2.ÜNİTE : ETİK VE GÜVENLİK

A. ETİK , İNTERNET ETİĞİ KAVRAMI

ETİK : Doğru ile yanlışı, haklı ile haksızı, iyi ile kötüyü, adil ile adil olmayanı ayırt etmek, bunun sonucunda da doğru, haklı, iyi ve adil olduğuna inandığımız şeyleri yapmaktır. Kısacası iyi ve doğru olanı yapmaktır.

İNTERNET ETİĞİ : İnternet üzerinde iletişimde bulunurken doğru ve ahlaki olan davranışlarla, yanlış ve ahlaki olmayan davranışları belirleyen kurallar bütünüdür. Kısacası gerçek hayatta insanlara gösterdiğiniz saygı ve nezaketin internet ortamında da gösterilmesidir.

İNTERNET ETİĞİNE UYGUN DAVRANIŞLAR

- İnterneti, insanlara zarar vermek için kullanmamalıyız.
- Başkalarının internette yaptığı çalışmalara engel olmamalıyız.
- Başkalarının gizli ve kişisel dosyalarını internet yoluyla çalmamalıyız.
- Parasını ödemediğimiz yazılımları kopyalayıp kendi malımız gibi kullanmamalıyız.
- Başkalarının elektronik iletişim kaynaklarını izinsiz kullanmamalıyız.
- Elektronik iletişim ortamını başkalarının haklarına saygı göstererek kullanmalıyız.

B. DİJİTAL YURTTAŞLIK

DİJİTAL YURTTAŞ : İnternet aracılığı ile dünyanın dört bir yanından birbirine bağlanan insanlar aynı çevrim içi ortamı paylaşırlar. Buna **dijital** ya da **siber dünya** da diyebiliriz .İşte bu siber dünyadaki herkese **Dijital Yurttaş** denir.

DİJİTAL YURTTAŞLIK ÖRNEKLERİ :

- e-devlet uygulamasını kullanarak resmi işlemlerini yapabilen kişiler,
- e-okul uygulamasını kullanarak notlarını , devamsızlığını öğrenen öğrenci ya da veli,
- e-nabız uygulamasını kullanarak sağlık ile ilgili işlemlerini takip eden kişiler ,
- e-ticaret uygulamalarını kullanarak alışveriş yapan kişiler

Dijital vatandaş olmanın vatandaşlar ve bu hizmeti veren kurumlar açısından birçok avantajları bulunmaktadır.

Vatandaş açısından avantajları:

- İşlemleri daha hızlı ve daha kolay yapabilme
- Zamandan tasarruf
- İnternet olan her yerden hizmet alabilme
- Maddi tasarruf
- İşlem basamaklarını kolayca görebilme

Kurumlar açısından avantajları:

- Personel tasarrufu
- Kırtasiye, posta giderleri vb. tasarrufları
- Zaman tasarrufu
- Hızlı ve kaliteli hizmet
- Vatandaş memnuniyeti

Dijital Vatandaşlığın 9 Boyutu :

1. **Dijital Erişim :** Toplumun tamamının yüksek hızda ve yüksek kalitede teknolojiye erişimini ifade eder.
2. **Dijital Ticaret** : Güvenli internet siteleri üzerinden alışveriş yapma bilincinin ve yeterliliğinin olmasını ifade eder. Aynı zamanda çevrimiçi bankacılık hizmetlerinin güvenlik ve gizliliğini sağlayabilmesini içerir.
3. **Dijital İletişim :** Farklı dijital iletişim kaynaklarını doğru zamanda kullanma ve bilgi alışverişi yapma becerisine sahip olmayı ifade eder.

4. **Dijital Okuryazarlık :** Öğrenme ve öğretme süreçlerinde teknolojinin kullanılmasını içerir. Dijital ortam kullanarak doğru bilgiye ulaşma, üretme ve paylaşabilme bilincine sahip olmayı ifade eder.
5. **Dijital Etik :** Dijital araçların ne zaman ve nasıl kullanılacağı konusunda sorumluluk sahibi olmayı ve başkalarının haklarına saygı duymayı içerir.
6. **Dijital Kanun :** Dijital ortamlarda geçerli olan gizlilik kuralları, kullanım politikaları gibi çeşitli kurallar hakkında bilinçli olmayı, bunlara uymayı ve uymayanları uyarmayı içerir.
7. **Dijital Hak ve Sorumluluklar:** Dijital araçları kullanarak herkesin kendini özgürce ifade etme hakkını, dijital ortamda yapılan haksızlıklar ve işlenen suçlar için de şikayet etme sorumluluğunu ifade eder.
8. **Dijital Sağlık :** Teknoloji kullanmanın getirdiği yeni hastalıklar hakkında bilgili ve bilinçli olmayı ifade eder.
9. **Dijital Güvenlik :** Kişilerin dijital araçları kullanırken donanım, yazılım, ağ ve kişisel bilgi güvenliklerini sağlayabilmesini ifade eder.

Dijital Ayak İzi

Dijital ayak izi, interneti kullanırken oluşturduğunuz veri izidir. Ziyaret ettiğiniz web sitelerini, gönderdiğiniz e-postaları ve çevrim içi hizmetlere gönderdiğiniz bilgileri, fotoğrafları, videoları içerir.

DİJİTAL YURTTAŞLIK KURALLARI :

1. İnternette rastladığımız içeriğin doğru olup olmadığını kontrol etmeliyiz.
2. İnternetteki yanıltıcı reklamlara kanmamalıyız.
3. İnternette iletişim kurduğumuz kişilere saygılı davranmalıyız.
4. İnternette gerçek yaşamda yapmayacağımız hiçbir hareketi yapmamalıyız.
5. Gerçek yaşamda suç olan davranışların internette de suç olduğunu bilmeliyiz.
6. İnternette bize yapılmasını istemediğimiz bir davranışı biz de başkasına yapmamalıyız.
7. İnterneti bağımlılık derecesinde kullanmamalıyız.
8. İnternette kişisel bilgilerin gizliliğine dikkat etmeliyiz.

C.SİBER ZORBALIK

Siber Zorbalık : Kişi ya da kişilerce bilişim teknolojileri aracılığı ile karşısındaki kişiye zarar vermek amacıyla kötü niyetle ve tekrarlayan şekilde yapılan davranışlara **siber zorbalık** denir. Siber zorbalık ; bilgisayar , tablet , telefonda kullanılan sosyal medya (twitter, facebook , instagram vb.) , iletişim uygulamaları (whatsapp , discort ,skype vb..) ya da online oyunlar üzerinden yapılabilir.

Siber Zorbalık Belirtileri :

Siber zorbalık belirtileri olarak bunları sayabiliriz ;

- Aşağılama
- Tehdit Etme
- Şantaj Yapma
- İftira Atma
- Dedikodu Yapma
- Küfür Etme
- Utandırma
- Dışlama
- Taciz Etme

Siber Zorbalığa Maruz Kalınca Yapılacaklar :

1. Sosyal medya hesaplarınızın gizlilik ayarlarını sadece sizin izin verdiğiniz kişilerin size ulaşabileceği şekilde ayarlayın.
2. Sizi rahatsız eden bir kişi olursa onun hesabını engelleyin.
3. Siber zorbalığa maruz kaldığınızda uygulamanın "şikayet et" özelliğini kullanarak o kişiyi rapor edin.
4. İnternet ortamında bir zorbalıkla karşılaştığınızda o uygulamayı kapatın ya da o gruptan ayrılın.

5. Siber zorbalıkla karşılaştığınızda bunu bir büyüğünüze hemen söyleyin.
6. Zorbalığın derecesinin artması ihtimali nedeniyle siber zorbanın gönderdiği iletileri silmeyin.
7. Zorbalık yapan kişiye cevap vermeyin , misilleme yapmayın.
8. Kendinize yapılmamasını istemediğiniz hiçbir davranışı siz de internet ortamında kimse o şekilde davranmayın.
9.

E.GÜÇLÜ ŞİFRELER

İnternet ortamında kişisel bilgilerimizin güvenliği sağlamak için güçlü şifreler oluşturmalıyız. Güçlü şifre oluştururken dikkat etmemiz gereken kurallar aşağıda verilmiştir.

- Şifremiz en az 8 karakterden oluşmalıdır.
- Şifrede direkt sözlükten alınmış anlamlı kelimeler kullanılmamalıdır.
- Şifremizde kişisel bilgilerimize yer verilmemelidir. (Ad, Soyadı, TC Kimlik No , Anne Adı , Doğum tarihi vb..)
- Şifremiz kolay tahmin edilen bilgiler içermemelidir.(klavyede yan yana gelen tuşlar(asd,123 vb..) ,tuttuğunuz takım , evcil hayvan adı , oturduğun yer , hoşlandığı şeyler vb…)
- Şifrenizin içinde mutlaka büyük – küçük harf , sayı ve sembol olmalıdır.(Ör :bilgisayar yerine B1lg1s@y@r yaparak şifreyi güçlendirebiliriz.)
- Şifreyi belirlerken önce unutmayacağımız bir cümle belirleyip onun üzerinde değişiklik yapmak şifremizi kolay hatırlamamızı sağlar.

ÖRNEKLER :

-
  - Sevdiğiniz bir şarkıdaki sözü belirleyebilirsiniz. Mesela “Bugün bayram erken kalkın çocuklar” şarkı sözünde geçen **Bugün bayram** şifremiz olsun.Şifrede tekrarlanan B harfleri yerine 8 a harfleri yerine 6 koyalım. Boşluk yerine de nokta . Şifremiz **8uGün.86yr6m** oldu.
  - **Her sabah 7.15’te kalkarım.** Cümlesinden sesli harfleri atalım. **Hrsbh7.15’tklkrm.** işte güçlü şifremiz.
  - **2006 yılında Kırklareli Lüleburgaz’da doğdum.** Cümlesinde kelimelerin ilk harflerini alalım. **2006yKLd.** İşte güçlü şifremiz.

- Güçlü şifre belirledikten sonra bu şifrede ufak değişiklikler yaparak hesaplarımızda kullanabiliriz. (**8uGün.86yr6m** şifremiz olsun bunu facebook’ta kullanırken başına FA , İnstagram’ da kullanırken Başına İN ekleyebilirsiniz.
- 6 ayda bir şifrelerinizi değiştirin.
- Ortak kullanılan bilgisayarlarda Beni Hatırla / Kaydet özelliklerini kullanarak şifrelerinizi bilgisayara kayıtlı hale getirmeyin.
- Açtığınız hesapları Oturumu Kapat diyerek kapatın.

F. SİBER TUZAKLAR

İyi bir dijital vatandaş olmak için interneti bilinçli kullanmak ve dijital ortamlardaki tehlikelere karşı dikkatli olmak gerekir.

Siber Tuzaklara Düşmemek için Dikkat Etmen Gereken 10 Madde:

1- İnternette kimlik bilgilerini girmen gereken sitelere karşı dikkatli olmalısın! Gizli kalması gereken bilgilerini yazma!

2- Hediye kazandığını söyleyen reklam mesajlarına inanma!

3- Eğlenceli gibi görünen bazı testle senin hakkında bilgi toplamak amacıyla yapılmış olabilir. İyice düşünmeden bunları doldurma!

4- Hiç bir firma ya da kurum senin parola gibi gizli bilgilerini e-posta, kısa mesaj, telefon yoluyla istemez. Bu isteklere sakın cevap verme!

5- Bazı internet sitelerinde açılır pencere(pop-up) yoluyla açılan yarışma, anket vb. reklam pencerelerini kapat. Bu pencerelerde yer alan bağlantıları tıklama!

6- Kimin gönderdiğini bilmediğin, şüpheli görünen e-posta ve kısa mesajlardaki bağlantılara tıklama!

7- Tanımadığın kişilerden gelen bir e-postayı açma!

8- "Bu mesajı 10 kişiye gönder, sonra en çok istediğin şey olacak" benzeri zincir e-postalar aktif adres toplamak için yapılmaktadır. Seni ve arkadaşlarını tehlikeye atabilir. Bu mesajları sil! Gönderen kişileri uyar!

9- Bilgisayarında bulunan kamera çeşitli zararlı yazılımlar ile isteğin dışında kullanılabilir. Güvenlik yazılımları kullandığından emin ol. Kullanmadığın dönemlerde kameranı kapalı tut!

10- Oyun oynamak için üye olmanı isteyen bir site varsa önce siteyi ve istediği bilgileri kontrol et.