SECURITY & AWARENESS TRAINING QUARTERLY NEWSLETTER

2025 Q3

What's New

Welcome to this month's issue, packed with fresh insights and engaging content to sharpen your security know-how. From headline-grabbing Security News to a featured Cool Tool that could make your digital life safer, we've got something for everyone. This edition also challenges your brain with a cybersecurity-themed Wordsearch, and features Ask The Analyst, where we tackle common security questions with expert answers.

Don't forget to weigh in on our latest Security Poll, your input helps shape future content. And finally, check out our Team Message for a quick pulse on what's happening behind the scenes.

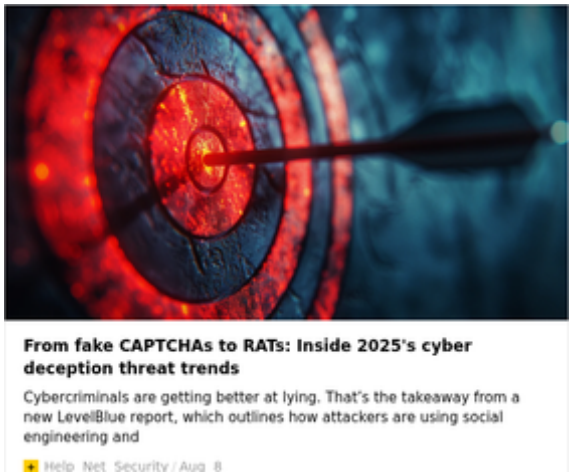
Stay sharp, stay curious, and as always, think before you click.

WHAT'S INSIDE THIS ISSUE?

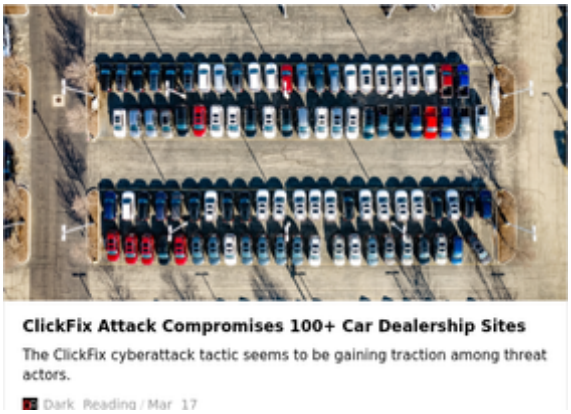
Security News

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...

[Google Calendar Malware Is on the Rise. Here's How to Stay Safe]



[From fake CAPTCHAs to RATs: Inside 2025's cyber deception threat trends]



[ClickFix Attack Compromises 100+ Car Dealership Sites]

Cool Tool

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 following website for ease of use and convenience to help ease your data breach concerns:

https://haveibeenpwned.com

Have I Been Pwned (HIBP) is a searchable database of billions of compromised accounts from known data breaches. It lets you check if your personal or work email address has been involved in any of them. It is a free and trusted online security tool that helps you find out instantly.

Step 1: Visit https://haveibeenpwned.com
Step 2: Enter an email address to search for data breaches.
Step 3: Review your results!

If the email you searched for appears in a breach, HIBP will show the name of the breached service (e.g., LinkedIn, Adobe), what kind of data was exposed (e.g., passwords, phone numbers), and when the breach occurred.

It can act like an early warning system for your online accounts. By entering your email address, you can quickly find out if your credentials have been exposed often before attackers get the chance to use them. This knowledge can prompt you to change compromised passwords immediately, adopt stronger and unique credentials for each account, and avoid the risks of password reuse. All without needing to create an account or provide any personal details beyond your email.

Wordsearch

One day, a HACKER sent a PHISHING email with a shady LINK, trying to install MALWARE, a nasty VIRUS, and some SPYWARE. Luckily, the user had strong PASSWORD practices, used a PASSWORDMANAGER, and logged in with TWOFACTOR authentication through a secure BROWSER. Their FIREWALL, ANTIVIRUS, and VPN kept most threats at bay, while ENCRYPTION protected sensitive ACCOUNT details. When a BREACH was detected, they did a quick BACKUP, ran a DELETE on infected files, and performed an UPDATE to patch the system. They avoided the SCAM, spotted the fake CAPTCHA, and remembered to UPLOAD only safe files and DOWNLOAD from trusted sources. With good PRIVACY habits and a little vigilance, they turned what could have been a disaster into just another day on the internet.

T	D	Y	J	C	R	Q	F	Z	E	C	W	D	X	G	R	P	T	Y	U	A	E	F	U	W
D	W	W	F	M	S	U	R	I	V	I	T	N	A	R	T	N	T	T	U	P	L	O	A	D
Y	M	A	H	C	T	P	A	C	Y	Q	I	B	S	L	W	L	J	K	Q	U	P	L	L	X
U	J	R	K	J	I	V	P	B	Z	X	F	U	P	D	A	T	E	V	I	S	A	F	B	G
H	Y	Q	E	I	V	A	W	C	T	L	Y	M	A	S	C	I	M	G	N	P	L	V	B	O
E	U	M	P	G	K	B	F	P	B	G	U	H	Z	V	N	I	J	C	X	Y	E	B	D	P
S	H	G	J	R	A	Q	P	I	U	W	Z	D	M	U	W	B	B	Y	A	W	N	Q	A	H
Y	S	L	N	C	M	N	W	U	H	K	Q	M	A	L	W	A	R	E	C	A	C	B	H	O
Z	B	G	S	B	B	C	A	N	R	C	C	X	G	I	F	B	W	A	S	R	R	T	Y	D
S	W	O	P	Q	E	X	G	M	Y	N	A	A	N	T	L	A	S	K	J	E	Y	B	F	A
D	Z	D	U	F	P	N	T	W	D	F	V	E	B	H	Y	F	X	G	V	F	P	A	Z	I
U	D	R	D	C	R	P	L	K	H	R	Q	A	R	P	K	I	Z	A	M	E	T	P	F	X
G	I	O	O	H	I	N	I	J	X	T	O	M	Z	B	B	U	U	A	F	V	I	Q	S	K
N	P	W	Y	C	V	G	E	E	T	F	D	W	E	L	G	L	C	Y	M	I	O	O	S	N
I	Y	S	E	W	A	U	Y	X	I	M	E	R	S	G	Y	S	K	F	R	Z	N	G	G	X
H	O	S	E	D	C	V	F	R	X	L	L	A	P	S	J	I	E	O	P	Q	R	J	D	I
S	B	A	S	V	Y	L	E	A	G	T	E	N	P	V	A	F	T	P	O	J	K	B	S	W
I	H	P	W	W	F	W	C	P	N	Z	T	R	J	O	M	P	I	K	X	Q	S	E	F	S
H	I	C	N	V	A	N	D	U	A	X	E	E	R	O	T	C	A	F	O	W	T	R	B	U
P	D	A	O	L	N	W	O	D	R	G	D	K	U	I	L	M	C	Y	W	T	F	R	L	R
I	X	C	L	O	N	C	D	B	J	G	L	C	K	J	N	A	G	H	G	A	O	D	W	I
U	L	I	N	K	C	R	W	V	F	S	Z	A	U	R	N	B	G	V	C	W	Y	G	J	V
G	H	U	R	A	F	A	U	V	P	C	U	H	U	U	H	G	R	J	S	K	G	Y	F	H
T	F	Y	C	O	O	K	I	E	E	N	G	C	V	J	K	E	U	E	H	L	E	U	Y	I
Z	Z	F	X	K	L	U	B	E	Z	X	F	X	Z	Z	E	W	R	F	X	J	P	F	G	C

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. Over time, we've noticed many of the same questions popping up from people at work and at home. Some are small but important, like "Do I really need a different password for everything?". Others tackle bigger topics, such as "What exactly does a VPN do?". If enough people are asking, it's a sign the answer is worth sharing more widely.

How can I tell if a website is secure before entering my information?

Start by checking that the web address begins with https:// (the "s" stands for "secure") and that a padlock icon appears in the address bar. Both indicate the site is using encryption to protect data in transit. Click on the padlock to view details about the site's security certificate and verify it's issued to the organization you expect. Also, watch for small red flags such as misspellings in the domain name, odd-looking subdomains, or unexpected pop-ups. While HTTPS is important, it doesn't guarantee the site itself is trustworthy so combine this check with common sense.

Why does IT keep asking me to update my software?

Software updates aren't just about adding new features. They often contain critical security patches that fix vulnerabilities attackers could exploit. Cybercriminals actively look for devices running outdated versions so they can use known flaws to break in, steal data, or install malware. By installing updates promptly, you're closing those doors before anyone can walk through them. In short, timely updates are one of the simplest and most effective ways to keep your device, and your information, safe.

What's the most common security mistake people make at work?

Some of the biggest workplace security slip-ups are surprisingly simple—and avoidable. Sharing passwords, clicking on suspicious links without verifying them, and leaving computers or mobile devices unlocked can all give attackers an easy way in. These small lapses can lead to big consequences, from data breaches to downtime. The safest approach is to keep your login details private, take a moment to verify links and attachments before clicking, and always lock your screen when stepping away, even for a minute. A little extra caution can go a long way toward protecting both you and your organization.

New Security Poll - Passwords & MFA

Calling all guardians of cyber space, take our security poll and help us defend you against digital threats!

In an age where every click, tap, or swipe could potentially lead to a security breach, it's crucial for us to band together and fortify our defenses against cyber threats. That's why we're inviting you to click the link below and participate in this quarter's set of questions.

https://links.sysoft.ca/securitypoll

Whether you're a security professional, an online user, or somewhere in between, your perspective is invaluable in our mission to protect digital realms from malicious actors. Together, let's strengthen our collective resilience and take a stand against cyber threats. Complete our security poll today and join the frontline defenders of the digital world.

Team Message

As the temperatures climb and vacation plans take shape, it's natural for our focus to shift toward relaxation, travel, and time with friends and family. But while you're unwinding, it's important to remember that cybercriminals don't take summers off. In fact, the warmer months often bring a spike in online scams, account compromise attempts, and phishing campaigns. Many designed to exploit the fact that people are away from their usual routines, using unfamiliar networks, and generally paying a little less attention to security.

If you'll be working from outside of Canada, please let us know ahead of time. This allows us to put extra safeguards in place, monitor your business account for unusual activity, and ensure your access remains both secure and uninterrupted.

Summer should be a time for making memories, not dealing with cyber incidents. So enjoy the season, stay aware, and stay safe out there!