6 Simple ways to improve your cybersecurity

Cybersecurity is an increasingly challenging battlefront. Hackers reportedly attack every 39 seconds, and 95% of these breaches result from human error. Traditional computers aside, an expansive array of smart devices (from cars to appliances, voice controllers, wearable tech and much more) have amplified security challenges.

Anyone who connects to the Internet or another device using Wi-Fi can be hacked. Someone with physical access (Ethernet, Bluetooth, etc.) can also launch a malware attack—on any programmable device, service or network—to steal passwords, social media accounts, sensitive work information, financial data and more for profit.

Cybersecurity education is essential to mitigate digital risks. Remember these tips, and consult sites like Cybrary, InfoSecInstitue and Udemy to learn more.

Use reliable charging cables and drives

If you find one laying around somewhere, don't use it. It can be programmed to automatically execute a malicious code as soon as it's plugged in and receives power, enabling hackers to easily take over your device and spy on your webcam in a matter of seconds. Public USB charging stations (as often seen in airports, hotels and other places) also increase your risk. Use AC charging ports instead.

Enable two-factor authentication

This requires two different methods to confirm your identity before you can access an app or website. Make a

7600 Leesburg Pike, Suite 300, Falls Church, VA 22043-2004 (800) 543-2002

list of all your accounts that require a log-in (email, banking, etc.), and download an authenticator app (such as Authy) or pick up a hardware-based authentication key (like YubiKey). These options are more secure from a cybersecurity approach than being texted a security code, since text messages can also be hacked.

Ensure a website or a specific URL is safe

Copy and paste a URL into URLVoid.com to check the most reputable website safety authorities for any flags. URLVoid also checks transparencyreport.google.com, a widely trusted resource.

Report social engineering incidences to your company's security team.

Common examples include phishing emails—fraudulent messages containing spam links or attachments. When an email looks suspicious (even if it appears to be from someone you know), delete it. Additionally, never click on unsolicited links in text messages, social media messages, pop-up ads and so on.

Beware of online job scams.

This is a growing front on the cybersecurity battlefield. The FBI's Internet Crime Complaint Center saw a 20% spike in scam-related complaints this year, with losses exceeding $3,000 per victim. In some cases, fraudsters pose as legitimate employers, conducting interviews and "hiring" the victim online. After that, they request the person's personal and financial data.

Additional Resource: Use this FBI tip sheet to stay safe.

Shut down computers at night

Don't just let them go into sleep mode. Also, disable remote connectivity (Wi-Fi, Bluetooth) of any mobile devices not in use. This will decrease your breach vulnerability and prevent hackers from accessing your devices and your network.

7600 Leesburg Pike, Suite 300, Falls Church, VA 22043-2004 (800) 543-2002