AİLE OKULU PROJESİ

BİLİNÇLİ VE GÜVENLİ TEKNOLOJİ KULLANIMI

İÇİNDEKİLER

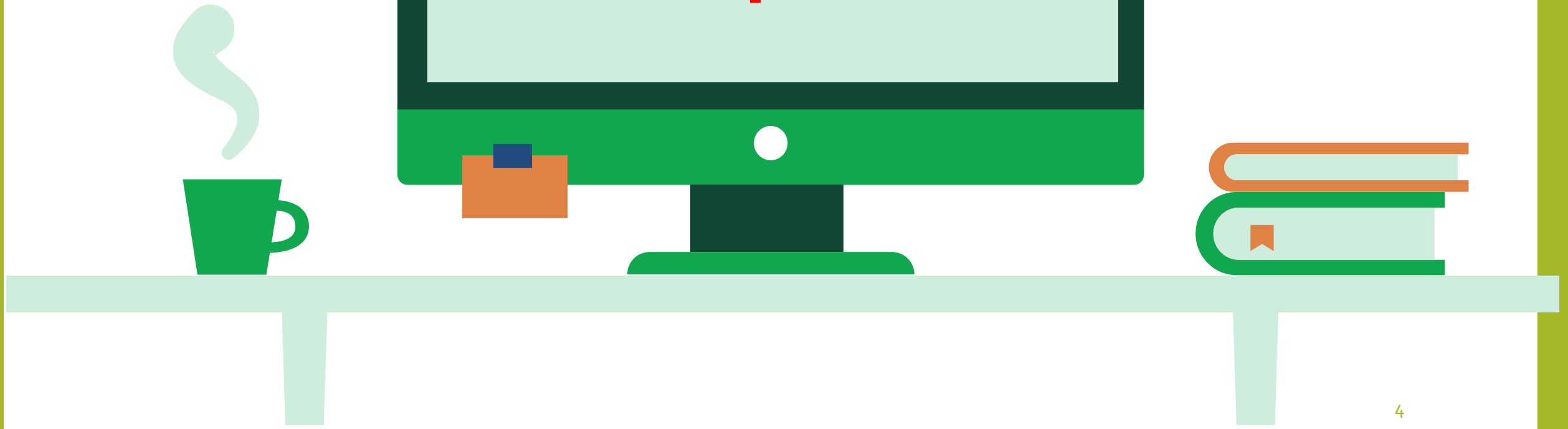
Dijitalleşme

Dijitalleşme ile birlikte;

- **internet,**
- **akıllı telefonlar,**
- **yapay zekâ uygulamaları,**
- **siber güvenlik,**
- **sosyal medya**

gibi kavramlar gündelik yaşantıları önemli ölçüde etkilediği görülmektedir.

İnternet ile Neler Yapabiliriz?




Dizi/film/video izlemek
Oyun oynamak
Bilgilenme
İçerik Üretme
Sosyal Medya
Ürün alma / satma
Eğitim (alma/verme)
E-vatandaşlık
Ürünlerle ilgili bilgi sahibi olma
İletişim
Eğlence
Araştırma Yapma

İnternet: Yararlı mı? Zararlı mı?

İnternetin birçok farklı kullanım alanı vardır. Güvenli ve doğru bir şekilde kullandığımızda bu kullanım alanları bize pek çok fayda sağlar. Uygun sınırlarda kullanmadığımızda ise bazı risklerle karşılaşabiliriz.

İnterneti Doğru Kullanma Kılavuzu

Dijital dünyadaki risklerle baş edebilmek, çevrimiçi ortamlarda daha güvenli şekilde hareket edebilmek için bazı becerilere sahip olmalıyız.

Bu beceriler:

Dijital vatandaşlığı kavramak ve uygulamak,

Dijital dünyanın **sorumlulukları**nı fark etmek,

Dijital **okuryazar** olabilmek,

Siber zorbalığın farkında olmak.

Ülkemizde sosyal medya kullanımı

- Türkiye'deki internet kullanıcılarının internette günlük olarak harcadığı ortalama zaman **8 saat.** Bunun mobil cihazlarda geçirilen süresi 4 saat 16 dakika, bilgisayarlarda geçirilen ise 3 saat 44 dakika.
- Türkiye, tüm dünyada sosyal medyayı en aktif kullanan 6. ülke konumunda. Dünyada sosyal medyayı en aktif kullanan ülkelerse Brezilya, Hindistan, Endonezya, Filipinler, Malezya, Türkiye ve Çin.
- Sosyal medya kullanıcılarının **nüfusa oranı ülkemizde %80 oranında.**
- İnternet kullanıcılarının sosyal medyada harcadığı zaman ortalama **2 saat 27 dakika.**

Neden paylaşım yaparız?

- yetkinlik duygusu,
- öğrenme isteği,
- kişisel çıkar,
- fedakârlık,
- empati,
- sosyal angajman,
- topluluk ilgisi,
- etkileşim
- itibar

Fotoğraf/video paylaşımı

Yapılan bir araştırmada **internet kullanıcılarının sadece %7'si dijital ortamda bilgilerini paylaşmıyor**. (66 Milyon internet – 60 Milyon sosyal medya kullanıcısı var)

Paylaşımların en çok olduğu konular:

- %87 yapılan **seyahat**e ilişkin video ve resimler,
- %82 ile başka şeylere ait ve hassas veri içermeyen video ve resimler,
- %70 ile **çocuğunun** video ve resimleri

Yaş oranı düştükçe daha fazla paylaşım yapılıyor. 16-24 yaş arası paylaşım yapan gençlerin sayısı ile 55 yaş üzeri paylaşım yapan yetişkinler arasında oransal olarak aşırı bir fark bulunmamaktadır.

Bilgilerini paylaşmayan kullanıcıların bilgilerini paylaşan kullanıcılara oranla akıllı telefon ve bilgisayarlarında daha az veri kayıpları yaşamaktadır.

Tatildeyim, ev boş MESAJI VERMEYİN!

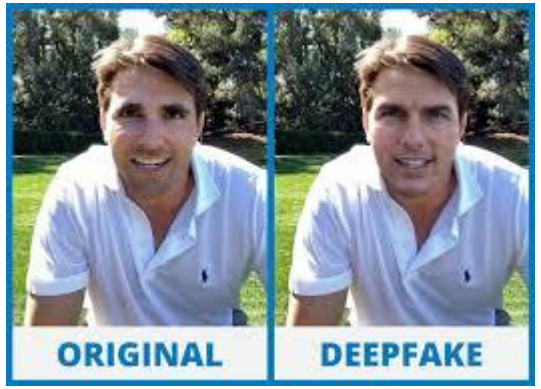
- Ev adresinizi ya da evde olmadığınızı siber korsanlara bildiriyorsunuz.

Phishing (oltalama)

- Bir öğretmen değerlendirme sitesinde sizinle ilgili çok kötü ifadeler yazılmış!
- Mavi Tık alamaya hak hazandınız!
- Telif haklarını uygun davranmadınız…
- Borsada para kazandırıyoruz….
- Kombine bilet kazanma şansı…
- Bedava tatil kazandınız…
- Devlet …. konusunda yardım yapacaktır. Sizde yararlanmak istiyorsanız…

Deepfake

- Yapay zeka ile derin öğrenme ve sahte sentetiklik, görsel-işitsel, yüzlerin manipüle edildiği (bir başkasını temsil etmek için) veya konuşmanın (kişinin aslında söylemediği bir şeyi söylemesini sağlamak) kullanıldığı materyallerdir. Görsel-işitsel içerikler insanların hala en çok güvendikleri kaynaklardır- bu nedenle, daha fazla aldatma potansiyeli vardır.



Algı Operasyonları

- Algı yönetmenleri ve manipülatörlerin bilgiyi işlemden geçirirken başvurdukları bir diğer teknik vurgulamadır. Bir haberde neyin öne çıkarılacağı, hangi hususun vurgulanıp manşete taşınacağı, hangi bilginin önemsizleştirileceği dikkatle hesaplanmaktadır.
- Mesela şöyle bir haberle muhtemelen hiç karşılaşmamışsınızdır: ***"Elektrik Mühendisinin Kızı Hızlı Araba Sürmekten Ceza Aldı."***

Doğru Bilgiye Nasıl Ulaşırız?

Yapılan çeşitli araştırmalara göre:

Yanlış bilgi içeren paylaşımlar insanlara doğru bilgi içeren paylaşımlardan **6 kat** daha hızlı ulaşıyor.

Gerçek haberler, 1000 sosyal medya kullanıcısından daha fazla kişiye nadiren ulaşırken yanlış bir haber rutin olarak **10 binden** fazla kişiye ulaşıyor.

Bilişim Suçu / Siber Suç

TCK'daki Bilişim Suçları

5237 sayılı TCK (Türk Ceza Kanunu), "Bilişim Alanında İşlenen Suçlar" başlığı altında tüm bilişim suçlarını 243 ile 245 maddeleri arasında düzenlemiştir.

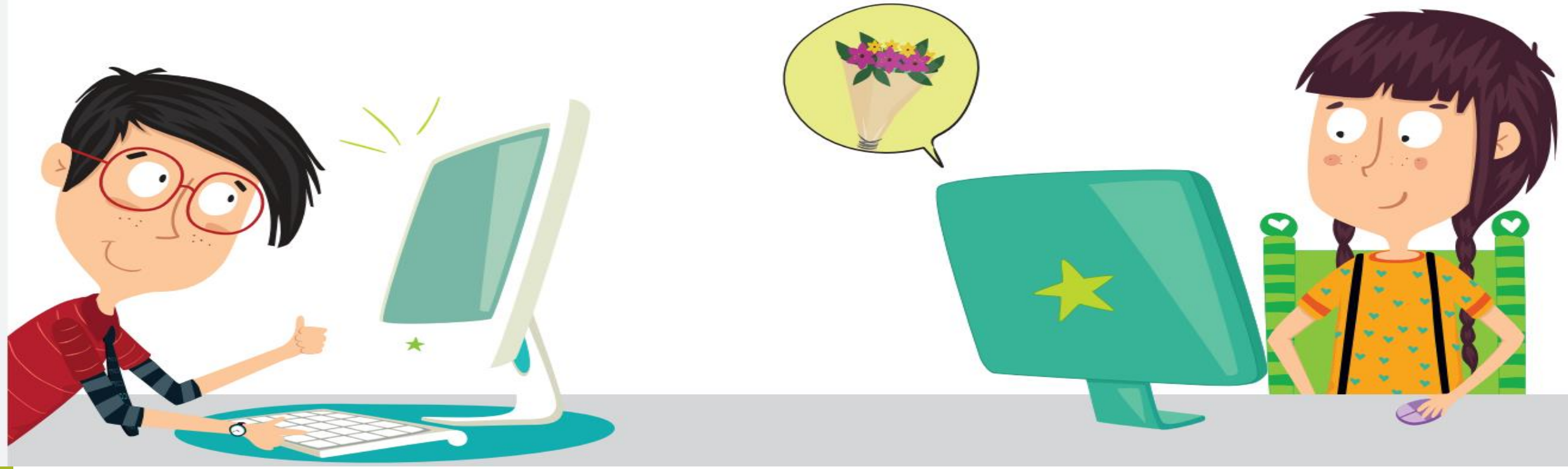
5237 sayılı TCK'da düzenlenen bilişim suçları şunlardır:

- *Bilişim sistemine girme suçu* (TCK m.243),
- *Sistemi Engelleme, Bozma, Erişilmez Kılma, Verileri Yok Etme veya Değiştirme Suçu* (TCK m.244),
- *Banka veya kredi kartının kötüye kullanılması suçu* (TCK m.245),
- *Yasak cihaz veya program kullanma suçu* (TCK m.245/a).

Başvuracağınız bazı kurum ve kuruluşlar:

1) İnternet Yardım Merkezi
http://www.internetyardim.org.tr/
2) Siber Suçlarla Mücadele
http://siber.pol.tr
3) Bilgi İhbar Merkezi
http://www.ihbarweb.org.tr
4) Tüketici Bilgi Sistemi
https://tuketicisikayet.btk.gov.tr/
5)Güvenli İnternet Merkezi
https://www.gim.org.tr/

İNTERNET ETİĞİ NEDİR?



İNTERNET'İ İNSANLARA ZARAR VERMEK İÇİN KULLANMAMALIYIZ.

BAŞKALARININ İNTERNET'TE YAPTIĞI ÇALIŞMALARA ENGEL OLMAMALIYIZ.

BAŞKALARININ GİZLİ VE KİŞİSEL DOSYALARINA ULAŞMAMALIYIZ.

İNTERNET'İ YALANCI ŞAHİT OLARAK KULLANMAMALIYIZ.

ÜCRETİNİ ÖDEMEDİĞİMİZ YAZILIMLARI KULLANMAMALIYIZ.

İnterneti Güvenli Kullanım İçin İpuçları

İnternette veya sosyal medya hesaplarında kişisel bilgilerini (T.C. kimlik no, telefon, adres, yaş, aile bilgileri vb.) hiçbir şekilde paylaşmamalısın.

Kullandığın şifrelerin sadece senin anlayabileceğin güçlü şifreler olabilmesi için sayı, harf ve sembolleri birlikte kullanmaya çalışabilirsin.

Dosya ya da program indirme gibi işlemleri bilinen ve güvenli internet sitelerinden yapabilirsin. Tanımadığın kişilerden ya da internet sitelerinden gelen mesajları açma ve linkleri tıklamadığından emin ol.

İnterneti Güvenli Kullanım İçin İpuçları

Hesap gizlilik ayarlarını değiştirerek kimlerin profilini görebileceğine, sana doğrudan mesaj gönderebileceğine veya gönderilerine yorum yapabileceğine karar verebilirsin.

İnternette veya sosyal medyada yeni arkadaşlar edinirken dikkatli ol. Tanımadığın kişiler arkadaşlık teklifinde bulunduğunda kabul etmemek daha güvenli olacaktır.

İnterneti Güvenli Kullanım İçin İpuçları

Halka açık ya da bilmediğin alanlardaki WİFİ ağları tehlikeli olabilir. Bu ağlar kişisel bilgilerini çalmak için oluşturulmuş sahte bağlantılar olabilir.

Bluetooth veya Airdrop'u kullanmadığın zaman devre dışı bırak. Bu bağlantı birçok cihazın birbiri ile etkileşim halinde bulunmasına olanak sağlar ve bir hacker bu açık Bluetooth bağlantıları içinden cihazına erişim sağlayabilir.

Cep telefonunda bulunan uygulama marketlerinin izin vermediği, güvenli olmayan uygulamaları indirme.

İnterneti Güvenli Kullanım İçin İpuçları

Herhangi bir içerik paylaşmadan önce durmak ve bu içerik ile zarar verebilir veya mi zarar görebilir miyim diye düşünmek gerekir.

Paylaşılan fotoğrafların / videoların kötü niyetli kişiler tarafından değiştirilebileceğini unutmamak gerekir. Bu yüzden paylaşılan fotoğrafları dikkatli seçmeliyiz.

Kullanılmayan hesapların silinmesi veya devre dışı bırakılması. Hesabını öylece bırakırsan haberin bile olmadan ele geçirilebilir.

DİJİTAL VATANDAŞLIK

Dijital Vatandaşlık Nedir?

Dijital vatandaş, bilgi ve iletişim kaynaklarını kullanırken eleştirebilen, çevrimiçi davranışlarının etik sonuçlarını bilen, teknolojiyi kötüye kullanmayan, **dijital** dünyada iletişim kurarken ve işbirliği yaparken doğru ve ahlaki davranışı teşvik eden vatandaştır. Günümüzde artan internet kullanımı ile birlikte "**dijital vatandaşlık**" kavramı ortaya çıkmıştır. **Dijital vatandaş** ise teknolojiyi sorumlu biçimde kullanan ve doğru davranış sergileyen kimse olarak tarif edilmektedir.

DİJİTAL SAĞLIK

Bilişim teknolojilerini ve İnternet'i kullanırken fiziksel ve zihinsel sağlığını korumalı, bağımlılık derecesinde kullanımdan kaçınmalıdır.

DİJİTAL GÜVENLİK

Kişisel bilgi güvenliğine İnternet üstünde oldukça dikkat etmeli ve İnternet ortamında gezindiği sayfaların güvenilirliğine dikkat etmelidir.

DİJİTAL YURTTAŞLIĞIN 9 BOYUTU

DİJİTAL HAK VE SORUMLULUKLAR

İnternet'te kendisine yapılmasını istemediği davranışları başkalarına da yapmamalıdır. Başkalarının içeriklerini izinsiz kullanmamalıdır.

DİJİTAL YURTTAŞLIĞIN 9 BOYUTU

DİJİTAL ETİK

Gerçek yaşamda olduğu gibi İnternet'te de etik değerlere saygılı olmalı, ahlak çerçevesinde yapması gereken davranışlar sergilemelidir.

DİJİTAL YURTTAŞLIĞIN 9 BOYUTU

DİJİTAL KANUN

Gerçek hayatta suç olan tüm davranışların İnternet'te de yapılmasının suç olduğunu bilir, buna uymayanları ilgili birimlere bildirir.

DİJİTAL YURTDAŞLIĞIN 9 BOYUTU

DİJİTAL İLETİŞİM

İnternet'te konuştuğu, paylaşımda bulunduğu diğer kişilerle saygılı bir iletişim kurabilmeli, İnternet ortamında kişisel bilgilerinin gizliliğini kötü niyetli insanlardan koruyabilmelidir.

DİJİTAL YURTTAŞLIĞIN 9 BOYUTU

DİJİTAL OKUR YAZARLIK

Bilişim teknolojilerini ve İnternet'i etkili biçimde kullanabilmeli, dijital araçlarla üretebilmelidir.

DİJİTAL YURTTAŞLIĞIN 9 BOYUTU

DİJİTAL ERİŞİM

Bireyin, bilgi ve iletişim teknolojilerinin kullanıldığı araçlardan kendi amaçları doğrultusunda yararlanabilmesidir. Bu süreç, bireysel ihtiyaçlarla ilişkili gerekli tüm yazılım ve donanım uygulamalarını, ilgi alanlarına uygun teknoloji temelli içerik ve servislere erişimi ve bu konuda ihtiyaç duyulan sosyal ve teknik destek ile performans katkısının alınabilmesini kapsamaktadır.

DİJİTAL YURTTAŞLIĞIN 9 BOYUTU

DİJİTAL TİCARET

İnternet'ten alışveriş ile riskleri bilmeli, güvenli alışveriş yapabilmeli, yanıltıcı içeriklere kanmamalıdır.

DİJİTAL YURTTAŞLIĞIN 9 BOYUTU

- İnternet'i, insanlara zarar vermek için kullanmamalıyız.
- Başkalarının İnternet'te yaptığı çalışmalara engel olmamalıyız.
- Başkalarının gizli ve kişisel dosyalarına İnternet yoluyla ulaşmamalıyız.
- Bilgilerin doğruluğuna tam olarak emin olmadan bilgileri savunmamalıyız.
- Parasını ödemediğimiz yazılımları kopyalayıp kendi malımız gibi kullanmamalıyız.
- Başkalarının elektronik iletişim kaynaklarını izinsiz kullanmamalıyız.
- Elektronik iletişim ortamını başkalarının haklarına saygı göstererek kullanmalıyız.
- İletişim sürecinde kullandığımız dilin doğuracağı sonuçları önceden düşünmeliyiz.

Zorbalık ve Siber Zorbalık

Zorbalık, fiziksel veya sözlü olabilen, bir kişi ya da grup tarafından uygulanan ve çoğunlukla kişilerin kendilerine göre güçsüz ya da zayıf kişileri hedef aldığı yüz yüze, tekrarlanan, saldırgan davranışlardır.

Siber zorbalık, dijital teknolojilerin kullanımıyla sosyal medyada, mesajlaşma platformlarında, oyun platformlarında kişiyi korkutmayı, kızdırmayı veya utandırmayı amaçlayan, tekrarlayan zorba davranışlardır.

Siber Zorbalık

- Sosyal medyada birinin hakkında yalanlar yaymak veya utanç verici fotoğraflarını yayınlamak
- Mesajlaşma platformları aracılığıyla incitici mesajlar veya tehditler göndermek
- Birinin kimliğine bürünmek veya onun adına başkalarına mesajlar göndermek

Şaka mı, Zorbalık mı?

- Tüm arkadaşlar birbirleriyle şakalaşır. Ancak seni üzen bir şaka durmasını istemene rağmen devam ediyorsa ve senin için artık eğlenceli değilse, bu zorbalık olabilir.

- Zorbalık çevrimiçi gerçekleştiğinde, hiç tanımadığınız insanlar dahil geniş kitlelere ulaşabilir ve istenmeyen bir ilgiye neden olabilir. İçinde bulunduğun durumun seni üzdüğünü ve artık dozunu aştığını düşünüyorsan buna bir dur diyebilirsin.

Paylaşım yapmadan önce kendine sor:

- Bunu birinin yüzüne de söyler miydin?
- Başka biri yazdığın şeyi yanlış anlayabilir mi?
- Birinin itibarını zedeler mi?
- Biri senin hakkında böyle söylese ya da yazsa nasıl hissederdin?
- Arkadaşlarının, ailenin ve öğretmenlerinin yazdığın bu tür şeyleri okumasını ister miydin?

Çevrimiçiyken sana nasıl davranılmasını istiyorsan sen de insanlara öyle davran.