Sysoft.ca

# SECURITY & AWARENESS TRAINING QUARTERLY NEWSLETTER

2025 Q2

## What’s New

Welcome to this month’s Security Awareness Training newsletter!

In this issue, we’ve got a wealth of valuable updates to keep you ahead of the curve. From the latest security news to debunking common misconceptions in our 'Myths vs. Facts' section, we’re here to set the record straight. Spoiler alert: Macs aren’t invincible! We’ll also dive into the results of our last Security Poll regarding phishing and introduce a brand-new one to get your thoughts on passwords and MFA.

Stay alert, stay informed, and remember - when in doubt, don’t click! Urgency is often a tactic used by cybercriminals, so always take a moment to assess before taking action.

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...

**Top 3 MS Office Exploits Hackers Use in 2025 – Stay Alert!**

Phishing Office files and CVE-2017-11882 exploits still active in 2025, exposing unpatched systems to malware.

The Hacker News

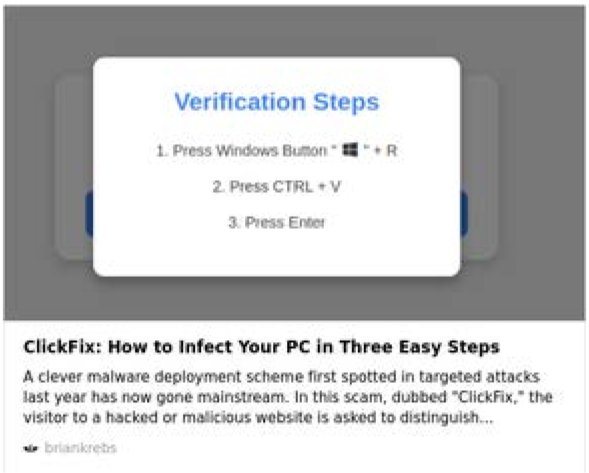
[Top 3 MS Office Exploits Hackers Use in 2025](#)

[Law Firms & Legal Departments Singled Out for Cyberattacks](#)

**Law Firms & Legal Departments Singled Out for Cyberattacks**

Cybercriminals use legal search terms to ensnare unwitting victims, then launch ransomware or business email compromise attacks.

Dark Reading / Nov 30, 2023



Verification Steps

1. Press Windows Button "⊞" + R

2. Press CTRL + V

3. Press Enter

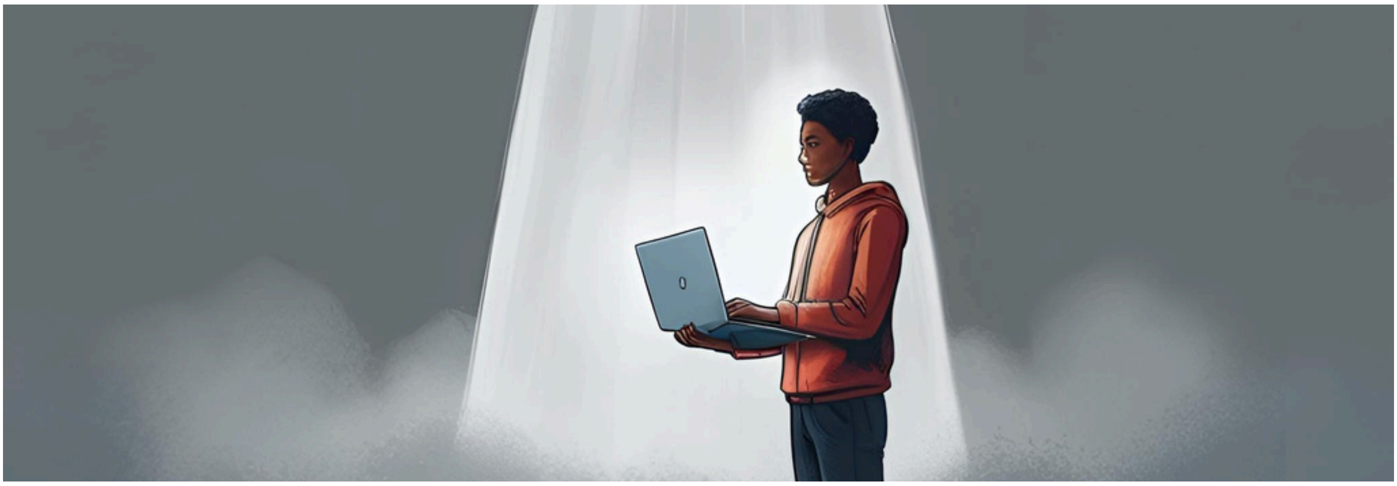
**ClickFix: How to Infect Your PC in Three Easy Steps**

A clever malware deployment scheme first spotted in targeted attacks last year has now gone mainstream. In this scam, dubbed "ClickFix," the visitor to a hacked or malicious website is asked to distinguish...

briankrebs

[ClickFix: How to Infect Your PC in Three Easy Steps](#)

# Myths vs. Facts



In today's digital age, cybersecurity is more important than ever. However, many misconceptions and myths can lead to inadequate protection and increased vulnerability. This section aims to debunk common cybersecurity myths and present the facts that will help you stay safe online.

MYTH: **My password is long, so I don’t need MFA.**

FACT: A long password alone is not enough protection, no matter how strong, passwords can still be phished, reused, or stolen in data breaches. MFA adds a critical second layer of defence, stopping attackers even if they have your password.

MTYH: **All types of MFA are secure.**

FACT: Not all types of MFA offer the same level of security. Methods like SMS codes can be intercepted through SIM swapping or phishing attacks. Stronger MFA options, such as app-based authenticators or hardware tokens, provide much better protection against these threats.

MTYH: **Cybersecrity is only the IT department’s responsibility.**

FACT: Cybersecurity is not just the responsibility of the IT department; every employee contributes to the overall security posture of an organization. While IT teams implement security tools and policies, human error remains the biggest vulnerability.

# iSecure...Right?

As Macs gain traction in the IT world, more organizations are adopting Apple devices for their reliability, and user-friendly experience. Macs have a reputation for being secure, but no system is completely immune to threats. As cyber threats continue to evolve, it's essential to stay informed about the best practices for securing your Mac. In this section, we'll start to debunk the myth of Mac invulnerability and provide practical tips to enhance your Mac's security and to keep your Mac safe. Here are some reasons why Macs might not be the fortress of security that you might think they are:

- **Mac-Specific Malware**: As Macs have grown in popularity, they have become a more attractive target for cybercriminals. Malware like Silver Sparrow and Shlayer have specifically targeted Macs

- **macOS Vulnerabilities**: Despite macOS being based on Unix, which is known for its security, it still has vulnerabilities. Hackers can exploit zero-day vulnerabilities, security flaws that are unknown to users, to gain access

- **Phishing and Social Engineering Attacks**: These attacks exploit human behavior rather than software vulnerabilities. Phishing emails and fake login pages can deceive users into disclosing personal information or installing malware

- **Built-in Security Feature Reliance**: Features like Gatekeeper and FileVault are excellent, but they are not foolproof. They may not detect sophisticated malware or protect against phishing attacks and network vulnerabilities

To stay safe, it's important to keep your Mac updated, use reliable security software, and be cautious of suspicious emails and links.

# Old Security Poll - Phishing Results

The results are in from the last security poll on phishing and it has revealed some eye-opening insights into how we perceive and respond to phishing threats. As phishing attacks continue to evolve in sophistication, these insights provide a valuable look into the current state of cybersecurity readiness. Let's dive into the results and what they mean.

**Question #1: How confident are you in your ability to identify a phishing attack?**

Our first question asked respondents how confident they are in identifying a phishing attack. While the majority expressed confidence, a notable 33% admitted they are only somewhat confident. This highlights a critical gap. Attackers rely on uncertainty and hesitation to slip past defenses. Even a small moment of doubt can lead to a successful phishing attempt. This finding underscores the importance of continuous security awareness training, real-world phishing simulations, and reinforced reporting mechanisms to boost confidence and detection accuracy.

**Question #2: Have you ever been a victim of a phishing attack?**

When asked if they had ever been a victim of a phishing attack, 30% of respondents admitted they had fallen for one. This statistic is a stark reminder of how effective phishing tactics remain, often leading to financial loss, reputational damage, or even further security breaches. Attackers continuously refine their techniques, making it easier for even security-conscious individuals to be deceived. This reinforces the need for proactive defenses, such as regular phishing simulations, multi-layered security controls, and a strong culture of reporting suspicious emails before damage occurs.

**Question #3: Have you ever received a phishing email?**

Phishing attacks are not just a possibility, they're a certainty. Every single respondent reported receiving a phishing email, confirming that these threats are a constant presence in our inboxes. What's concerning is that while some people lack confidence in identifying phishing attempts, and 30% have already fallen victim, the attacks keep coming. This highlights the need for a layered security approach: user education, robust email filtering, and rapid reporting mechanisms. Recognizing that phishing is inevitable is the first step, what matters most is how well we prepare and respond.

# Old Security Poll - Phishing Results

**Question #4: Are phishing attacks always delivered via email?**

While most respondents recognize that phishing extends beyond email, 10% still believe it’s an email-only threat. This misconception can leave organizations vulnerable, as phishing attacks are increasingly delivered through text messages (smishing), phone calls (vishing), and even social media. Cybercriminals adapt their tactics to bypass traditional email security, making it crucial to educate users on the diverse ways phishing attempts can occur. Strengthening awareness across all communication channels is key to staying ahead of evolving threats.

**Question #5: Do you know what steps to take if you suspect that you may have been phished?**

Encouragingly, 86% of respondents reported knowing what steps to take if they suspect they've been phished. However, that still leaves a concerning 14% who may not be prepared to respond effectively. Quick action is critical in minimizing damage, whether it’s reporting the incident to IT or securing accounts. Clear, well-communicated response protocols should be in place so that everyone knows exactly what to do in the event of a phishing attempt because speed and awareness can make all the difference.

**Question #6: Would you be apprehensive to let anyone know if you had been phished due to disciplinary concerns?**

Transparency is key in mitigating phishing threats, and the results are reassuring because 95% of respondents said they would not hesitate to report a phishing incident due to disciplinary concerns. This is a positive sign that organizations are fostering a culture where reporting security incidents is encouraged rather than punished. Prompt reporting allows IT teams to take swift action, reducing the risk of data breaches or financial loss. However, it’s essential to ensure that the remaining 5% also feel safe coming forward, as hesitation in reporting can allow an attack to escalate unchecked.

**Question #7: Do you participate in your organization's monthly Security and Awareness Training courses?**

A concerning 19% of respondents indicated that they do not participate in their organization's monthly Security Awareness Training (SAT) courses. This training is crucial for minimizing human error, which is responsible for a significant portion of security breaches. Staying informed and up to date on best practices is essential to protect both personal and company data from evolving threats. It’s vital that all employees engage in these courses, as the more aware and prepared the team is, the stronger the defense against cyberattacks.

# 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.

Security Poll - Passwords & MFA

Your input matters! This security poll is here to gather your thoughts on passwords and MFA. Take a moment to share your perspective with us. Thank you.

# Team Message

As part of our team's ongoing commitment to security awareness training, we want to remind you of the importance of staying vigilant against attacks personally and professionally.

Some ways to protect yourself include always verifying a sender's identity, not clicking on suspicious links, and never sharing sensitive information without confirming the authenticity of the request.

Protecting your passwords is also crucial to safeguarding your digital identify from being used fraudulently or maliciously.

- Use long and strong passwords
- Do not re-use passwords
- Always enable MFA (Multi-Factor Authentication)

By following these tips, you can significantly reduce the risk of unauthorized access to your accounts. Stay vigilant and protect your digital identity.