ZOOMING IN ON CYBERSECURITY

A close analysis of computer security and fraud awareness

THIS MONTH'S TOPICS:

Computer Security

Best practices to keep computers secure

Fraud Awareness

How to prevent, spot, and report fraud

Scam of the Month:

Funeral Streaming Scams...

Monthly Cyber News:

Recent News and Upcoming Dates...

As we approach the end of the year, it's more important than ever to stay vigilant against the evolving threats of cybercrime and fraud. Cyber attacks and fraudulent schemes continue to target businesses, often exploiting human error and security vulnerabilities.

In this month's newsletter, we'll focus on actionable tips to secure your computers and protect yourself and your organization against fraud. By staying informed, practicing safe online habits, and fostering a culture of awareness, we can collectively reduce the risks and protect our online environments.

COMPUTER SECURITY

With cyber threats evolving rapidly, every business employee needs to take proactive measures to protect their computer and digital identity. By implementing the latest best practices, you can help ensure that your work devices stay secure and resistant to attacks.

BEST PRACTICES:

- **Keep software up to date.** Outdated programs are often vulnerable to malware, ransomware, and other attacks. It's important to install security updates as soon as they are available to patch vulnerabilities that hackers can exploit. Automatic updates should be enabled to ensure you never miss a crucial update.

- **Remember physical security measures.** To avoid a device being lost or stolen, do not leave devices in your vehicle when traveling. When you are in busy areas, make sure devices are safe in a bag or out of sight. Keep all devices password protected and enable remote wiping. This gives you better control of your sensitive information if a device is stolen.

- **Stay vigilant against malware and scams.** One way to avoid malware is by not clicking on unsolicited links in messages. Verify websites before interacting with them online.

TIPS AND STRATEGIES FOR FRAUD AWARENESS

Fraud can have devastating consequences financially and reputationally. Let's go over the strategies to protect yourself and your organization.

Preventing

Use caution when online. Do not click on unsolicited links. Be wary of giving out personal information over the phone.

Detecting

Check your bank and credit card statements carefully and often for any signs of fraud. If your contact information or login details have been changed, these could be signs of account compromise.

Resolving

Report signs of fraud to credit bureaus and to any organizations where fraudulent activity has occurred.

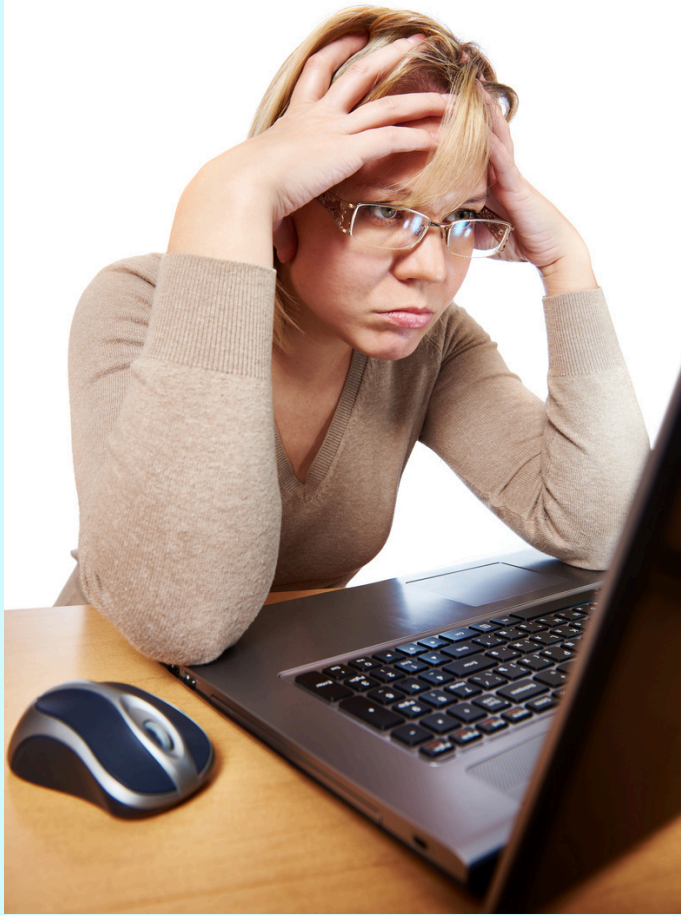
PROTECT YOUR DEVICES WITH SECURITY SOFTWARE

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.

Trish had been scrolling through social media when she received the heartbreaking news of a former colleague's passing. She wanted to find a way to pay her respects. It wasn't long before she stumbled upon a Facebook group that seemed to be organizing a live-streamed funeral for the deceased. The page appeared legitimate, featuring heartfelt messages, photos of her colleague, and detailed funeral arrangements. Trish clicked on the link to join the live stream.

Upon entering the group, she was informed that, to access the stream, she would need to pay a small fee. The website was well-designed, and the request for payment didn't seem unusual at first, given the growing trend of online events charging access fees. Without thinking twice, Trish began to enter her credit card information. Only after did she realize that the live stream wasn't real, and she had fallen for a scam.



Did you spot the red flags?

- Trish should have confirmed funeral details through those close to the deceased or through other official channels before searching for information online.
- Never provide personal or financial information unless you are certain of a website's legitimacy.

Check the funeral home's website. Often times the funeral home or family of the deceased will indicate whether the service is being live streamed and provide legitimate links to access the service for free.

Look for warning signs of fake pages and read website reviews. Some scam websites might appear professional at first, but many have subtle red flags, such as poorly written descriptions, fake reviews, or blurry designs.

CYBER NEWS

NOVEMBER
2024

SCAMS OFFER TO LOWER INTEREST RATES

Scammers are offering to lower interest rates in mortgage relief scams. These scams target homeowners looking to lower their payments through refinancing. Scammers pose as representatives from loan servicers, offering help for upfront fees or retainers. They may also urge users to stop communicating with their lender or any other contacts related to their mortgage. To avoid these scams, take your time and verify information independently. Begin by contacting your mortgage servicer or lender directly, as they can provide accurate information about your loan and legitimate options for reducing your payments.

UPCOMING DATES

November 30th is Computer Security Day. To celebrate, follow the tips in this newsletter and share them with others to make sure your friends, family, and colleagues are safe and secure.

FAKE SHOPPING WEBSITES ON THE RISE

A cybercriminal group has created thousands of fake online shopping websites in an attempt to steal user payment card details. The sites offer discounts and deals that are too good to be true. Many of these websites mimic legitimate companies such as North Face, IKEA, Wayfair, and more. Shopping scams like these typically increase around the holidays. Users should verify the URL of a website before clicking and avoid following links from ads or social media posts. Financial accounts should also be protected with any additional measures available like multi-factor authentication.