SEE YOURSELF IN CYBER

Cybersecurity Awareness Month 2022

THIS MONTH'S TOPICS:

The Wi-Fi Guide

Everything you need to know...

Smart Devices

The future of smart devices...

Scam of the Month:

Payment Platform Scams...

Cyber Zen Den:

Align your habits with digital safety...

October is Cybersecurity Awareness Month. With this year's theme being "See Yourself in Cyber," we will be covering important topics that will help users be confident about their place in the future of cybersecurity.

Many users feel like they should already be pros when it comes to technology. The reality is, most don't fully understand the security risks that come along with the technology they use every day.

With a better understanding of how to stay secure, you can feel confident about your place in this digital world.

THE WI-FI GUIDE

Everything you need to know about Wi-Fi

What is Wi-Fi?

Wi-Fi is a wireless network that allows devices to connect to the internet and communicate with other nearby devices wirelessly by radio waves.

Public Wi-Fi

Public Wi-Fi can be accessed by anyone. Many stores, hotels, and businesses offer public Wi-Fi. While this can be convenient, it poses a great security risk.

Public Wi-Fi Risks

Wi-Fi snooping and malware distribution are risks of public Wi-Fi. Anyone who hacks the network or has access to it can monitor activity or inject malware.

Airplane Wi-Fi

Airplane and airport Wi-Fi are often targeted by hackers due to the high volume of activity. If you do connect, use caution, and avoid viewing personal data due to the potential lack of privacy.

Home Wi-Fi

Most people rely on home Wi-Fi for everything. Make sure your router is updated and has encryption turned on. Change the default name and turn off network name broadcasting to increase privacy and prevent hacking.

Wi-Fi Tips

-Use a VPN (Virtual Private Network) if using public Wi-Fi.

-Avoid accessing personal data on public Wi-Fi.

-Use a separate network and password for house guests and use a strong firewall.

The Future of Smart Devices

Smart devices bring convenience to a whole new level. Unfortunately, this ease of access creates an opportunity for cybercriminals. Smart devices aren't going anywhere, so it is important to know how to keep them secure.

1 Smart Watches

Smart watches allow you to track your fitness or send a a message right from your wrist. They are an extension of phones and should be treated as such when it comes to security. Disable features like microphone, camera, and location when not in use. Make sure you have security settings enabled so if your watch is stolen, it cannot be paired with new devices.

2 Smart Home Assistants

With voice-activated smart home assistants, you can turn on an alarm, unlock your smart door, or carry out many other commands. But if a hacker accesses this device remotely, they could order similar commands or even listen in on conversations or access your information. Make sure the password to access your smart home assistant is strong and utilize any additional security features offered.

3 Smart Security Cameras

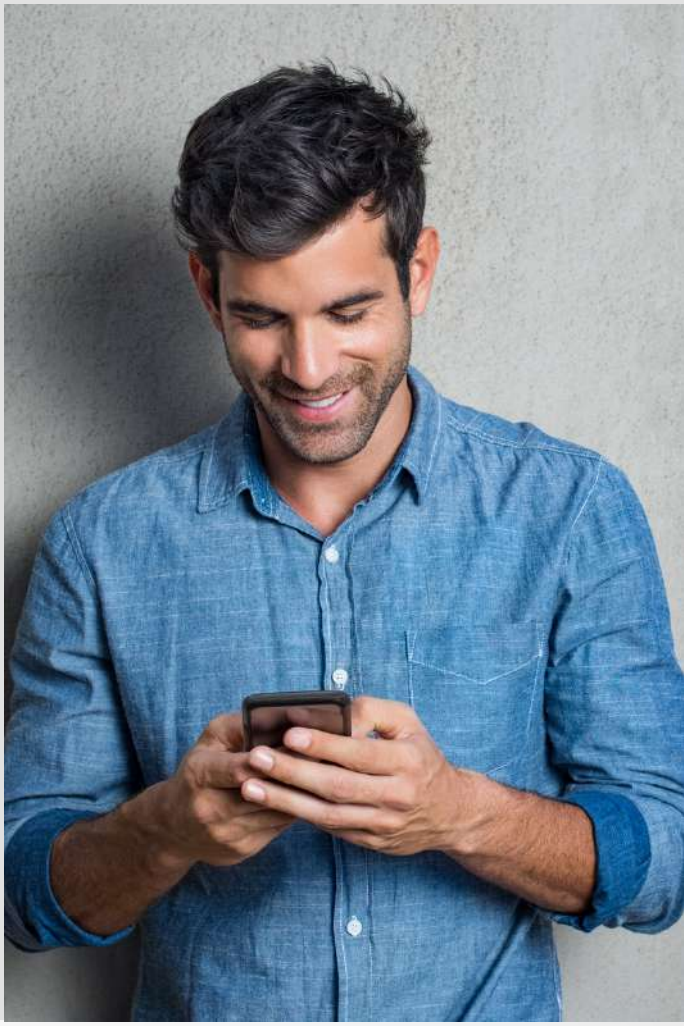
Smart security cameras are often targeted by hackers. Credential stuffing is often used to gain access. It occurs when a hacker uses your personal information to guess your account login. Wi-Fi security cameras pose an additional risk if your Wi-Fi network is not as encrypted or protected as it should be. There are ways to spot if your security camera has been hacked. Look for unusual rotations, blinking lights, or strange noises.

Smart Device Security Tips

- Utilize a strong and unique password and multi-factor authentication.
- Create a secondary Wi-Fi network for your smart devices.
- Update your smart device's operating system regularly.
- Turn devices off when not in use or disable certain settings.

SCAM OF THE MONTH

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.



Carlos was scrolling through his phone when an email notification popped up on the screen from a well-known online payment platform. He went to the email and saw that it was an invoice for a recent purchase.

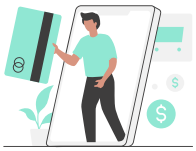
Since he had recently made a purchase through the platform, Carlos assumed this must be the invoice for that item. The seller's name sounded familiar, and the amount seemed correct. Carlos clicked on the "View and Pay Invoice" button and made the payment.

The next day, Carlos was checking his bank account and realized he had already paid for the item last week. He went back to the email from the day before and saw that it included a customer service phone number to call if the invoice was not correct. He called the number on the email to dispute the invoice and explain the situation.

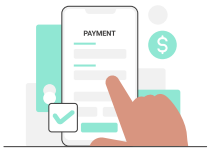
The person who answered the phone seemed helpful and told Carlos that he could reverse the transaction. All he needed to do was input the card number and details that the refund would be made to. Carlos provided his card information and left the conversation happy that the issue was resolved. Or so he thought.

Did you spot the red flags?

- Carlos did not confirm what the payment request was for. He assumed it was for a past purchase without double-checking the payment amount or seller name.
- Carlos did not check the website that the "View and Pay Invoice" button led him to for signs of a fake website. He assumed it was the legitimate payment platform.
- By calling the phone number on an email that he already knew was suspicious, Carlos put himself at even more at risk.



Always confirm customer service numbers before calling. Avoid giving away credit card details to unconfirmed phone numbers.



Keep track of your online purchases and payments. Always keep record of payments and invoices in case any issues occur.

Scammers are creating fake profiles on popular online payment platforms. They are even impersonating real people and businesses.
Be cautious of unsolicited requests or messages from payment platforms.

Key Takeaways

Scammers can access our information in more places than ever before.

With the rise of public Wi-Fi, smart devices, and new online platforms, it is important to know what risks come with new technology.

The security risks of public Wi-Fi:
While using a VPN is a great way to minimize the security risks of public Wi-Fi, it is best to access personal information at home or on a private network.

Smart devices call for increased security:
Many smart devices are not setup with security measures enabled. Make sure all smart devices are updated and have a password if possible. Turn off smart devices when they are not in use or disable features like microphones and tracking.

See Yourself in Cyber:
Educating yourself on what is new in cybersecurity, and how to keep your information safe, will make your role in cybersecurity a positive one.

Alignment

The way the body is supposed to be arranged in a yoga posture. A gentle movement or correction can create alignment and entirely modify a posture.

How does this relate to cybersecurity?

Making small changes to online habits can make a huge difference in your security posture. By doing the little things like enabling automatic updates, or using a stronger password, it can be easy to stay safe online.

Now apply this concept to cyber-awareness.

As you go throughout your day, think about all of the different devices you have that are connected to the internet.

Make the little corrections that are necessary to create alignment with good cybersecurity practices. By putting into practice the things you have learned, you will positively modify your cybersecurity posture.