BECOME A CYBER SLEUTH

Learn how to detect and avoid cybercrime

THIS MONTH'S TOPICS:

Avoid Unwanted Calls

How to spot scam calls...

Have you been Hacked?

Signs of a compromised device

Scam of the Month:

Fake App Scams...

Cyber Zen Den:

Accepting your security position...

The ever-changing techniques used by cybercriminals can be difficult to spot.

We are all affected by cybercrime more than we think. Persistent phone calls from the unknown, and deteriorating device performances are daily frustrations many people face that may be a result of a cybercriminal.

In this month's newsletter, become a cyber sleuth and learn how to detect and avoid cybercrime.

HOW TO AVOID UNWANTED CALLS

CALL BLOCKING

-Check for built-in features on smartphones.

-Download a call-blocking app.

-Check with your carrier to see what options they offer.

-Block or silence unknown callers.

REGISTER FOR THE DO NOT CALL LIST

Caller ID Spoofing
Scammers spoof local phone numbers to disguise their identities and build trust. Just because a call looks like it is local, doesn't mean it is.

Voicemail Hackers
Many voicemails are preset to allow access when called from your own phone number. Set a password on your voicemail so that hackers cannot access it.

Reporting
Let your phone carrier know if you have call-blocking enabled and are still receiving spam calls.

AVOIDING SCAM CALLS

- **Do not answer calls from unknown numbers.**
- **If you do accidentally answer a scam call, hang up immediately.**
- **Do not answer questions or press buttons on an unknown call as this verifies your number for the scammer.**

HAVE YOU BEEN HACKED?

HACKED ACCOUNTS

Signs of a hacked account:

- There are posts or messages sent from your account that you did not make
- Your name, email, or password has been changed

If your account has been hacked:

- Notify friends immediately
- Scan devices for malware
- Change passwords to all key accounts

COMPROMISED DEVICES

Signs a computer has a virus:

- Slow performance, missing files, and system crashes
- Unexpected pop-ups and applications

If your computer has a virus:

- Use an antivirus program to run a system scan
- Review recommended actions from computer scan
- Notify your organization and technical support

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.

Amanda was at the airport, waiting for her flight to board when she decided to download a game to play. Heading to the app store, she scrolled through her options.

As she looked at the different Solitaire apps, she decided on one randomly. It had five stars and looked like the typical game. Once downloaded, she was disappointed to see that it had many glitches and would not close properly.

Upon closer inspection, she realized many images on the app and on the description page in the app store were blurry and not the same as a normal game. She dismissed the app as a bad knock-off version and downloaded a new one.

Amanda did not use the old app again but soon after, her phone started having performance issues. What she didn't realize was that when she downloaded the app, her phone was infected with malware: her personal information, and account data, now exposed.

Did you spot the red flags?

- Just because an app has five stars doesn't mean it is legitimate. Look at the number of ratings, as well. Popular apps typically have thousands of ratings.
- Amanda picked an app at random without any investigation. Look for apps that give a thorough explanation of what they do and include privacy practices.
- Amanda did not delete the app or warn others after having issues with it.

Look out for apps that are difficult to close or that contain ads to suspicious sites. Research and read app reviews before downloading.

Cybercriminals make apps that look nearly identical to real apps. Look closely at visuals and logos on the app description page.

Cybercriminals create fake apps that mimic real apps and post them in the app store. If downloaded, these apps can deliver malware.

Use two-factor authentication and strong passwords for app stores and apps.

Key Takeaways

Look into call blocking options and be cautious with unknown calls.

Cybercrime often comes with many warning signs. Keep an eye out for these signs and take the necessary steps if a cybercrime does occur.

Blocking out the scammers: Enable call blocking features to stop unwanted calls. Avoid answering unknown calls or giving up personal information over the phone.

Device and account suspicions: If you notice slow performance on a device or changes to an account, these could be signs of hacking. Change passwords and scan devices if a security incident does occur.

Inspection and detection: Whether you download a new app or notice changes to an account, it is important to make regular inspections of all technology in order to detect issues.

Acceptance

In psychology, acceptance is a person's acknowledgment of a situation. It is known as the beginning of healing and can bring many benefits.

How does this relate to cybersecurity?

Accepting the current state of your cybersecurity situation is the first step towards preventing security incidents from occurring in the future.

Now apply this concept to cyber-awareness.

Be mindful throughout the day of things that could pose a security risk. Accept that there will be risks and that there is a potential for cybercrime on a daily basis.

Use what you have learned to acknowledge the situation and accept the changes that might need to be made in order to improve your digital safety.