THE SEASON OF CYBER AWARENESS

The terms and to-dos for top-notch security

THIS MONTH'S TOPICS:

Cyber Clean up:
Digital Safety Checklist

The SLAM Method:
Slam Scams Before They Take Root

Scam of the Month:
Fake Job Recruiter Scams

Travel Cyber Safely:
Protect Your Data While Traveling

As the seasons change, it's the perfect time to refresh not only our homes but also our digital security. This month, we're diving into essential cybersecurity topics to keep you safe and protected.

In this issue, you'll learn how to clean up your digital safety habits, spot fraudulent job offers, stay secure while traveling, and use the SLAM method to outsmart cybercriminals. Cyber scams can spring up just about anywhere, but with the right knowledge, you can better protect yourself and your loved ones!

CYBER Clean Up

DIGITAL SAFETY CHECKLIST

Account & Password Hygiene

✅ Update Passwords – Change weak/reused passwords and consider using a password manager.

✅ Enable Multi-Factor Authentication (MFA) – Secure all important accounts with MFA.

✅ Review Saved Passwords – Remove any saved passwords from browsers, documents, or notepads and store them in a secure password manager.

Digital Decluttering

✅ Delete Unused Accounts – Close old or inactive online accounts to reduce attack opportunities.

✅ Unsubscribe from Spam Emails – Use trusted tools to manage email subscriptions.

✅ Clean Up Old Files & Downloads – Delete unnecessary documents, duplicates, and outdated files.

Device Security Check

✅ Update All Software & Apps – Ensure your OS, applications, and browsers are up to date.

✅ Run Security Scans – Scan for malware/viruses using a trusted antivirus program.

✅ Enable Automatic Updates – Turn on automatic updates for devices and apps.

WHEN CONSIDERING THE VALIDITY OF AN EMAIL, DON'T FORGET TO USE...

The SLAM Method

S — SENDER

Carefully analyze the sender's email address

L — LINKS

To see a link's true path, hover your mouse over links without clicking

A — ATTACHMENTS

Use caution when opening unsolicited or unexpected attachments

M — MESSAGE

Within the body of the email, watch for generalized greetings and "out of character" phrasing

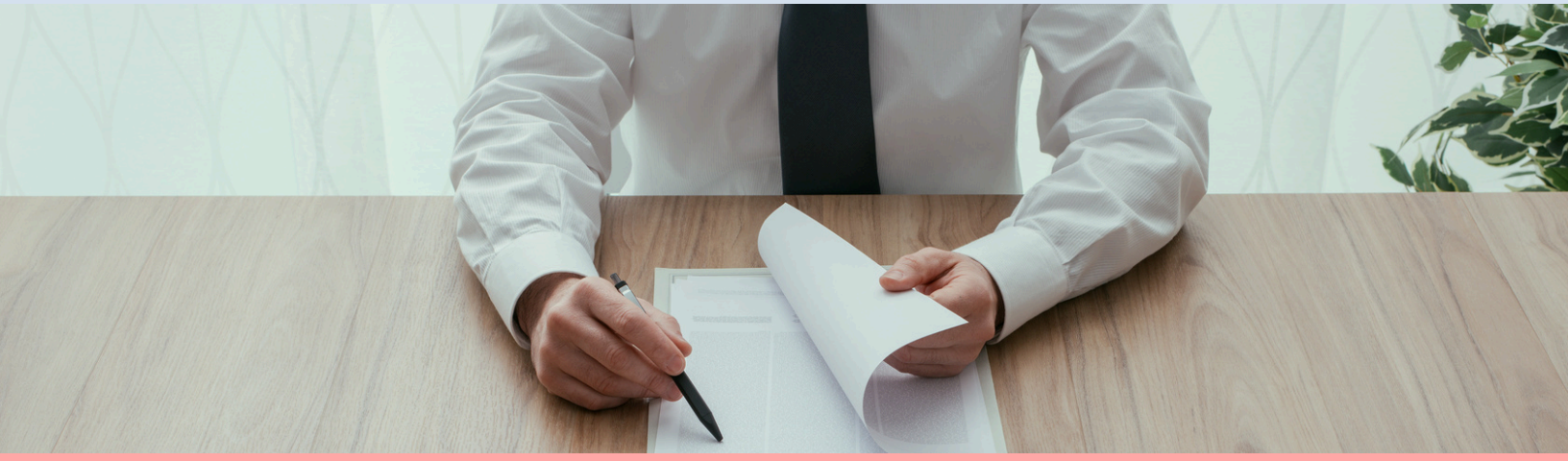
SCAM OF THE MONTH

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

Mark was scrolling through social media on his phone when he received a LinkedIn message from Sarah Collins, a recruiter for a top tech company. The role had a lot of interest, but Sarah believed from his experience that he would be a perfect fit for the job. She warned him to apply quickly though, as interviews had already started. She forwarded the application document, fast-tracked him through a text-based interview, and sent an official-looking offer.

To finalize hiring, she requested his SSN, bank details, and ID. It was then that Mark started to feel suspicious and researched the company, only to find no record of the job or Sarah. An article he read online exposed similar scams where imposters posed as recruiters to steal personal information.

Mark reported the scam to his national scam response center, and "Sarah" vanished. Lesson learned: **Always verify unsolicited messages first before interacting with them.**



DID YOU SPOT THE RED FLAGS?

- Sarah's job offer sounded too good to be true, and it was.
- Pressure tactics that create a sense of urgency are a clear red flag.

STAY SAFE

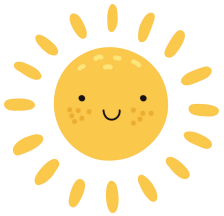
HOW TO PROTECT YOURSELF

- Social media outreach from contacts you do not know should be treated with caution. Do your due diligence and research first before interacting.
- Be skeptical of unsolicited job offers. If you're not actively looking for a job, any message about a "perfect role" is suspicious.
- Never click links or download attachments. In an unsolicited message, these things can pose a threat to your system.

TRAVEL CYBER SAFELY

BEWARE OF FAKE GIVEAWAYS AND TRAVEL DEALS

Scammers often use social media to lure travelers into clicking malicious links.

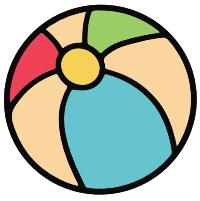


DON'T USE PUBLIC COMPUTERS FOR SENSITIVE TRANSACTIONS

Cybercriminals can install keyloggers to steal your login information.

AVOID PUBLIC WI-FI (OR USE A VPN)

Hackers can intercept your data on public networks. If possible, use a Virtual Private Network (VPN) for secure browsing.



IF YOU LOSE YOUR DEVICE

If you can't recover a lost device, **remotely erase personal data** to prevent unauthorized access.