



SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI

GÜVENLİ İNTERNET KULLANIMI



İnternetin Tanımı



* **İnternet;** iş, iletişim, eğlence, alışveriş ve en önemlisi bilgiye ulaşmak için en sık kullanılan platformlardan biridir. İnternetin bu kadar önemli alanlarda rol almasıyla doğru orantılı olarak internette paylaşılan bilgi miktarı da artmıştır.



İnternetin Tanımı

* İnternet üzerinde paylaşılan bu bilgilerin insanlara sağladığı yararlar oldukça fazladır. Ancak internet **büyük ve karmaşık bir sistem** olduğu için bu sistem üzerindeki boşlukların kötü amaçlar için kullanılması internet kullanıcılarını tehdit edebilmektedir.





İnternet Güvenli mi?



* Gerekli **tedbirler alınmadığında** internetin güvenli olduğunu söylemek doğru değildir. İnternet kullanıcıları kendi üzerlerine düşen sorumlulukları yerine getirirlerse, interneti belli bir düzeyde güvenli hale getirebilirler. Bu sorumluluklar şunlardır:



1. Kişisel Bilgileri Profesyonel ve Sınırlı Tutun.

* Üyesi olduğunuz sosyal ağ sitelerinde ve herkesin erişimine açık olan internet ortamlarında, **kişisel bilgilerinizi paylaşmamalısınız.** Bu bilgileri ele geçiren zararlı yazılım veya kişiler, kişisel güvenliğinizi tehlikeye atıcı girişimler yapabilir.





2. Gizlilik Ayarlarınızı Açık Tutun.

* Web tarayıcıların ve mobil işletim sistemlerin **gizliliğinizi çevrimiçi korumak** için çeşitli ayarlar bulunmaktadır. Güvenlik ayarlarını detaylı bir şekilde gözden geçirip tüm güvenlik ayarlarınızın açık olduğundan emin olmalısınız.





3. Grdğnz Her Linke Tıklamayın.

* Siber suçlular, tehlikeli gibi gözkmeyen ancak ierisinde bir ok tuzak barındıran sahte ierikleri kullanırlar. **Dikkatsiz tıklamalar** sonucunda kişisel verilerinizin aıa ıkabileceėi gibi elektronik cihazlarınıza **malware** diye tabir edilen kt amalı yazılımların yklenmesine de sebebiyet verebilir. O yzden Őpheli grdğnz ieriklerdeki linklere tıklamamalısınız.



4. İnternet Bağlantınızın Güvenli Olduğundan Emin Olun.

* Herkese açık bir Wi-Fi bağlantısı kullanarak çevrimiçi olduğunuzda, artık cihazınızın güvenliğinin üzerinde doğrudan kontrolünüz olmadığını bilmelisiniz. Eğer banka hesap numaranız gibi önemli bilgileri girecekseniz önce cihazınızın bağlandığı **ağın güvenli olduğundan** emin olmalısınız. Eğer güvenlik ile ilgili herhangi bir şüpheniz varsa, güvenli bir Wi-Fi ağına bağlanana kadar beklemelisiniz.



5. Ne İndirdiđinize Dikkat Edin.

* İnternet ortamından, size yararlı olabileceđini dűşűndűđűnűz her dosyayı indirmemelisiniz. Gűvendiđiniz ya da **uzun sűredir kullandiđınız siteler** aracılıđıyla iřleminizi sađlamanız yararlı olacaktır.





6. Güçlü Şifreleri Seçin.

* İnternet ortamında sahip olduğunuz tüm hesaplar için, **en az 3 ayda bir**, şifrelerinizi farklı kompleks bir yapıda güncellemelisiniz. Güçlü bir parola belirleyebilmek için, **benzersiz kelime grupları oluşturmalı** ve **en az 15 karakter uzunluğunda**, harfleri, sayıları ve özel karakterleri barındıran şifreler kullanmalısınız.





7. Güvenli Sitelerden Satın Alım Yapın.

* Çevrimiçi bir ürün satın aldığınızda, kredi kartı veya banka hesabı bilgilerinizi kullanmanız gerekmektedir. Ürün satın almadan önce kart bilgilerinizi gireceğiniz web sitelerinin **https:** ile başladığından emin olmalısınız. Eğer yalnızca **http:** ile başlıyorsa o siteden kesinlikle alışveriş yapmamalısınız. Burada sonda bulunan **“S” ifadesi secure yani güvenli anlamına gelmektedir.**



8. Ne Yazdığınıza Dikkat Edin.

* İnternette bir silme anahtarı yoktur yani sizin internet üzerinde paylaştığınız tüm yorumlar, resimler ve içerikler silseniz dahi internet üzerinde sonsuza dek kalabilirler. İçerik paylaşırken ailenizin, potansiyel işvereninizin ve geri kalan çevrenizin görmesini istemeyeceğiniz şeyler paylaşmamaya özen gösterin.





9. Kiminle Tanıştığınıza Dikkat Edin.

* Çevrimiçi olarak tanıştığınız kişiler, her zaman iddia ettikleri kişiler olmayabilir, gerçek kişiler bile olmayabilir. Çevrimiçi sosyal yaşamınızda, kişisel sosyal yaşamınızda olduğunuz kadar dikkatli ve mantıklı olmanızda fayda vardır.





10. Virüs Koruma Programınızı Güncel Tutun.



* İnternet güvenlik yazılımlarınız sizi her tehdide karşı koruyamayacaktır, ancak bu **yazılımları güncel tuttuğunuz** müddetçe sizi bir çok malware virüslerinden koruyacaklardır. Dolayısıyla, işletim sisteminizin ve kullandığınız başta güvenlik yazılımlarınız olmak üzere tüm uygulamaların güncellemelerini aksatmadan düzenli bir şekilde yapmalısınız.



Bilgileri en az 3 farklı güvenilir kaynaktan kontrol et.

**Kaynak
güvenilir mi?**

**İletişim bilgisi
var mı?**

**Sayfa içeriği
güncel mi?**

**Alan uzantısına
dikkat
.gov .org .com vb. ?**



Yalan Haber ve Asılsız Bilgi ile Mücadele

- * **ARAŞTIRMA** (Haberin kaynağını araştırın.)
- * **DİKKAT** (Haberin oluşturulma tarihinin güncel olmasına dikkat edelim.)
- * **GÜVENİLİR KAYNAK** (Bilgiye resmi kaynakların açıklamalarından erişin.)
- * **SORGULAMA** (Haber içeriğini objektif bir açısı ile okuyun ve sorgulayın.)



Yalan Haber ve Asılsız Bilgi ile Mücadele

- * **DOĞRULAMA** (Bilgiyi farklı kaynaklardan doğrulayın ve doğrulanmamış bilgilere güvenmeyin.)
- * **DESTEK** (Haberi doğrulamak için, haber doğrulama platformlarından destek alın.)
- * **PAYLAŞ(MA)** (Kaynağı olmayan, şüphe uyandıran ve teyit etmediğiniz hiçbir bilgiyi paylaşmayın.)



İnternetin Güvenli Kullanımı

- * **Anti-virüs kullanmak**, firewall programı kullanmak ve işletim sistemimizi güncel tutmak,
- * **Bilgiyi nerede aradığımıza dikkat etmek**,
- * **Kablosuz ağ şifremizi paylaşmamak**, herkese açık şekilde bırakmamak ve **şifre güvenliğine dikkat etmek**,
- * **İnternet üzerinden alışveriş yapıyorsak alışveriş yaptığımız sitelerin güvenilirliğinden emin olmak** ve **sanal kart kullanmak**,



İnternetin Güvenli Kullanımı

- * Şüpheli linkleri ve e-mailleri açmamak, **Phishing (e dolandırıcılık)** tuzağına düşmemek,
- * Birden fazla kişinin kullandığı bilgisayarda, bankacılık işlemlerini mecbur kalmadıkça yapmamak,
- * Üyelik istenen sitelerde **kimlik hırsızlığına** maruz kalmamak için kişisel bilgilerin tamamını vermemek,
- * Sosyal paylaşım sitelerinde kişisel gizlilik, mahremiyet ve paylaşım konularında sınırlar belirlemek,



İnternetin Güvenli Kullanımı

- * Tanımadığınız kişilerden gelen eposta ve bağlantıları açmamak,
- * İnternette gezinirken isteminiz dışında inen dosyaları açmamak,
- * Ani açılan **pop-up pencerelere** dikkat etmek,
- * **'Benim başıma gelmez.'** veya **'Güvenli olmayan sitelere girmiyorum.'** diye düşünmeyip, şüpheli olmamız gerekir.



Çocukların İnternet Kullanımı

- * Çocuklarınızın kullandıkları teknolojiler hakkında bilgi sahibi olmalısınız.
- * Çocuğunuzun çevrimiçi faaliyetleri hakkında bilgi sahibi olun.
- * Çevrimiçi faaliyetlerini kontrol edin, ne yaptığı ve neden yaptığı konusunda onlarla konuşun.
- * Çocuğunuzun ziyaret ettiği siteler ve oynadığı oyunlara aşina olun.



Çocukların İnternet Kullanımı

- * **Çocuğunuzun internet erişiminde kullandığı araçları (cep telefonu, tablet, laptop vs.) yatak odalarının dışında ortak kullanım alanında bulundurun.**
- * **İnternet filtrelerini (çocuk filtresi) ve gerekiyorsa aile kontrol uygulamalarını indirin.**
- * **İnterneti ne zaman, ne kadar süreli kullanacağına ilişkin birlikte kurallar koyun.**
- * **Çevrimiçi davranışlarınızla ve teknoloji kullanımınız ile çocuğunuza model olun.**



Dijital Oyunlar

- * **Farkında mıyız?**
- * **Çocuklarımız hangi oyunları oynuyor?**
- * **Oynadığı oyunlar yaşına uygun mu?**
- * **Oynadığı oyunların içeriğini biliyor muyuz? (Şiddet, nefret, müstehcenlik, korku, bahis vb.)**



Çocuk Profili



- * Çocuk profili içeriği uzmanlarca belirlenen kriterlere uygun sitelerden oluşmaktadır.
- * Psikoloji, pedagoji, sosyoloji ve hukuk alanlarında uzman akademisyenlerin bulunduğu bir kurul tarafından kriterler tespit edilmektedir.



166 HATTI

166 Hattı Ne İşe Yarar?

* İnternette ilgili olan sorunlar hakkında bilgi edinmeye ve şikayette bulunmaya yaramaktadır.

Hangi Durumlarda Aranır?

* İnternet hakkında bilgi almak ya da internette ilgili olan konularda bir durumu ihbar etmek ve şikayetçi olmak için aranır.



Sonuç

- * **Ebeveyn olarak kendimizi çocuğumuzun yerine koyup onun interneti nasıl algıladığını görmeye çalışmalıyız.**
- * **Eğer çocuğumuz interneti bir öğrenme aracı olarak görüyorsa bulunduğumuz konumu korumalıyız.**
- * **Çocuğunuz çok meraklıysa ve bizden bazı şeyleri gizliyorsaa dikkatli olmalı; internetin olumlu yönlerinin, olumsuzluklardan daha önemli olduğunu vurgulamalıyız.**



SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI

GÜVENLİ İNTERNET KULLANIMI