkes için erişilebilir olmasını sağlamak.

Dijital etik değerlerinin hukuki yansımaları, çeşitli yasalar ve düzenlemeler aracılığıyla korunur ve uygulanır:

Gizlilik: Kişisel Verilerin Korunması Kanunu (KVKK) ve Avrupa Birliği Genel Veri Koruma Yönetmeliği (GDPR), bireylerin kişisel verilerinin gizliliğini korur ve veri işleyen kuruluşların sıkı güvenlik önlemleri almasını zorunlu kılar.

Şeffaflık: GDPR, veri işleyen kuruluşların veri toplama ve işleme süreçlerinde şeffaf olmalarını gerektirir. Kullanıcıların hangi verilerin toplandığını ve nasıl kullanıldığını anlamalarını sağlar.

Güvenlik: Yasanın adından bahsedilmiyorsa ve düzenlemeleri, dijital sistemlerin korunmasını ve siber saldırılara karşı önlemler alınmasını sağlar. Bu yasal çerçeveler, veri ihlalleri durumunda yaptırımlar uygular.

Adalet: Erişilebilirlik Yasaları, dijital hizmetlerin ve içeriklerin herkes için erişilebilir olmasını sağlar. Engelli bireylerin dijital ortamlarda eşit imkânlarla sahip olmalarını zorunlu kılar.

Doğruluk: Yanıltıcı Reklam Yasaları, dijital platformlarda yayımlanan bilgilerin doğru ve güvenilir olmasını zorunlu kılar. Yanıltıcı veya sahte bilgilere karşı yaptırımlar uygular.

Sorumluluk: Elektronik Ticaret Yasaları, dijital ürün ve hizmet sağlayıcılarının sorumluluklarını belirler. Müşteri haklarını koruyan düzenlemeler içerir.

Saygı: Çevrim İçi Taciz ve Zorbalık Yasaları, dijital ortamlarda kullanıcıların haklarına saygı gösterilmesini zorunlu kılar. Taciz ve zorbalık durumlarında hukuki yaptırımlar uygular.

Gizlilik: Veri Koruma Yasaları, bireylerin çevrim içi ve çevrim dışı mahremiyetinin korunmasını sağlar. İzinsiz veri işleme ve paylaşma durumlarına karşı hukuki yaptırımlar içerir.

İzin: GDPR ve benzeri düzenlemeler, verilerin işlenmesi ve paylaşılması için açık ve bilgilendirilmiş rıza alınmasını zorunlu kılar. Kullanıcıların verilerini kontrol etmelerini sağlar.

Erişilebilirlik: Engelli Hakları Yasaları ve WCAG (Web Content Accessibility Guidelines) standartları, dijital platformların erişilebilir olmasını sağlar. Bu standartlara uyum, yasal bir gerekliliktir.

9. Dijital Hak ve Sorumluluklarla İlişkisi

Dijital haklar ve sorumluluklar, bireylerin dijital ortamlarda sahip oldukları haklar ve bu hakların kullanımından doğan sorumlulukları ifade eder. Dijital hukuk, dijital hakların korunması ve sorumlulukların belirlenmesi için yasal çerçeve sağlar (Doğan, 2021). Özellikle kişisel verilerin korunması, dijital içeriklerin mülkiyet hakları ve çevrim içi ifade özgürlüğü gibi konular dijital hukuk kapsamında düzenlenir (Ersoy, 2021). Böylece, bireylerin dijital dünyada haklarını bilinçli bir şekilde kullanmaları ve sorumluluklarını yerine getirmeleri sağlanır.

9.1. Grup Tartışması



Etkinlik

Katılımcılardan dijital hak ve sorumluluklarla ilgili sorun ve çözüm önerilerini belirlemeleri istenir. (10') Gönüllü katılımcılarla grup tartışması devam ettirilir.

Sorunlar:

Gizlilik İhlalleri: Kişisel verilerin izinsiz paylaşılması ve kullanılması.

Telif Hakkı İhlalleri: Dijital içeriklerin izinsiz kopyalanması ve dağıtılması.

Çevrim İçi Taciz ve Zorbalık: Dijital platformlarda zorbalık, taciz ve tehditlerin artması.

Veri Güvenliği: Hassas bilgilerin çalınması veya sızdırılması.

Dezenformasyon: Yanlış bilgilendirme ve sahte haberlerin yayılması.

Erişim Engelleri: Engelli bireylerin dijital platformlara ve içeriklere erişimde zorluk yaşaması.

İnternet Erişim Eşitsizliği: Kırsal bölgelerde veya düşük gelirli topluluklarda internet erişiminin sınırlı olması.

Siber Suçlar: Kimlik hırsızlığı, dolandırıcılık ve kötü amaçlı yazılımlar gibi suçların artması.

Çözüm Önerileri:

Gizlilik İhlalleri: Güçlü veri koruma yasaları (örneğin, GDPR ve KVKK) uygulanmalı. Şirketler ve kurumlar, veri gizliliği politikalarını şeffaf bir şekilde belirlemeli ve bu politikalara uymalıdır.

Telif Hakkı İhlalleri: Telif hakkı yasaları sıkı bir şekilde uygulanmalı ve ihlallerde yaptırımlar artırılmalı. Dijital platformlar, telif hakkı sahiplerine koruma sağlamak için gelişmiş izleme ve bildirim sistemleri kullanmalıdır.

Çevrim İçi Taciz ve Zorbalık: Sosyal medya ve dijital platformlarda zorbalık ve tacizi önlemek için daha sıkı denetimler ve politikalar uygulanmalı. Kullanıcılara çevrim içi zorbalık ve taciz hakkında eğitimler verilmeli.

Veri Güvenliği: Kişisel ve hassas verilerin şifrelenmesi ve güvenli veri saklama yöntemleri kullanılmalı. Veri güvenliği konusunda kullanıcılar ve çalışanlar düzenli olarak eğitilmeli.

Dezenformasyon: Sosyal medya platformları, sahte haberlerin yayılmasını önlemek için içerik doğrulama sistemleri geliştirmeli. Kullanıcılara medya okuryazarlığı eğitimleri verilmeli ve doğru bilginin nasıl tespit edileceği öğretilmeli.

Erişim Engelleri: Dijital platformlar ve içerikler, herkes için erişilebilir olmalı. Engellilere yönelik özel erişim çözümleri geliştirilmeli. Erişilebilirlik standartları belirlenmeli ve bu standartlara uyulmalı.

İnternet Eriřim Eřitsizlięi: Kırsal bölgelerde ve düşük gelirli topluluklarda internet altyapısı geliştirilmeli. Dijital uçurumu kapatmak için devlet destekli programlar ve projeler başlatılmalı.

Siber Suçlar: Siber suçlarla mücadele için ulusal ve uluslararası iş birlikleri artırılmalı. Kullanıcılara ve kurumlara siber güvenlik konusunda eğitimler verilerek farkındalık artırılmalı.

EK1. Vaka Analizi Çalışma Kâğıdı

EK - 1

Vaka 1: Elektronik Sağlık Kayıtlarının İhlâli

Senaryo: Bir hastane, elektronik sağlık kayıtları sisteminde veri ihlâli yaşar ve hastaların sağlık bilgileri izinsiz olarak üçüncü şahısların eline geçer.

Olası Hukuki Sorunlar:

Çözüm Önerileri:

Vaka 2: Sağlık Uygulamalarının Veri Toplaması

Senaryo: Bir mobil sağlık uygulaması, kullanıcıların sağlık verilerini izinsiz olarak toplar ve ticari amaçlarla kullanır.

Olası Hukuki Sorunlar:

Çözüm Önerileri:

Vaka 3: Dijital Sağlık Sistemlerine Yönelik Siber Saldırıları

Senaryo: Bir hastane, siber saldırıya uğrar ve hasta bilgilerinin bir kısmı fidye yazılımı tarafından ele geçirilir.

Olası Hukuki Sorunlar:

Çözüm Önerileri:

Vaka 4: Uygulama Hatası Nedeniyle Yanlış Tedavi

Senaryo: Bir hastane, hastaların tedavi sürecini takip etmek için dijital bir uygulama kullanmaktadır. Ancak uygulamada yaşanan bir hata nedeniyle bazı hastalar yanlış tedavi almaktadır.

Olası Hukuki Sorunlar:

Çözüm Önerileri:

Vaka 5: Sağlık Bilgilerinin İşverenle Paylaşılması

Senaryo: Bir sağlık sigortası şirketi, müşterilerinin sağlık bilgilerini işverenlerle paylaşarak iş başvurusunda bulunan adayların sağlığını değerlendirir.

Olası Hukuki Sorunlar:

Çözüm Önerileri:

Vaka 6: Yanıltıcı Dijital Sağlık Reklamları

Senaryo: Bir sağlık ürünü, dijital platformlarda yanıltıcı reklamlarla tanıtılır ve bu ürünün sağlık üzerindeki etkileri abartılarak gösterilir.

Olası Hukuki Sorunlar:

Çözüm Önerileri:

Vaka 7: Çevrim İçi Sağlık Danışmanlığında Gizlilik İhlali

Senaryo: Bir çevrim içi sağlık danışmanlığı hizmeti, kullanıcıların sağlık bilgilerini izinsiz olarak üçüncü şahıslarla paylaşmaktadır.

Olası Hukuki Sorunlar:

Çözüm Önerileri:

Vaka 8: Dijital Sağlık Verilerinin Yanlış Kullanımı

Senaryo: Bir araştırma merkezi, hastaların dijital sağlık verilerini izinsiz kullanarak ticari bir ürün geliştirir.

Olası Hukuki Sorunlar:

Çözüm Önerileri:

Not: Her bir vaka senaryosu --- işaretli yerlerden kesilerek gruplara dağıtılmalıdır.

KAYNAKÇA

Ateş, M. (2012). Fikri Hukukta Eser Sahipliği. Ankara: Adalet Yayınları.

Bradford, A. (2020). The Brussels Effect: How the European Union Rules the World. Oxford University Press.

Cini, M., & Czulno, P. (2022). Digital Single Market and the EU Competition Regime: An Explanation of Policy Change.

Doğan, C. (2021). Dijital Haklar ve Sorumluluklar. Ankara: Seçkin Yayıncılık.

Elektronik Ticaretin Düzenlenmesi Hakkında Kanun, 2014. Kanun No: 6563. Resmî Gazete No: 29166.

Ersoy, Ç. (2021). Dijital İletişim ve Hukuk. Ankara: Seçkin Yayıncılık.

European Union. General Data Protection Regulation (GDPR). (Erişim tarihi: 28.10.2024).

https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en

Gökçen, Y. (2018). Dijital Erişim ve Eşitlik. İstanbul: Beta Yayınları.

Güneş, Y. (2019). Dijital Etik ve Hukuk. İstanbul: Derin Yayınları.

<https://copilot.microsoft.com/>

Kaya, A. A. (2021). Yapay Zekâ Hukuku. Seçkin Yayıncılık.

Kişisel Verileri Koruma Kurumu. (2020). Kişisel Verileri Koruma Kanunu. (Erişim tarihi: 28.10.2024).

<https://www.kvkk.gov.tr/>

OECD. E-commerce Regulation. (Erişim tarihi: 28.10.2024).

<https://www.oecd.org/sti/consumer/e-commerce.htm>

Türk Ceza Kanunu, 2020. Kanun No: 5237. Resmî Gazete No: 25611.

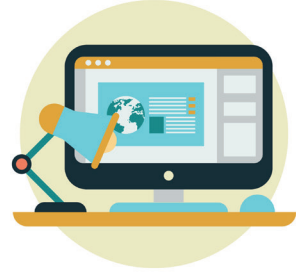
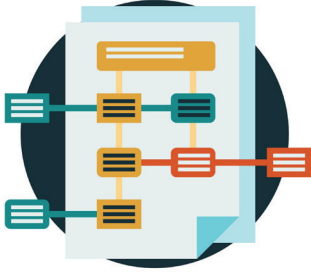
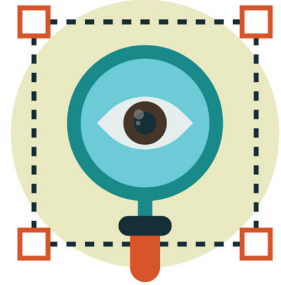
United Nations Office on Drugs and Crime. Cybercrime. (Erişim tarihi: 28.10.2024).

<https://www.unodc.org/unodc/en/cybercrime/index.html>

World Intellectual Property Organization. Intellectual Property. (Erişim tarihi: 28.10.2024).

MODÜL 9

Dijital Hak ve Sorumluluklar



Modül Kapsamı

Bu modül, eğitimcilerin “Dijital Vatandaşlık” kavramıyla önem kazanan “Dijital Haklar ve Sorumluluklar” konusunda farkındalık kazanmalarını ve bu farkındalığı günlük yaşamda kullanılan dijital ortamlara ve öğrencilerine aktarabilmelerini amaçlayan bir eğitim programıdır. Geleneksel anlamda vatandaşların hak ve sorumlulukları bulunduğu gibi, dijital vatandaşların da dijital ortamlarda sahip olduğu haklar ve yerine getirmekle yükümlü olduğu sorumluluklar bulunmaktadır. Dijital vatandaşların hem kendi hak ve sorumluluklarının bilincinde olması ve bunları koruması hem de başkalarının haklarını ve sorumluluklarını gözetmesi önemlidir (Council of Europe, t.y.). Bu kapsamda dijital hak ve sorumluluklar sırasıyla eğitim hakkı, kişisel verilerin korunması hakkı, bilgiye erişim ve iletişim hakkı, özel gereksinimi olan bireylere yönelik haklar, aile ve çocuklara yönelik haklar olmak üzere beş başlıkta ele alınacaktır.

Öğrenme Kazanımları

Modülün sonuna kadar katılımcılar;

- Dijital toplum içerisindeki bireylerin hak ve sorumluluklarını tanımlayabilecektir.
- Eğitim hakkı kavramı ve bu hakkın dijital ortamdaki karşılığı ile ilgili farkındalık kazanacaktır.
- Kişisel verilerin korunması hakkı kavramı ve bu hakkın dijital ortamda karşılığı ile ilgili farkındalık kazanacaktır.
- Bilgiye erişim ve iletişim hakkı kavramı ve bu hakkın dijital ortamda karşılığı ile ilgili farkındalık kazanacaktır.
- Özel gereksinimi olan bireylere yönelik haklar ve bu hakların dijital ortamda karşılığı ile ilgili farkındalık kazanacaktır.
- Aile ve çocuklara yönelik haklar ve bu hakların dijital ortamda karşılığı ile ilgili farkındalık kazanacaktır.

İçerik Ağacı

1. Giriş
 - 1.1. Tartışma: Hak ve Sorumluluklar
2. Eğitim Hakkı
 - 2.1. Dijital Ortamda Eğitim Hakkı
 - 2.2. Grup Çalışması: Öğretmenler Dijital Dönüşümde Eğitim Hakkını Nasıl Değerlendiriyor?
3. Kişisel Verilerin Korunması Hakkı
 - 3.1. Dijital Ortamda Kişisel Verilerin Korunması Hakkı
 - 3.2. Grup Çalışması: Kişisel Verileri Koruma
4. Bilgiye Erişim ve İletişim Hakkı
 - 4.1. Dijital Ortamda Bilgiye Erişim ve İletişim Hakkı
 - 4.2. Tartışma Çemberleri: Bilgiye Erişim ve İletişim

5. Özel Gereksinimi Olan Bireylere Yönelik Haklar
 - 5.1. Dijital Ortamda Özel Gereksinimi Olan Bireylere Yönelik Haklar
 - 5.2. Düşün-Eşleş-Paylaş: Özel Bir Yol Haritası
6. Aileye ve Çocuklara Yönelik Haklar
 - 6.1. Dijital Ortamda Aileye ve Çocuklara Yönelik Haklar
 - 6.2. İnceleme: Dijital Ortamlarda Çocuk Hakları ile İlgili Genel Yorum No.25

Giriş

Dijital teknolojilerin geliştirilmesi ve toplumun kullanımına sunulması, bireylerin dijital ortamlarda aktif olarak yer almasını sağlamıştır. Dijital hak, bireylerin dijital ortamlarda teknolojik cihazlar yoluyla bilgiye erişimini, içerik oluşturabilme imkânını ve oluşturduğu içeriği yayımlama özgürlüğünü (Bayzan, 2019), bunları yaparken kişisel bilgilerini ve mahremiyetini koruma hakkını ifade eder. Türk Dil Kurumu “sorumluluk” kelimesini; “kişinin kendi davranışlarını veya kendi yetki alanına giren herhangi bir olayın sonuçlarını üstlenmesi” olarak tanımlamıştır. Bu bağlamda bireyin, dijital haklarından doğan davranışlarının sonuçlarını üstlenmesi dijital sorumluluk kapsamında değerlendirilebilir. Bireylerin kendi hak ve sorumluluklarının farkında olması ve bunları koruması aynı zamanda diğer bireylerin hak ve sorumluluklarının da farkında olmasını ve gözetmesini gerekli kılar. Bu farkındalığı kazandırmak için öğrencilere erken dönemlerde eğitim verilmesinin gerekliliği kaçınılmazdır. Ribble (2011), dijital araçları kullanım yaşının gittikçe düşmesi nedeniyle dijital vatandaşlık kavramı ve dijital araçların kullanımı konusunda çocuklara erken yaşlardan itibaren eğitim verilmesi gerektiğini belirtmiş ve aynı zamanda Selwyn ve Facer (2007), çocukların bilinçli seçimler yapabilmesi için dijital toplumların destek sunması gerekliliğini vurgulamıştır (Akt., Yıldırım ve Keser, 2022). Dijital çağda ebeveynlerin ve kurumların aldıkları önlemler bulunsa da çocukların kendi haklarının ve sorumluluklarının farkında olması kalıcı çözümler sağlayacaktır (Yıldırım ve Keser, 2022). Bu nedenle çocuklara, dijital hak ve sorumluluklar konusunda eğitim verilmesi ve rehberlik edilmesi dijital vatandaşlık bağlamında gereklidir. Öğrencilerin hak ve sorumluluklarının farkında olarak dijital ortamlarda var olmaları gerekmektedir (Akt., Yılmaz, 2014).

Türkiye Yüzyılı Maarif Modeli’nde öğrencilerin okuryazarlık becerilerini geliştirmesi önemsenmiştir. Modelde okuryazarlık becerisi; bilgi okuryazarlığı, dijital okuryazarlık, finansal okuryazarlık, görsel okuryazarlık, kültür okuryazarlığı, vatandaşlık okuryazarlığı, veri okuryazarlığı, sürdürülebilirlik okuryazarlığı ve sanat okuryazarlığı alt başlıklarında ele alınmıştır. Türkiye Yüzyılı Maarif Modeli’nde yer alan okuryazarlık becerilerine ait süreç bileşenleri üç düzeyde ele alınmıştır. “Bu üç düzey; okuryazarlık türünde geçen temel bilgi, terim, kavram ve olguları tanımlama, anlama, bunların farkında olma ve duyarlılık göstermeye yönelik farkındalık düzeyi; öğrencilerin bu bilgi, terim, kavram ve olgulara yönelik bütüncül ilişkiyi fark etmelerine yönelik işlevsellik düzeyi ve edinilen bilgilere yönelik öğrencilerin eyleme geçeceği eylemsellik düzeyidir. Bu düzeyler, gelişime uygun ve sarmal bir yapıda kurgulanmıştır” (Millî Eğitim Bakanlığı [MEB], 2024).

FARKINDALIK	İŞLEVSELLİK	EYLEMSELLİK
- Dijital Bilgiye Ulaşma ve Dijital Bilgiyi Tanıma - Dijital İletişimi Anlama	- Fikrî Mülkiyet Haklarına Uygun Davranma - Dijital Bilgiyi Anlamlandırma - Dijital Ortamlar İçin İçerik Oluşturma ve Paylaşma	- İletişim Kurma ve Paylaşma - Dijital Araçlarla İş Görme - E-Güvenlik Önlemleri Alma - Dijital Bilgiyi Kullanarak Eleştirel Düşünme

1.1.Tartışma: Hak ve Sorumluluklar

Aşağıdaki soruları tartışınız.



- ✓ Dijital bir toplum içerisinde bireylerin/öğrencilerin hangi hak ve sorumlulukları bulunmaktadır?
- ✓ Dijital toplumda bireylere/öğrencilere bu hak ve sorumluluklar nasıl kazandırılır?

2. Eğitim Hakkı

Eğitim hakkı ve insan hakları ortak bir amaç altında birleştirilebilir. Herkesin sahip olduğu özgürlük, refah ve insan onuruna uygun bir yaşam hakkı bulunmalıdır (Akt., Binbir ve Arastaman, 2021). Eğitim hakkı; insanın hak, özgürlük ve sorumluluklarını kullanarak kendi potansiyelini en etkili şekilde kullanmasını sağlayan temel haktır. Böylelikle birey hem kendine hem de topluma üst düzeyde katkı sağlamaktadır. Eğitim, okul aracılığıyla öncelikli olarak çocukları ve farklı eğitim kurumları ile tüm yaş gruplarını kapsayan bir süreçtir (Akt., Binbir ve Arastaman, 2021). Ataman (2018) eğitim hakkının; temel bir insanlık hakkı olduğunu belirterek herkesin ırk, cinsiyet, etnik köken, dini veya politik görüş, yaş, özel eğitim gereksinimi gibi durumuna bakılmaksızın eğitimden yararlanması gerekliliğini vurgulamıştır (Akt., Binbir ve Arastaman, 2021).

2.1.Dijital Ortamda Eğitim Hakkı

Dijital teknolojiler eğitim alanında hızlı bir şekilde yer edinmektedir. Özellikle COVID-19 pandemisinden sonra bu hızın arttığı ve birçok bireyin eğitimden dijital ortamda da yararlandığı söylenebilir. Günlük yaşamdaki dijitalleşmenin doğal bir sonucu olarak eğitimde de dijital dönüşüm beklentisi kaçınılmazdır (Akt., Parlak, 2017). Bu dönüşüm eğitim ortamlarında kullanılan

dijital araçların, bilgi ve iletişim teknolojilerinin çeşitlenmesini sağlamaktadır. Dijital araçların bir kısmı “donanım”, bir kısmı “yazılım” ve diğer bir kısmı da “ortamlar” olarak sınıflandırılabilir (Akt., Parlak, 2017). Dijital ortamlarda eğitim hakkı bu bağlamda önem kazanmaktadır. Dijital dönüşüm yeni fırsatlar sunarken koşulların düzenlenmesi, eğitim hakkından her bireyin yararlanması ve fırsat eşitliğinin sağlanması için belirli düzenlemelerin yapılması gereklidir. Günümüzde giderek artan dijital dışlanma ve dijital cehaletin bir problem olduğu ve bunu önleyecek etkin yolların bulunması gerektiği belirtilmektedir (Akt., Parlak, 2017).

2.2. Grup Çalışması: Öğretmenler Dijital Dönüşümde Eğitim Hakkını Nasıl Değerlendiriyor?

Modüllerde birden fazla etkinlik seçeneği sunulmuştur, uygun bulduğunuz etkinliği kullanabilirsiniz.



Geleneksel ve dijital ortamlarda eğitim hakkına ilişkin düşüncelerinizi 3-5 kişilik küçük gruplara ayrılarak tartışınız. Aşağıdaki soruları bu bağlamda inceleyiniz.

- Geleneksel ve dijital eğitim ortamlarında eğitim hakkını ihlâl eden durumlar neler olabilir?
- Geleneksel ve dijital eğitim ortamlarını düşündüğünüzde şimdiye kadar eğitim hakkının ihlâli ile ilgili ne tür durumlarla karşılaştınız?
- Geleneksel ve dijital ortamlar karşılaştırıldığında eğitim hakkı ihlâli hangi ortamda daha görünürdür?
- Bu tür eğitim hakkı ihlâllerine yönelik çözüm önerileriniz neler olabilir?
- Eğitim hakkını destekleyecek düşüncelerinizi sloganlaştırsaydınız bu slogan ne olurdu?

3. Kişisel Verilerin Korunması Hakkı

İnsan hakları; kişilerin doğuştan sahip olduğu dokunulmaz ve devredilmez haklar olarak kabul edilmektedir. Kişi özgürlükleri, bireyi devlete ve topluma karşı koruyan haklardır ve koruyucu haklar olarak ifade edilmektedir. Kişisel verilerin korunması, özel hayatın gizliliği temel hakkından (Kılınç, 2012) kaynaklanan bir hak olarak ele alınabilir. Kişisel veri, belirli ya da belirlenebilir nitelikteki bir kişiye ilişkin her türlü bilgi şeklinde tanımlanmaktadır (Akgül, 2016).

Bir kişinin yalnızca özel yaşamı hakkındaki değil, ekonomik ve mesleki bilgileri dâhil onun bütün bilgilerini içeren kişisel veri; özünde bireyin kimliğini ortaya çıkartan, bir kişiyi belirli kılan ve karakterize eden verilerdir. Kişinin adı, adresi, doğum tarihi, medeni hâli, tabiiyeti, mesleği, görüntüsü, kanaatleri, fotoğrafı, e-posta adresi, banka bilgileri, kimlik, emeklilik, kurum sicili ve vergi numarası, parmak izi, eğitim bilgileri, sağlık verileri, telefon mesajları, telefon rehberi, e-posta veya Facebook ve X gibi sosyal paylaşım sitelerinde yazdığı veya paylaştığı yazı, fotoğraf, ses veya görüntü kayıtları kişisel verileri olarak belirtilmektedir (Akgül, 2016, s. 13).

Kişisel verilerin korunması hakkının temel amacı, bireyin özel yaşamının gizliliğinin güvence altına alarak tutulan kayıtların korunması yoluyla bireyi korumaktır (Akgül, 2016).

Kişisel Verilerin Korunması Kurumu (KVKK, t.y.)’nun hazırladığı 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun amacı ve kapsamında belirtildiği üzere Kişisel Verilerin Korunması Kanunu’nun düzenlenmesindeki amaç:

- Kişisel verilerin işlenmesinde, kişilerin temel hak ve özgürlüklerini korumak,
- Kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek (disiplin altına almak),
- Kişilerin mahremiyetini korumak (özel hayatın gizliliği),
- Kişisel veri güvenliğini sağlamak olarak sayılabilir.

3.1. Dijital Ortamda Kişisel Verilerin Korunması Hakkı

Dijital teknolojilerin gündelik yaşantıda, sağlıkta, eğitimde aktif şekilde kullanılması bireylerin dijital ortamlara dâhil olmasına ve davranışta bulunmasına neden olmaktadır. Bireyler bu ortamlarda verilerini paylaşmaktadır. Dijital dönüşümün etkisiyle gelişen dijital ortamlarda kişisel verilerin korunması bir gereklilik olmaktadır.

UNICEF (2018)’in 6 Şubat 2018 tarihinde yaptığı açıklamaya göre her gün 175 bin civarı çocuk ilk kez internete girmekte, buna göre her yarım saniyede bir çocuk internete erişim sağlamaktadır. Tüm dünyada her üç internet kullanıcısından biri çocuktur. Dijital erişimin sağladığı faydalar ve olanaklar beraberinde riskleri ve ihlalleri de dikkate almak gerekmektedir. Bu riskler çocukların zararlı içeriklere maruz kalmaları, siber zorbalık ve kişisel bilgilerin kötüye kullanılması olarak sıralanabilir. Çocukları dijital ortamda koruma sorumluluğunun hükümetler, aileler, okullar ve başka diğer kurumlar olduğu belirtilmektedir. Tüm bu önlemler alındığında bile en önemli koruyucu yöntem çocukların dijital ortamlardaki kuralları öğrenmeleridir. Kendilerini dijital ortamlarda korumayı, haklarının farkında olmaları ve hem diğerlerinin kişisel alanlarına saygı göstermeleri hem de kendi kişisel bilgilerini korumaları gerektiği öğretilmelidir. Çocukların kişisel verilerinin paylaşımı, kaydedilmesi ve işlenmesi konusunda yaşları dolayısıyla rıza göstermelerine yönelik ehliyetleri bulunmamaktadır. Bu bağlamda çocukların dijital ortamda bulunmaları kişisel verilerinin paylaşımına, bu bilgilerin depolanmasına ve buna yönelik profiller çıkarılmasına neden olmaktadır. Bu profiller çocukların dijital okuryazarlık becerilerinin yeterli olmamaları nedeniyle üçüncü şahısların ticari kullanımı açısından bir risk faktörü oluşturmaktadır. Bunun yanında eğitim ve sağlık verilerinin paylaşımı da suistimale açık bir konudur (Esen Baygüneş, 2021). Diğer bir önemli konu ise sosyal medya kullanımında ebeveyn paylaşımıdır. “Paylaşan ebeveynlik (sharenting)” kavramı sosyal medyada ebeveynin çocuğuna ait bilgileri ve görselleri paylaşmasını ifade eden bir kavramdır. Ebeveynin çocuğunun rızasını gözetmeden mahremiyet ve güvenlik sınırlarını aşması tartışmalı bir durum yaratmaktadır. Ebeveynin bu geçici “paylaşımı” çocuk için uzun dönemde yetişkin yaşamını olumsuz etkileyecek durumlara neden olabilir (Esen Baygüneş, 2021).

3.2. Grup Çalışması: Kişisel Verileri Koruma

Kursiyerler iki gruba ayrılır. Her gruptaki öğrencilerin kullanması için bir kontrol listesi oluşturur. Grupların kontrol listelerini oluşturduktan sonra listeleri büyük grupta paylaşımları ve iki kontrol listesinin ortak yönleri üzerinde konuşmaları istenir.



- 1. Grup: Öğrencilerin günlük yaşamlarında kişisel verilerini korumak için alabilecekleri önlemlere yönelik bir liste hazırlar.
- 2. Grup: Öğrencilerin dijital ortamda kişisel verilerini korumak için alabilecekleri önlemlere yönelik bir liste hazırlar.

4. Bilgiye Erişim ve İletişim Hakkı

Bilgi Edinme ve Değerlendirme Kurumu (2021) bilgi edinme hakkını; “En basit anlamıyla bilgi edinme hakkı, bireylerin kamu kurum ve kuruluşlarının görevlerinden dolayı sahip oldukları bilgilere erişim hakkıdır.” olarak tanımlamıştır. Bilgi edinme hakkının düşünce ve ifade özgürlüğünün bir uzantısı olarak düzenlendiği veya ayrı bir hak olarak görülüp temel haklar kategorisine eklendiği belirtilmektedir (Yalçınkaya, t.y.). Bilgi edinme hakkı ile kuruluşlardan bilgi talep edilebilir, dilek, istek, şikâyetler de dile getirilebilir (BEDK, 2021).

İletişim hakkı; insanların yaşam alanlarını geliştirmelerini, her yerde kendilerini ifade edebilmelerini sağlayan haklardır. İletişim hakkı temel ve kapsayıcı olarak iki bakış açısıyla ele alınabilir. Temel bakış açısında, herkesin iletişim hakkına sahip olduğu vurgulanır. Kapsayıcı bakış açısında ise gerekli kaynaklara erişme özgürlüğü ve katılımcılık olarak ifade edilmektedir. İletişim hakkından bahsedebilmek için iletişim kaynaklarının herkesin temel ihtiyaçlarını karşılaması gerekmektedir (Şen ve Şen, 2015).

4.1. Dijital Ortamda Bilgiye Erişim ve İletişim Hakkı

Dijital ortamın gelişmesi ve yayılması sonucu bilgiye erişim ve bilgi kaynağı olarak internetten söz edilebilir. Dijital ortamda (internet aracılığıyla) sunulan ve kullanılan bilgi çeşitliliğinin artması hem bir sonuç hem de bir neden olarak değerlendirilebilir. Erişim yaygınlığı, maliyet düşüklüğü, interaktif katılım, zaman ve mekâna bağlı olmadan bilgi kaynağına dijital teknolojiler ile ulaşmak önemli hâle gelmiştir. İnternetin yaygınlığı ona bilgi kaynağı olarak erişilmesine, 2021 Ocak sonu itibarıyla dünyada düzenli internet kullanıcısı olan insan sayısının 4,66 milyara ulaşılmasına imkân sağlamakta ve bilgiye erişen bu grubun demografik özellikleri bakımında her yaşta insanı kapsadığını göstermektedir (Akkaya, 2021).

Çocukların dijital çağda bilgiye erişim, katılım ve iletişim hakkı bulunduğu ifade edilmektedir. Çocuğun katılım hakkı toplumsal ve kültürel alanda kendilerinin ve başkalarının yaşamını etkileyen konularda kendi görüşlerini belirtme olarak tanımlanabilir (Kaya, 2021). UNICEF (t.y.) Dijital Çağda Çocuk Hakları ile ilgili; “Katılımda ve hakların kullanılmasında çocuklar dijital medyanın sunduğu fırsatlardan yararlanabilirler ve de karşılaştıkları risklere karşı direnç geliştirebilirler. Bağlı dijital medya kullanıcıları olarak çocukların eleştirel düşüncelerine, kendi dillerini, görüşlerini, stratejilerini ilişkilerini ve ilgilerini geliştirmelerine izin verilmelidir.” olarak belirtmiştir.

4.2. Tartışma Çemberleri: Bilgiye Erişim ve İletişim

10 kişilik gruplar hâlinde bir iç ve bir dış çember olmak üzere iki tartışma çemberi oluşturunuz. Çember içinde bir katılımcıyla eşleşerek aşağıdaki sorular üzerine tartışınız.



- Çocukların bilgiye erişim, iletişim ve katılım haklarını sağlamak için neler yapılabilir?
- Çocukların dijital ortamlarda karşılaşacağı bilgiye erişim, iletişim ve katılım hakları açısından risk faktörleri neler olabilir?
- Bu risk faktörlerinin önlenmesi için eğitim ortamlarında neler yapılabilir?

5. Özel Gereksinimi Olan Bireylere Yönelik Haklar

Özel gereksinimi olan bireylerin topluma katılımını sağlamak için çeşitli kanunlarda düzenlemeler yapılmaktadır. Birleşmiş Milletlerin bu haklara ilişkin sözleşmesi;

- ✓ Tüm insan haklarının ve temel özgürlüklerin (herhangi bir ayrımcılık yapılmadan) özel gereksinimi olan bireyler için de geçerli olduğuna,
- ✓ Fırsat eşitliğine, sürdürülebilir kalkınma stratejilerinin parçası olması gerekliliğine,
- ✓ Özel gereksinimi olan bireylerin kendi içlerindeki çeşitliliğe kabul gösterilmesine,
- ✓ Her türlü destek, güçlendirme ve koruma ihtiyacına, kontrolüne, haklarına dünyanın her yerinde aynı saygının ve dikkatin gösterilmesine,
- ✓ Tüm katılımlarına, kalkınmalarına, yoksulluktan kurtulmalarına katkıda bulunulmasına,
- ✓ Bireysel varlık ve bağımsızlıklarına saygı gösterilmesine,
- ✓ İhmal, istismar ve kötü muamele risklerine karşı korunmalarına,
- ✓ Bilgiye eşit erişim, yaşam hakkı, yasa önünde diğer insanlarla eşit olma, bağımsız yaşam sürdürebilme, adalete erişebilme, düşünce ve ifade özgürlüğü, eğitim/sağlık/rehabilitasyona erişebilme, kültürel ve toplumsal yaşama katılım gibi hak ve özgürlüklere vurgu yapmakta (Akt., Temiz ve Yılmaz, 2021) ve “özel gereksinimi olma” kavramını birbirleriyle ilişkili haklar ve özgürlükler üzerinden açıklamaktadır (Temiz ve Yılmaz, 2021).

5.1. Dijital Ortamda Özel Gereksinimi Olan Bireylerin Hakkı

Dijital dönüşümün gerçekleştiği dijital çağda özel gereksinimi olan bireylerin bu hızla ayak uydurmaları ve sağlanan fırsatlardan yararlanmaları konusunda eşit haklara sahip olması gerekmektedir. Özel eğitim alanında yapılan dönüşümler ülkelerin ve kurumların kapasitelerine göre değişmektedir. Özel gereksinimi olan bireyler, özel gereksinimi olmayan bireylerle aynı anda ve aynı maliyetle aynı dijital içeriğe erişme konusunda vatandaşlık ve insani haklara sahiptir (Lazar ve Stein, 2017). Özel gereksinimi olan bireylerin bilgi çağına tam anlamıyla katılabilmesi için web erişilebilirliği gereklidir (Blanck, 2017). Dijital erişilebilirlik, özel gereksinimi olan bireylerin web siteleri, yazılımlar, mobil cihazlar ve e-okuyucular gibi elektronik bilgi kaynaklarına erişme becerisiyle ilgilidir (Elder, 2017). Eğitim, dijital teknolojilere erişilebilirlik sağlamak

açısından da önemlidir. İnsan haklarından temellenen eğitim hakkı kapsayıcı eğitim ile özel gereksinimi olan bireylere yayılır. Bilgi teknolojilerinin ilk ve orta dereceli okullara, kolejlere ve üniversitelere, yaşam boyu öğrenmeye ve yetişkinlere yönelik profesyonel eğitim ortamlarına entegre edilmesiyle özel gereksinimi olan bireylerin bu eğitim olanaklarına erişilebilirliği, kapsayıcı eğitimin sürdürülmesinin anahtarıdır (Ziegler ve Sloan, 2017). Özel gereksinimi olan bireylerin iletişim teknolojilerini kullanmasına yönelik toplumsal algı düşük olsa da aslında birçok uygulama ve proje ile dijital araçların ve internetin kullanımı yaygınlaştırılmaktadır (Akt., Oğuz Özgür, 2023). Özel gereksinimi olan bireylere yönelik ele alınan konular genel olarak bireylerin yaşadığı sorunlar, erişilebilirlik, eğitim ve sağlık alanında düzenlemeler ve çalışma hayatına dâhil olma konuları olarak belirlenmektedir (Akt., Oğuz Özgür, 2023).

5.2. Düşün-Eşleş-Paylaş: Özel Bir Yol Haritası



1. Düşün (Bireysel-3'): Özel gereksinimi olan bireylerin dijital dönüşüm hızına yetişebilmeleri ve potansiyellerini gerçekleştirebilmeleri için neler yapılabilir?
2. Eşleş (3'lü grup çalışması-7'): Grup üyelerinizle kendi görüşlerinizi paylaşın. Bu fikirlerinizin hangisini/hangilerini sınıflarınızda uygulayabilirsiniz? Uygulamak için nelere ihtiyaç duyarsınız?
3. Paylaş (Tüm katılımcılar-10'): Tartışma sonuçlarınızı tüm katılımcılarla paylaşın. Bu uygulamaları kullanarak geleneksel sınıf ortamını özel gereksinimi olan bireyler için nasıl dönüştürebilirsiniz?

6. Aileye ve Çocuğa Yönelik Haklar

Toplumun en temel yapı taşı olan birey, içinde bulunduğu sosyal çevreden hem etkilenir hem de onu etkiler. Bireyin geliştiği çocukluk yılları; kişilik, değerler, tutumlar ve davranışlar üzerinde belirleyicidir (Akt., Kesayak ve Karatekin, 2020). Bu nedenle bireyin bedensel, zihinsel ve ruhsal gelişimi, sağlıklı olması ve topluma katkı sunması, buna yönelik imkânların sağlanmasıyla gerçekleşebilir (Akt., Kesayak ve Karatekin, 2020). Çocukların gelişimlerini sürdürebilmek için çocuk haklarına saygılı bir ailesi olmalıdır (Akt., Kesayak ve Karatekin, 2020), fakat çocukların korunup ihtiyaçlarının karşılanmasında aileler yeterli olmadığı için (Akt., Kesayak ve Karatekin, 2020) çocuklara özel hakların verilmesinin gerekliliği ortaya çıkmıştır (Akt., Kesayak ve Karatekin, 2020). “Çocuk hakları, kanunen veya ahlâki olarak dünya üzerindeki tüm çocukların doğuştan sahip olduğu; eğitim, sağlık, yaşama, barınma; fiziksel, psikolojik veya cinsel sömürüye karşı korunma gibi haklarının hepsini birden tanımlamakta kullanılan evrensel kavramdır (İstanbul Üniversitesi Çocuk Koruma Uygulama ve Araştırma Merkezi, (t.y.).”

Çocuk Hakları Sözleşmesi'nin dört ana ilkesi hakların tamamının uygulanması için temel gereklilikleri ifade eder. Bu ilkeler aşağıda belirtilmiştir (UNICEF, 1989);

AYRIMCILIK YAPMAMA, tüm çocukların hakları.

ÇOCUĞUN ÜSTÜN YARARI, her eylemde çocuğun yararı önceliklidir.

ÇOCUĞUN VARLIĞINI VE GELİŞİMİNİ SÜRDÜRME, her çocuğun doğal olarak yaşama hakkı vardır.

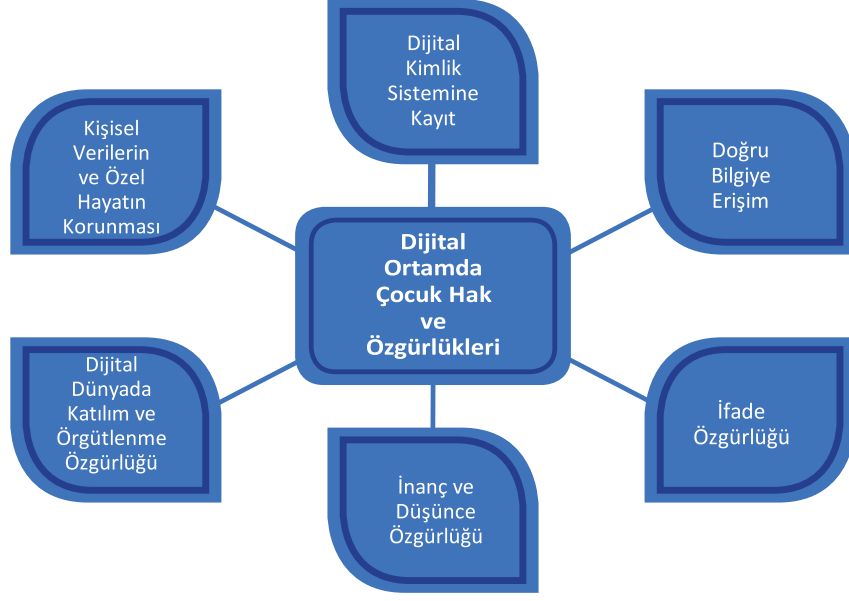
KATILIM, her çocuğun kendi ilişkin kararlarda ve genel durumlarda düşüncesini ifade etme hakkı vardır.

Ailenin haklarından bahsederken “Aile hayatına saygı hakkı” kavramı dikkate alınmaktadır. Bu hak, T.C. Anayasası 20. maddesinde “Özel Hayatın Gizliliği” başlığı altında düzenlenmiştir. Bu maddeye göre, “Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz” olarak tanımlanmıştır. “Ailenin Korunması ve Çocuk Hakları” başlığı altında düzenlenen 41. madde ailenin toplumun yapı taşı olduğunu kabul ederek devlete; aile hayatında huzurun sağlanması, özellikle anne ve çocukların korunması için tedbir alma yükümlüğü vermektedir (Usta, 2022). Böylece aile çocuk haklarının yerine getirilmesiyle yükümlüken devlet hem ailenin hem de çocukların haklarını gözeten tedbirlerle yükümlüdür.

6.1. Dijital Ortamda Aileye ve Çocuğa Yönelik Haklar

Toplumsal ve çevresel dönüşümler hem yetişkinleri hem de çocukları etkilemektedir. Dijital dönüşümün hızlandığı bu çağda çocukların ve yetişkinlerin hak ve sorumlulukları da bu doğrultuda hızla değişmektedir. Dijital dünya; insan yaşamında yarattığı etki ile sosyal, ekonomik, siyasal ve kültürel yapıyı dönüştürerek (Akt., Sağlam, 2024) çocukların davranışlarını ve bakım verenin ebeveynlik şekillerini de değiştirmektedir. Ebeveynlik çocukların fiziksel ve sosyal ihtiyaçlarına yönelik tutumlar, algılar, beklentiler, bilgiler, değerler ve eylem yönelimlerinden oluşan bir inanç sistemidir (Sağlam, 2024). “Dijital çağ dönemi içerisinde teknolojinin doğru kullanılmasını çocuklarına öğretebilen, onlara rehberlik eden anne ve babalara ‘dijital ebeveyn’ denir.” (Deniz, 2023). Dijital ortamların ve teknolojilerin, çocuklardaki olumsuz etkilerini en aza indirmeye ve aracılık etmek için kullanılan ebeveynlik becerilerine “ebeveyn aracılığı” denilmektedir. Dijital dönüşümün yarattığı karmaşıklık, ebeveynleri ikilemli bir durumda bırakmıştır. Bir yandan eğitim ve sosyalleşme için dijital medyayı kullanmalarını desteklerken diğer yandan oluşacak riskleri ve olumsuz etkileri engellemeye çalışmaktadırlar (Sağlam, 2024). Bu bağlamda çocukların haklarını gözeterek onların dijital ortamda sağlıklı bir şekilde var olabilmelerini sağlamak için ebeveynin hem “dijital ebeveyn” olması hem de “ebeveyn aracılığı” yapabilmesi önemlidir.

Birleşmiş Milletler Çocuk Hakları Komitesi çocukların dijital dünyadaki haklarını anlatmak için 24 Mart 2021’de Genel Yorum 25’i yayımladı. Bu belgede belirtilen dijital ortamda çocuk hakları aşağıdaki şekilde gösterilmiştir (UNICEF, 2024).



6.2. İnceleme: Dijital Ortamlarda Çocuk Hakları ile İlgili Genel Yorum No.25



Birleşmiş Milletler Çocuk Hakları Komitesinin [Çocukların Dijital Dünyadaki Hakları](#) ile ilgili Genel Yorum 25'i okuyunuz.

- “Dijital ebeveyn” kavramı bağlamında çocukların hak ve özgürlüklerini dijital ortamda kullanmalarını nasıl sağlayabilirsiniz?
- Dijital dünyada öğrenciler için sınıflarınızda “ebeveyn aracılığı” kavramını “öğretmen aracılığı”na dönüştürmek için ne tür uygulamalar yapabilirsiniz?
- Aile ve eğitim ortamında ne tür eş zamanlı önlemler dijital dünyada çocukların hem haklarını kullanmayı hem de korumayı öğrenmelerine yardımcı olur?

KAYNAKÇA

- Akgül, A. (2016). Kişisel verilerin korunmasında yeni bir hak: “Unutulma Hakkı” ve AB Adalet Divanı’nın “Google Kararı”. Türkiye Barolar Birliği Dergisi, 116, 12-38
- Akkaya, M.A. (2021). Bilgi kaynağı ve bilgiye erişim aracı olarak internet algısı: Kuşaklararası yaklaşım farklılığının karşılaştırılması. Bilgi Yönetimi Dergisi, 4(2), 222-239
- Bayzan, Ş. (2019, 6 Kasım). Dijital Hak ve Sorumluluklarımız Nelerdir? 17 Ekim 2024 tarihinde <https://www.guvenliweb.org.tr/haber-detay/dijital-hak-ve-sorumluluklarimiz-nelerdir> adresinden edinilmiştir.
- Bilgi Edinme ve Değerlendirme Kurulu, (2021). 25 Soruda bilgi edinme hakkı. <https://cdn.bartın.edu.tr/personel/5befd0afd1b74cd2936a909c89f8ccb9/287202113133525-soruda-bilgi-edinme-hakki.pdf> adresinden edinilmiştir.
- Binbir, Ü. ve Arastaman, G. (2021). Eğitim hakkı: Bir sistematik derleme çalışması. OPUS–Uluslararası Toplum Araştırmaları Dergisi, 18 (Eğitim Bilimleri Özel Sayısı), 5067-5098. DOI: 10.26466/opus.898503.
- Blanck, P. (2017). Web Accessibility for People with Cognitive Disabilities: A Legal Right? In J. Lazar & M. A. Stein (Eds.), Disability, Human Rights, and Information Technology (pp. 41–57). University of Pennsylvania Press. <http://www.jstor.org/stable/j.ctv2t4d02.7>
- Council of Europe. (t. y.) Rights and responsibilities. 17 Ekim 2024 tarihinde <https://www.coe.int/en/web/education/rights-and-responsibility> adresinden edinilmiştir.
- Deniz, M.E. (2023, Ocak). Dijital ebeveynlik. 22 Ekim 2024 tarihinde <https://tesam.org.tr/wp-content/uploads/2023/02/Mehmet-Engin-Deniz.pdf> adresinden edinilmiştir.
- Elder, T. (2017). Open Government and Digital Accessibility. In J. Lazar & M. A. Stein (Eds.), Disability, Human Rights, and Information Technology (pp. 125–140). University of Pennsylvania Press. <http://www.jstor.org/stable/j.ctv2t4d02.12>
- Esen Baygüneş, M. (2021, Ocak). Dijital ortamda çocukların kişisel verilerinin korunması. Başkent Üniversitesi Hukuk Fakültesi Dergisi, 7(1), 165-182.
- İstanbul Üniversitesi Çocuk Koruma Uygulama ve Araştırma Merkezi. Çocuk hakları. 22 Ekim 2024 tarihinde <https://cocukkoruma.istanbul.edu.tr/tr/content/cocuk-haklari-unicef/cocuk-haklari> adresinden edinilmiştir.
- Kaya, L. (2021, 16 Kasım). Katılım, ifade, bilgiye erişim: Çocukların 3 temel hakkı ve dijital medya. 21 Ekim 2024 tarihinde <https://dijitalmedyavecocuk.bilgi.edu.tr/2021/11/16/katilim-ifade-bilgiye-erisim-cocukların-3-temel-hakki-ve-dijital-medya/> adresinden edinilmiştir.
- Kesayak, Y. ve Karatekin, K. (2020) Ebeveynlerin ailede çocuk haklarını uygulama düzeylerinin incelenmesi. Türkiye Bilimsel Araştırmalar Dergisi, 5(2), 313-335.
- Kılınç, D. (2012). Anayasal bir hak olarak kişisel verilerin korunması. Ankara Üniversitesi Hukuk Fakültesi Dergisi, 61(3), 1089-1169
- Kişisel Verileri Koruma Kurumu, (t.y.). 6698 Sayılı Kişisel Verilerin Korunması Kanununun Amacı ve Kapsamı. 18 Ekim 2024 tarihinde <https://www.kvkk.gov.tr/lcerik/4185/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanununun-Amaci-ve-Kapsami> adresinden edinilmiştir.
- Lazar, J., & Stein, M. A. (2017). Introduction. In J. Lazar & M. A. Stein (Eds.), Disability, Human Rights, and Information Technology (pp. 1–8). University of Pennsylvania Press. <http://www.jstor.org/stable/j.ctv2t4d02.4>
- Millî Eğitim Bakanlığı, (2024). Türkiye Yüzyılı Maarif Modeli. <https://tymm.meb.gov.tr/upload/brosur/2024programortakmetinOnayli.pdf> adresinden edinilmiştir.
- Oğuz Özgür, H. (2023). Engelli bireylerin güncel tehdit alanı: Çevrim içi dünya. M.Ö. Kalaç ve V. Tecim (Ed.), Engelsiz Bilişim 2023: Engelsiz Dijital Dönüşüm içinde (s. 27-47). Kriter Yayınevi.
- Parlak, B. (2017). Dijital çağda eğitim: olanaklar ve uygulamalar üzerine bir analiz. Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 22 (Kayfor15 Özel Sayısı), 1741-1759.

Sağlam, T. (2024). Çocuklarda teknoloji kullanımı ve dijital ebeveynlik. *Birey ve Toplum Sosyal Bilimler Dergisi*, 14(1), 123-129. DOI: 10.20493/birtop.1496639

Şen, A. F., ve Şen, Y. F. (2015). Sosyal medya, iletişim hakkı ve ifade özgürlüğü üzerine bir değerlendirme. *Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 17(2), 122-136.

Temiz, N. ve Yılmaz, B. (2021) Türkiye’de ilk ve orta öğretimde özel gereksinimli öğrencilere yönelik eğitim politikalarının incelenmesi. *Yaşadıkça Eğitim*, 35(1), 104-131.

Türk Dil Kurumu (t. y.) Türk Dil Kurumu Sözlükleri. 17 Ekim 2024 tarihinde <https://sozluk.gov.tr/> adresinden edinilmiştir.

UNICEF (2024). Dijital ortamlarda çocuk hakları ile ilgili genel yorum no.25. 22 Ekim 2024 tarihinde <https://www.unicef.org/turkiye/media/17626/file/Dijital%20Ortamlarda%20%C3%87ocuk%20Haklar%C4%B1%20ile%20%C4%B0lgili%20Genel%20Yorum%20No:%2025.pdf> adresinden edinilmiştir.

UNICEF Türkiye Milli Komitesi, (1989). Çocuk hakları hakkında. 22 Ekim 2024 tarihinde <https://www.unicefturk.org/yazi/cocuklar-icin-bilgi> adresinden edinilmiştir.

UNICEF Türkiye Milli Komitesi, (2018, 6 Şubat). Çocukları dijital dünyada koruma yükümlülüğü. 21 Ekim 2024 tarihinde https://www.unicefturk.org/yazi/-internetgunu?gad_source=1&gclid=CjwKCAjw1NK4BhAwEiwAVUHPUPaDZckyD8taMhaOjs_-ZLWBIEUEyi23aswMzZS6EcZcp7gsqZ5HVhoCbHYQAvD_BwE adresinden erişilmiştir.

UNICEF, (t. y.). Dijital çağda çocuk hakları. 21 Ekim 2024 tarihinde https://www.unicef.org/turkiye/media/2606/file/TURmedia_Dijital%20Cagda%20Cocuk%20Haklari.pdf%20.pdf adresinden edinilmiştir.

Usta, Ö. (2022). Aile hayatına saygı ve aile hayatının korunması hakkı bağlamında ele alınan birkaç kurum üzerine inceleme. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, 30(3), 1561-1590.

Yalçinkaya, B. (t. y.) Bilgiye erişim ve sürdürülebilir kalkınma. UNESCO Dünya Belleği Programı. 21 Ekim 2024 tarihinde https://www.unesco.org.tr/Content_Files/Content/buyukbulusmalar/3bb/i5.pdf adresinden edinilmiştir.

Yıldırım, S. ve Keser, H. (2022). Dijital hak ve sorumluluklar ölçeği geliştirme çalışması. *Pamukkale Üniversitesi Eğitim Fakültesi Dergisi (PAUEFD)*, 61, 414-437.

Yılmaz, N. (2014). Yönetici ve sınıf öğretmenlerinin dijital vatandaşlık algı düzeyleri ile bilgi okuryazarlığı algı düzeyleri arasındaki ilişki. [Tezsiz Yüksek Lisans Projesi, Pamukkale Üniversitesi]. Pamukkale Üniversitesi Açık Erişim Sistem. <https://gcris.pau.edu.tr/handle/11499/56582>

Ziegler, M. J., & Sloan, D. (2017). Accessibility and Online Learning. In J. Lazar & M. A. Stein (Eds.), *Disability, Human Rights, and Information Technology* (pp. 158–181). University of Pennsylvania Press. <http://www.jstor.org/stable/j.ctv2t4d02.14>

MODÜL 10

Yetişkin Eğitimi ve Mahallî Eğitimler



Öğrenme Kazanımları

- Hizmet içi eğitimlerin öğretmenlerin mesleki gelişimine katkısı hakkında bilgi sahibi olacak.
- Yetişkinlerin öğrenme süreçleri hakkında bilgi sahibi olacak.
- İletişim becerilerinin öneminin farkına varmak.
- Öğretmenlerin mesleki gelişiminde yeni yaklaşımlar konusunda bilgi sahibi olacak.
- Mahalli öğretmen eğitimlerinde izlenmesi gereken adımların farkına varmak.

1. Giriş

Hayat boyu öğrenme kavramı, günümüzde giderek daha fazla önem kazanmaktadır. Sürekli olarak mesleki ve bireysel gelişimlerini desteklemek ve güncel gelişmelere ayak uydurmalarını sağlamak önemli bir gereklilik hâline gelmiştir.

Okul yöneticileri ve öğretmenler; bir eğitim sisteminde eğitim politikalarını, reformları, öğretim programını, teknolojik gelişmeleri öğrencilerle buluşturan ve bu yenilikleri uygulamaya taşıyan kişilerdir. Hizmet içi eğitim faaliyetleri, eğitimcilerin mesleki becerilerini güncellemesine ve genişletmesine olanak tanır. Bu eğitimler, personelin bilgi birikimini artırırken aynı zamanda yeni teknikleri ve yöntemleri öğrenmelerine olanak sağlar.

Nitelikli öğretmen ve nitelikli öğretim için meslekî gelişim konusunda öğretmenlere ve okul yöneticilerine sürekli destek sağlanması gerekmektedir. Bu itibarla öğretmenlerin ve okul yöneticilerinin profesyonel gelişimleri için hizmet içi eğitim faaliyetleri düzenlenmekte, kişisel ve mesleki gelişim programları uzman kişi ve kurumların desteği ile geliştirilerek hizmet içi eğitimler kapsamında uygulanmaktadır.

Öğretmenlerin mesleki gelişimleri kapsamında eğitim ve öğretimde kullanılan yeni yaklaşımda; yöntem ve teknikler konusunda bilgilendirilmesi, mesleki bilgi ve becerilerine yönelik yeterliklerinin artırılması, yeni teknolojilerin ve teknolojik ortamların kullanımına yönelik becerilerinin geliştirilmesi öncelikli konular arasında yer almıştır.

Hizmet içi eğitim faaliyetleri, öğretmen ihtiyaç analizleriyle belirlenen mesleki gelişim alanları yanında Millî Eğitim Bakanlığının politika ve öncelikleri ile üst politika belgelerinin işaret ettiği alanlar doğrultusunda planlanmakta ve yürütülmektedir.

2. Öğretmenlerin Mesleki Gelişiminde Yeni Yaklaşımlar

Günümüzde dünyanın farklı ülkelerinde öğretmenlerin mesleki gelişimlerini sağlamak amacıyla yeni yaklaşımlar uygulanmaktadır. Bu kapsamda ülkemizde de hizmet içi eğitim faaliyetleri standart eğitim programları doğrultusunda kurs ve seminer faaliyetleri olarak dü-

zenlenmekte iken 11 Mart 2022 tarihinde yürürlüğe giren “Millî Eğitim Bakanlığı Personeli Hizmet İçi Eğitim Yönetmeliği¹” kapsamında “Öğretmen-yönetici hareketlilik programları”, “Okul temelli mesleki gelişim (OTMG) programları”, “Mesleki gelişim toplulukları (MGT)” şeklinde de yapılmaya başlanmıştır. Bu yeni yaklaşımlar, öğretmenlerin mesleki gelişimlerini desteklemek amacıyla kurulan Öğretmen Bilişim Ağı’nda (ÖBA) hizmete sunulmaktadır.

- 2.1. Okul Temelli Mesleki Gelişim (OTMG):** Okul tarafından belirlenen ve o okula özgü olan eğitim ihtiyacının karşılanması amacıyla mahallî hizmet içi eğitim planı kapsamında düzenlenen hizmet içi eğitim faaliyetleridir.
- 2.2. Mesleki Gelişim Toplulukları (MGT):** Okuldaki eğitim öğretim uygulamalarını geliştirmek, katılımcıların mesleki bilgi ve becerilerini artırmak, birbirlerinden ve uygulamadan öğrenerek mesleki gelişimlerini sağlamak amacıyla düzenlenmektedir. Mesleki gelişim topluluklarının topluluk içi iletişimi ve yapılan çalışmaların paylaşımı ÖBA üzerinden yapılmaktadır.
- 2.3. Öğretmen-Yönetici Hareketlilik Programı:** Bu program; başarısı, iyi uygulamaları, farklı projeleri veya farklı öğrenme ortamları ile ön plana çıkan okulların bilgi ve tecrübelerinin paylaşılması ile diğer okullarda görev yapan öğretmen ve yöneticilerin bu okulları ziyaretini sağlamak amacıyla düzenlenmektedir.

3. Yetişkin Eğitiminde Dikkat Edilmesi Gerekenler

Yetişkinlerin yaşına ve ilgi alanlarına uygun, anlamlı öğrenme deneyimleri yaratmak önemlidir. Teorik bilgiler yerine, pratik ve uygulanabilir bilgiler sunmak daha etkili olacaktır. Özellikle iş yaşamında karşılaşılan durumlara ve sorunlara çözüm öneren örnekler kullanmak, öğrenme sürecini daha verimli kılar. Yetişkinler, pasif alıcı olmaktan hoşlanmazlar. Oyunlar, ekip çalışmaları ve problem çözme egzersizleri ile aktif katılım sağlanmalıdır. Öğrenmenin büyük bir kısmı görsel öğelerle gerçekleşir. Bilginin estetik ve görsel olarak ilgi çekici bir şekilde sunulması, akılda kalıcılığı artırır. Çözüm üretmelerine imkân verecek sorular sormak, ilgiyi canlı tutar ve düşünmeye teşvik eder.

İletişim Becerileri

Yetişkin eğitiminde etkili iletişim becerileri eğitim sürecini etkili ve verimli kılmak için oldukça önemlidir. Özellikle eğitim sırasında aktif dinleme, empati kurma, açık ve net ifade, geri bildirim verme ve beden dilinin kullanımı konularına dikkat edilmesi gerekir.



Etkinlik

Aşağıda verilen etkinliği iletişim becerilerinin önemini kavratmak için katılımcılarla beraber uygulayabilirsiniz.

Sinyal Oyunu: İletişim kurarken yaşadığımız problemlere dikkat çekmek için katılımcıların grup olarak oyunu yöneten kişi tarafından verilen sinyali en hızlı şekilde grubun başındaki arkadaşlarına iletmeye çalıştığı bir oyundur. Oyuna başlamadan önce;

- 1) Sınıfta bulunan katılımcıları iki gruba ayırınız (maksimum on beşer kişilik).
- 2) Her grubun sandalyeler yardımıyla tek düze sıralanarak oturmalarını sağlayınız.
- 3) En önde bulunan iki sandalyenin bir metre önüne katılımcılara eşit mesafe uzaklıkta sinyal verildiğinde kalkıp almaları için bir şişe vb. bir eşya koyunuz.
- 4) Tüm katılımcıların, önünde bulunan katılımcının omzuna elini uzatmasını isteyiniz.
- 5) En arkada bulunan katılımcıların arasına oturarak bir madeni parayı havaya atıp yazı ya da tura gelme durumuna göre oyuncuların öndeki oyuncuya madeni paranın yazı gelmesi durumunda oyuncunun omzunu sıkması gerektiğini, tura geldiğinde ise bir şey yapmamaları gerektiğini belirtiniz.
- 6) Her bir oyuncunun bir öndeki oyuncunun omzunu sıkarak en baştaki oyuncuya en hızlı şekilde ulaştırması gerekmektedir.
- 7) En önde bulunan oyuncular sinyali aldıklarında önlerinde bulunan cismi almaya çalışacak. İlk alan grup bir sıra öne kayarak ilerleyebilecek. İlk başlayan oyuncu tekrar en öndeki sıraya geldiğinde oyun tamamlanmış olacak.

Oyun sonrasında katılımcılardan yaşadıkları zorlukları ve yanlış anlamaları paylaşmaları istenerek “iletişim sürecinde” yaşanabilecek tüm etkenleri değerlendirebilirsiniz.

Yetişkin Eğitiminde İletişim Araçları

Yetişkin eğitiminde, geleneksel eğitim araçlarının yanı sıra yetişkin öğrenenlerin ihtiyaç ve ilgi alanlarına uygun çeşitli dijital iletişim araçları kullanılır. Bu araçlar, yetişkinlerin bilgi ve becerilerini geliştirmelerine yardımcı olmak için önemli bir rol oynar.



Etkinlik

Yetişkin eğitiminde kullanılabilecek dijital araçlarla ve bu araçların nasıl kullanılacağıyla ilgili katılımcıların görüşlerini almak için bir beyin fırtınası yapınız. Bu beyin fırtınasını bir dijital araç üzerinden yapmayı unutmayınız.

4. Mahallî Öğretmen Eğitimleri

Mahallî öğretmen eğitimleri, il milli eğitim müdürlüklerinde hizmet içi eğitimlerden sorumlu şube müdürleriyle birlikte planlanmaktadır. Eğitici eğitimini alan öğretmenlerimizin illerinde bulunan şube müdürleriyle birlikte planlama sürecine katılarak illerinde Dijital Vatandaşlık eğitimlerini vermeleri beklenmektedir.

Eğitim Sırasında

Eğitim planlamaları yapıldıktan sonra eğitimcilerin belirlenen tarih ve katılımcılarla kursun mesleki gelişim programına uygun bir şekilde eğitim vermeleri beklenmektedir. Kurs için hazırlanan bu modüllerin eğitimcilere yol gösterici olmalarının yanı sıra katılımcıların eğitime gelmeden önce Öğretmen Bilişim Ağı (ÖBA)’nda yer alan “Dijital Vatandaşlık Eğitimi” kursunu da tamamlamaları için yönlendirme yapabilirsiniz. Bu, katılımcıların teorik bilgileri çevrim içi olarak tamamlamaları konusunda yardımcı olacaktır.

