Online Security Tips

Protect yourself when you're online!

Create strong passwords.

Use passwords that are hard to guess, and keep track of it using a password manager.

Be careful of what you download.

Don't download content from sites that are not trustworthy. These may contain malware.

Turn on privacy settings.

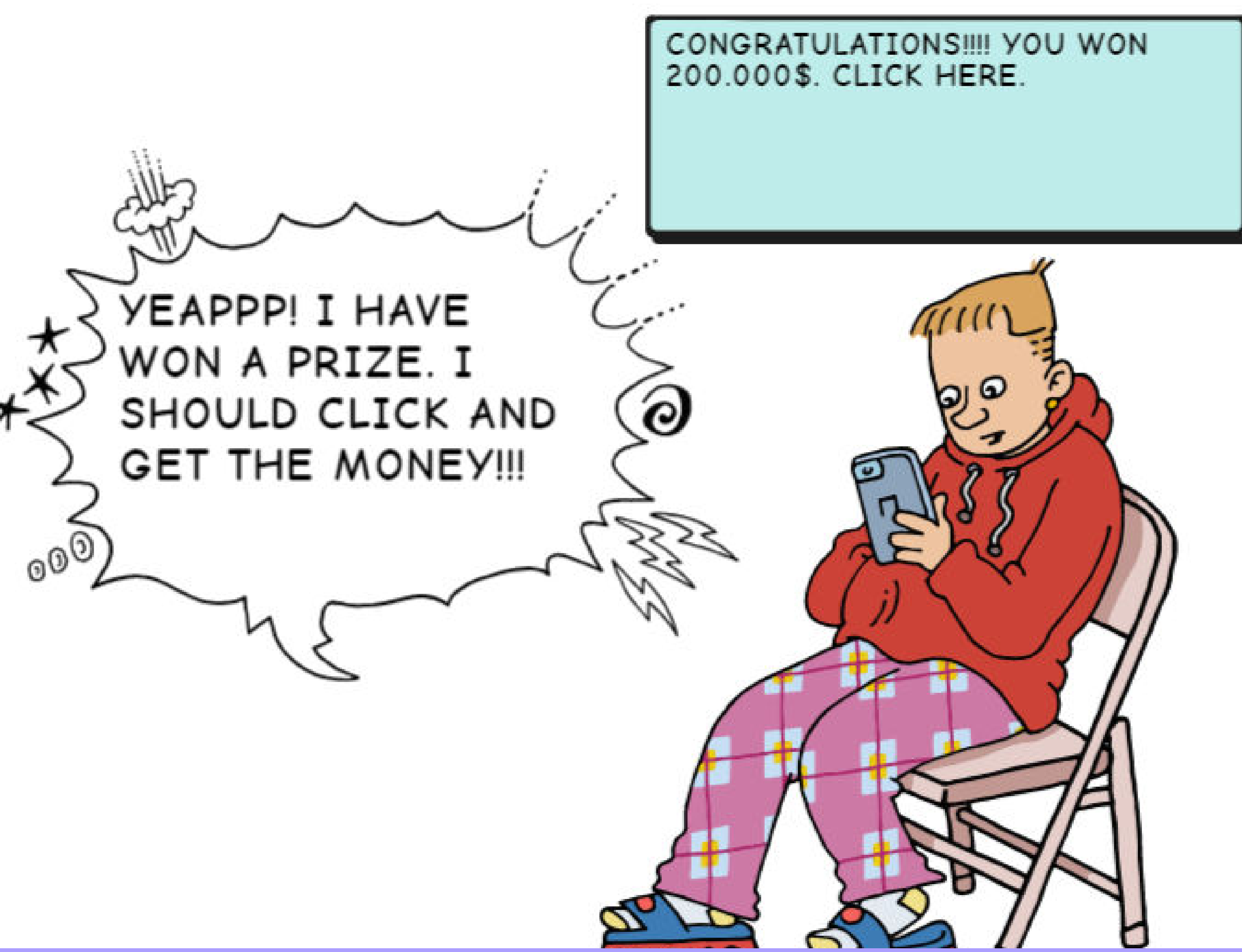
Take control of how companies use your data by enabling privacy features.

Think before you post.

Avoid posting sensitive personal information online. Don't share too much information either.

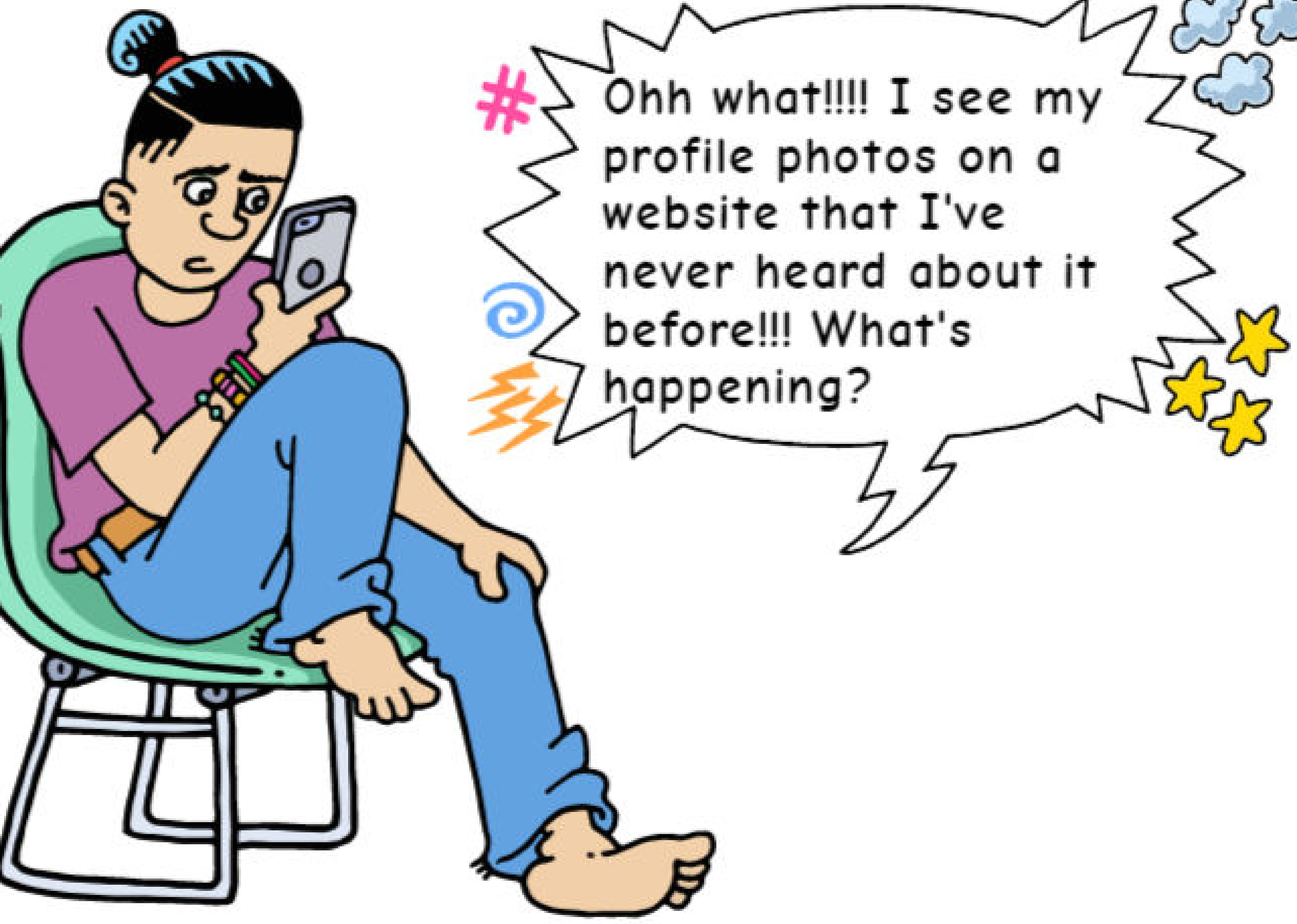
Use an anti-virus program.

Keep your anti-virus software updated so it can detect potential threats in your system.



DON'T GET TRAPPED ON THE INTERNET!

İNTERNETTE TUZAĞA DÜŞME!



LEARN ABOUT WHAT TO DO IN CASE OF ANY HACKING!

HESAP ÇALINMASI DURUMUNDA NE YAPILACAĞINI ÖĞREN!

İNTERNETTE GÜVENDE MİSİN?

ŞİFRELER

- Güçlü şifreler kullanıyor musun?
- İki aşamalı kimlik doğrulaması kullanıyor musun?

ANTİ-VİRÜS

- Güncel anti-virüs programlar kullanıyor musun?
- Düzenli virüs taraması yapıyor musun?

KAYNAKLAR

- Yazılımları güvenli kaynaklardan mı indiriyorsun?
- Tıklamadan önce bağlantıları kontrol ediyor musun?

SİBER ZORBALIĞIN GÖRÜLDÜĞÜ PLATFORMLAR

- FACEBOOK, INSTAGRAM, TWITTER VE DİĞER SOSYAL AĞLAR
- KISA MESAJLAR (SMS)
- E-MAIL VE ANLIK MESAJLAŞMA UYGULAMALARI
- DİĞER SOHBET PROGRAMLARI

İNTERNETİN FAYDALARI VE ZARARLARI

Güncel haberleri ve bilgileri öğrenebilirsin.

Görüş ve bilgi paylaşabilirsin.

Zamandan ve mekandan bağımsız, eş zamanlı ve eş zamansız iletişim sağlayabilirsin.

Ekonomik ve hızlı iletişim imkanı bulabilirsin.

Görsel ve işitsel öğelerle iletişim kalitesini artırabilirsin.

Yanlış ve zararlı bilgiye erişim,

Siber zorbalık,

Sanal dolandırıcılık,

Zararlı yazılımlar,

İnternet bağımlılığı,

Sağlık sorunları,

Uygunsuz içeriklerle karşılaşma ihtimalin olabilir.

DİJİTAL AYAK İZİ NEDİR?

İnternette gezindiğimiz her yerde bir iz bırakırız. Peki bu izler ne demek?

Bir alışveriş sitesinden okumak istediğiniz bir kitap almak istediniz. Araştırdığınız kitap türleri, o web sitesinin veri tabanlarında kayıt altına alınır. Bundan sonraki gezdiğiniz her web sayfasında o kitap türlerine benzer ürünler, reklam banner sayfası ya da pop-up olarak karşınıza çıkar.

DİJİTAL AYAK İZİ BIRAKMAK KÖTÜ BİR ŞEY Mİ?

Hayır. Çünkü bu teknoloji sayesinde suçlular yakalanabiliyor. Ama önemli olan, kendimizin nasıl bir dijital ayak izi bıraktığı. Dijital Ayak İzi aktif ve pasif olmak üzere 2'ye ayrılır. Pasif Dijital Ayak İzini istemsiz bırakırız. Örneğin, bir web sitesini ziyaret ettiğimizde IP adresimizi kaydedebilir. Aktif Dijital Ayak İzi ise sosyal medya hesabımızdan bir fotoğraf yüklediğimizde gerçekleşir. Kısaca internette ileti, mesaj, fotoğraf, durum paylaşımı gibi eylemleri ne kadar çok yaparsak, dijital ayak izimiz de o kadar büyür. Bu da tehlikeli olabilir.

NASIL BİR DİJİTAL AYAK İZİMİZ OLMALI?

- Bir web sitesine üye olurken sürekli aynı e-posta adresimizi yazmamalıyız.
- Sosyal medya ayarlarımızı sürekli gözden geçirmeliyiz. Gizlilik ayarları, kişileri düzenlemek gibi,
- Sosyal medya üzerinden aşırı paylaşım yapmaktan kaçınmalıyız.
- Şifrelerimizi periyodik olarak değiştirmeliyiz.
- Kablosuz ağlara dikkat etmeli, karşımıza çıkan linke rastgele tıklamamalıyız.
- Arama motorlarında adımızı ara sıra aratıp bizi rahatsız eden içerikleri belirleyebiliriz.

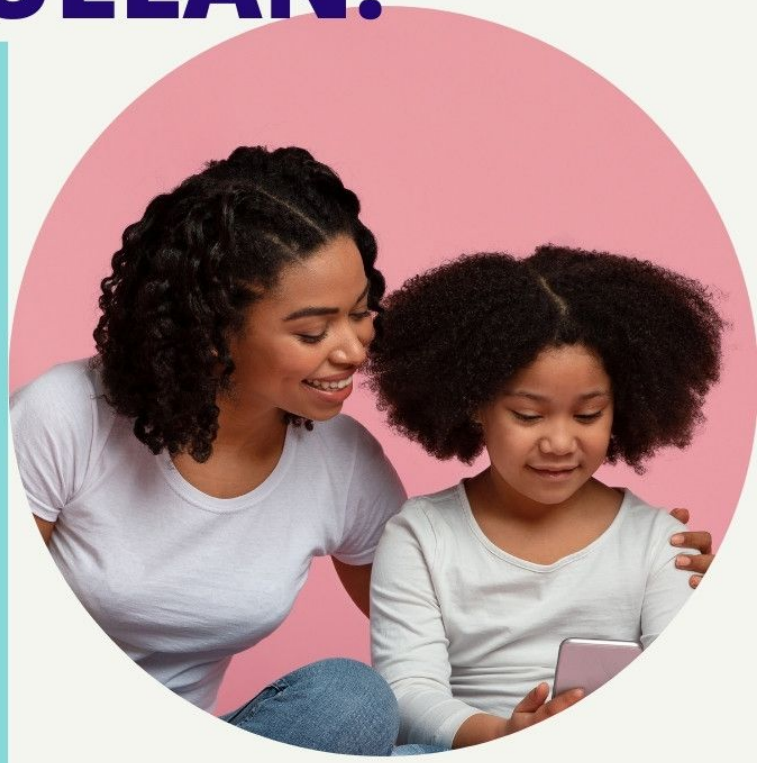
GÜVENLİ İNTERNET KULLAN!

Hesaplarının parolalarını periyodik olarak değiştirmeye ve güçlü şifre almaya üşenme!

Bilgiyi nerede aradığına dikkat et!

Antivirüs programı kullan!

Güvenlik duvarını açık tut!



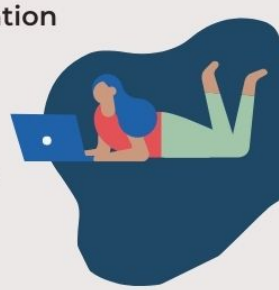
Ebeveyn kontrolünü açık tut!

7 INTERNET SAFETY TIPS

FOR EVERYONE!

1 Don't Give Out Personal Information

Avoid online phishing attempts by keeping your personal information private. Don't give out your phone number, social security information, or banking info to someone you don't know.



2 Create Complex Passwords

Create passwords with a combination of letters, numbers, and symbols. Consider using password managers to create and keep track of your passwords.

3 Check Website Reliability

Before purchasing anything on a website ensure that it's safe. You can do this by checking if it has a small lock icon or "https" before the URL. The "s" in "https" stands for "secure" and the lock means it's confirmed as a safe site by your browser.

4 Avoid Suspicious Online Links

Be careful of websites or emails containing suspicious links. Some websites may use quizzes, freebies, or salacious stories to get you to click on them and then steal your personal information.

5 Keep Your Computer Updated

Computer developers release updates to keep products safe. Keep your device software up to date so it is not vulnerable to malware.

6 Monitor App Permissions

Learn the privacy settings for any device, app or service you use. Some apps will ask for permission to access photos and other personal information. Stay informed so you aren't sharing anything you don't want to.

7 Be Cautious with Public Wifi

Be careful when you use public wifi. When accessing public networks, anyone can use unsecured networks to distribute malware and access private information.