SECURITY & AWARENESS TRAINING QUARTERLY NEWSLETTER

2025 Q4

HAVE YOU SIGNED UP FOR YOUR TECH TIPS YET?

Designed for busy professionals, these concise and practical insights take less than a minute to read, making them the perfect addition to your routine.

From safeguarding sensitive data to enhancing system security, these tips provide valuable strategies to protect yourself from ever-evolving cyber risks. Signing up is easy and completely free, empowering you to stay informed and proactive without any hassle.

Sign Up for your FREE Tech Tips Today!

CLICK HERE *or go to https://links.sysoft.ca/tip-of-the-week/*

This quarter's publication is provided courtesy of:

Alex Sochka
Director, Operations

Carl Dankwah
Technical Dispatch

What's New

Welcome to this quarter's Security & Awareness Training Newsletter.

Inside, you'll find useful tips and tools to help protect both company and personal data, along with updates on notable security news. This edition also features the fan-favourites Ask The Analyst, where we tackle common security questions with expert answers and a featured free but powerful Cybersecurity Safety Tool, VirusTotal, that could make your digital life safer.

Don't forget to weigh in on our latest Security Poll on Device & Data Security Protection and review last poll's results. Our Team Message provides seasonal tips to refresh your cybersecurity habits and finally challenge your brain with a cybersecurity-themed crossword puzzle.

Stay sharp, stay curious, and as always, think before you click.

WHAT'S INSIDE THIS ISSUE?

CYBERSECURITY ISN'T JUST ABOUT THE COMPANY — IT'S ABOUT YOU

Written By: Alex Sochka

It's easy to think of cybersecurity as something the IT team worries about — something that protects your employer from hackers, data breaches or ransomware. The truth is, every security measure we take and every good habit we practice protects you just as much as it protects the business.

When you log in to a work computer, you're connecting to a digital environment that touches both professional and personal spaces. Maybe you check your personal email during lunch, pay a bill at your online banking or sign in to a social media account on break. That's completely normal — but it also means that if a malicious actor compromises your session, they can reach far beyond company systems.

Cybercriminals don't care where the data comes from.

Once they gain a foothold — maybe through a phishing email, a weak password they take everything they can access. That could mean sensitive company nformation, but it can just as easily include your stored passwords, your personal documents, or your browser's saved logins.

Imagine opening your banking app on your work computer, not realizing that someone's already hijacked that session. They now have visibility into your credentials, and possibly your entire financial life.

It doesn't stop there.

Imagine your identity being used to phish someone else. If a hacker compromises your work credentials, they might use your name, your email, and your digital footprint to impersonate you — tricking your friends, family, or colleagues into sharing information or transferring money.

These social engineering attacks are often highly personal, using details pulled from your own accounts to make them believable. Imagine your identity being used to phish someone else.

Think of it this way: when you practice cybersecurity hygiene, you're building a digital habit that benefits you everywhere — not just at work.

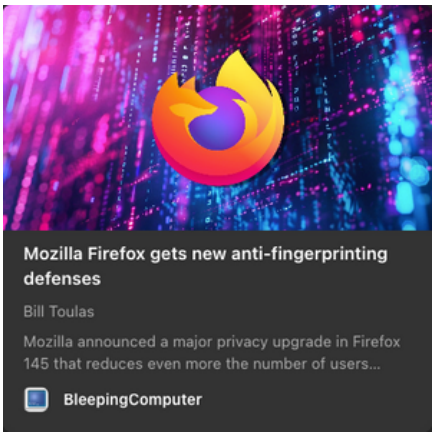
The same habits that protect your company email protect your online banking. The same awareness that helps you spot a phishing email helps you recognize a scam message in your personal inbox.

The company invests in cybersecurity because it protects its operations, reputation, and clients. But it's also an investment in you: in keeping your information safe, your identity private, and your work environment secure.

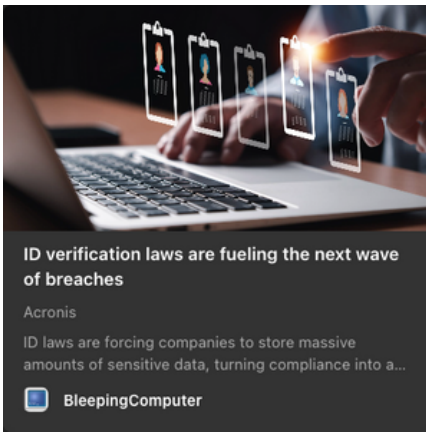
Cybersecurity isn't about fear — it's about you taking control. And by taking a few extra steps each day, you're not just doing your job — you're safeguarding your own digital life.

SECURITY NEWS

Here are a few of the latest insights, news, or updates into the ever-evolving world of IT security. From emerging threats and innovative defense strategies to regulatory changes and expert opinions, our curated selection of articles each quarter will keep you informed and prepared. Dive into these featured stories and stay ahead of the curve in safeguarding your digital landscape by clicking on the links below to read more...

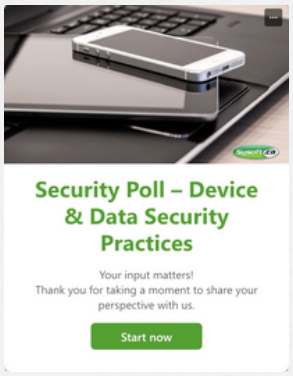


[Mozilla Firefox gets new anti-fingerprinting defenses]



[5 reasons why attackers are phishing over LinkedIn]

[ID verification laws are fueling the next wave of breaches]



2025 Q4 SECURITY POLL: DEVICE & DATA SECURITY PRACTICES

Calling all guardians of cyber space, take our security poll and help us defend you against digital threats!
Your participation in this poll is essential for strengthening how you and your colleagues protect devices and sensitive data. By reflecting on your own security habits and identifying where support is needed, you help create a safer workplace and reduce the risk of cyber threats for everyone.

https://links.sysoft.ca/securitypoll

ASK THE ANALYST

Cybersecurity can feel like a maze of unfamiliar terms, constant updates, and ever-changing threats. That's why we've created Ask the Analyst. A place where we break down common questions into clear, practical answers you can actually use.

If I only use my work computer for personal tasks once in a while, is that really a risk?

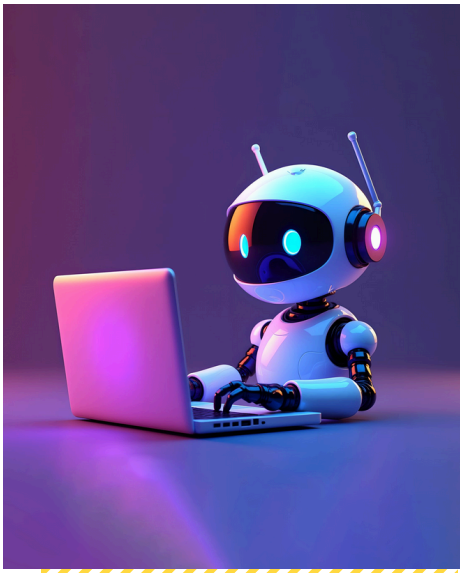
It can be — because when you use a shared or corporate system, your activity still runs through the same network, browser, and security layers that protect business data. If a threat slips in, it doesn't distinguish between work and personal content.

Whether it's an online purchase or checking a personal email, your information could be exposed in the same way. Staying alert, keeping browsers clean, and watching what links you open helps protect you, not just the company.

How can a hacker see my personal logins if I never share passwords?

Attackers often don't need your password — they hijack what's already active.

If malware or a malicious script compromises your browsing session, it can capture saved logins, session tokens, or cookies. You can lower this risk by logging out of sites when you're done, avoiding "stay signed in" options, and being cautious with attachments and pop-ups. These small habits make your



personal accounts much harder to exploit, even if a device is targeted.

If the company already has security software, why do my habits matter?

Because cybersecurity tools can only go so far — it's your clicks, logins, and decisions that matter most.

The same awareness that keeps company data safe also protects your personal privacy. When you pause before clicking a link, verify a sender, or question a pop-up, you're actively preventing someone from gaining access to your own information.

Think of cybersecurity as a shared shield — technology forms the base, but your habits keep it strong.

Do you have a question for the Analyst?
Submit your question to the asktheanalyst@sysoft.ca and if your question is answered on an upcoming newsletter you'll receive a $25 gift card!

SAFETY TOOL OF THE QUARTER

VirusTotal

As part of our ongoing commitment to helping you keep your digital environment secure, we're spotlighting a convenient security tool. These tools are chosen for their impact, ease of use, and relevance to everyday work and or personal scenarios.

This quarter, we are featuring the tool VirusTotal a quick and easy scanning tool:

https://www.virustotal.com

Ever get a strange email attachment or sketchy download link and wonder…
"Is this safe?"

Just drag and drop a file or paste a URL, and VirusTotal instantly checks it against 70+ leading antivirus engines and threat databases.

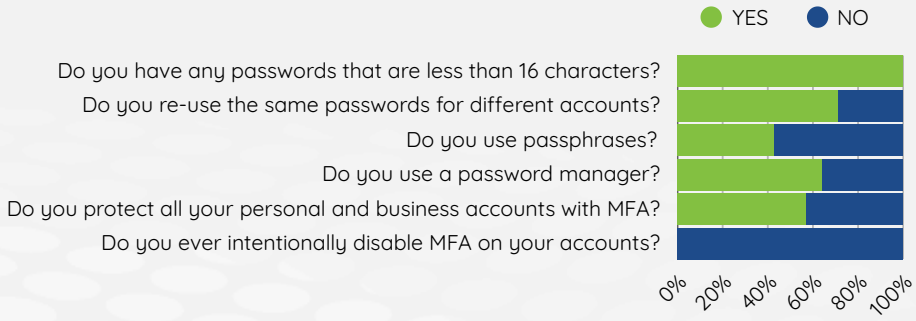
Within seconds, you'll see whether it's clean or dangerous — complete with detailed results from security vendors worldwide.

Why It's Cool:

- Works with files, links, domains, or IPs — all in one place.
- Uses cloud-based scanners, so there's nothing to install.
- Shows a quick "safe vs. flagged" summary plus deeper info for techies.
- Totally free and trusted by cybersecurity pros and everyday users alike.

Pro Tip: It's public — don't upload confidential business documents. Instead, use it for testing unknown downloads, email attachments, or USB finds before they spread trouble.

Across: 2. Breach, 6. MFA, 8. Authentication, 9. Ransomware, 10. Keylogger, 11. Firewall, 14. Backup, 16. Antivirus Down: 1. Cyber Hygiene, 3. PIPEDA, 4. Password, 5. Spear Phishing, 7. Compliance, 12. Botnet, 13. Audit, 15. Patch



2025 Q3 SECURITY POLL RESULTS

TOPIC: PASSWORDS AND MFA

An analysis reveals 3 key insights:

1) All respondents have at least one password that is less than 16 characters, which may pose a security risk despite other good practices.
2) The majority of users utilize password managers, indicating awareness of secure password practices.
3) A majority of respondents (71%) re-use the same passwords for different accounts, which increases vulnerability to security breaches.

A Message From Your Cybersecurity Team

Fall into Good Cybersecurity Habits This Season!

With autumn in full swing, nature reminds us of the beauty of change—and the importance of staying prepared. As you enjoy the vibrant colours and cooler air, we encourage you to take a moment to refresh your cybersecurity practices. Just as you layer up for the season, it's time to layer up your online security!

This fall, make it a habit to revisit your passwords and strengthen them where needed. Be especially watchful for phishing attempts and suspicious emails that might try to trick you into sharing sensitive information.

Regularly update your software and devices to patch vulnerabilities before they become a problem.

Consider enabling VPNs when working remotely and take advantage of multi-factor authentication for an extra layer of protection.

Security awareness is the key: train yourself and your teams to recognize threats, such as spyware or the dangers of shoulder surfing.

Remember, a zero trust mindset—never assuming anyone is automatically trustworthy—**is crucial to keeping you and your data safe**. And, of course, never hesitate to reach out if you notice anything unusual or need a refresher on best practices.

Warm wishes for a secure and vibrant fall, until next time.

CYBERSECURITY CROSSWORD

ACROSS

2 When information is accessed without permission.
6 Using more than one method to verify identity (Abbreviation).
8 Verifying a user's identity.
9 Malicious software that demands payment to unlock data.
10 Software that records what you type.
11 Device or program that blocks unauthorized network access.
14 A copy of data taken to restore after a loss.
16 Program that detects and removes malicious software.

DOWN

1 Good online safety habits (2 words).
3 Canadian law for protecting personal data.
4 Secret word or phrase for access.
5 Targeted attempt to trick someone into sharing information (2 words)
7 Following rules and regulations.
12 Network of infected computers controlled remotely.
13 Review of policies and practices to find weaknesses.
15 Update that fixes software issues.