CYBERSECURITY MYTH VS. FACT

What you think you know could put you at risk

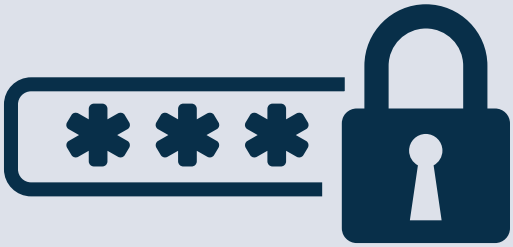
THIS MONTH'S TOPICS:

Cybersecurity is full of advice, warnings, and quick tips—but not all of it is accurate. In fact, some of the most common “best practices” are actually myths that can leave you more vulnerable than protected. Believing these myths can create a false sense of security, making it easier for cybercriminals to sneak past your defenses.

This month, we’re setting the record straight. In this issue, you’ll discover the truth behind three of the most widespread cybersecurity myths, learn why they can put you at risk, and gain simple, effective steps you can take to stay safe. Knowledge is your strongest defense. Let’s separate fact from fiction together.

MYTH #1: STRONG PASSWORDS ARE ENOUGH.

Fact: Even the strongest password can be stolen through data breaches, phishing scams, or reused credentials. Hackers often buy or trade stolen password databases on the dark web, making "strong" passwords just as vulnerable as weak ones if they're compromised.



Example: A law firm employee used a strong password, but it was leaked in a past breach and sold online. Hackers reused it to break into the firm's email.

What You Should Do:

- **Enable MFA on accounts when available.** Even if a password is stolen, an attacker can't log in without the second factor.
- **Don't share passwords.** Keep them private, even with trusted coworkers or family.
- **Use a password manager.** It creates strong, unique passwords for every account so you don't have to remember them.
- **Turn on login alerts.** Many accounts can notify you if a new device signs in.
- **Avoid password recycling.** Never reuse passwords across multiple accounts.

Key Takeaway:
A password is just the first lock—MFA is the deadbolt.

MYTH #2: HACKERS ONLY TARGET BIG COMPANIES.

Fact: In reality, small and mid-sized businesses are often prime targets because they tend to have weaker defenses. According to recent reports, nearly half of all cyberattacks are aimed at small businesses. Attackers know that one untrained employee or one outdated system can open the door.

Example: A small dentist's office fell victim to ransomware after an employee clicked a fake billing email. Patient data remained locked unless a ransom was paid.

What You Should Do:

- **Stay alert to phishing.** Regardless of your company's size, think before you click links or open attachments—attackers count on quick clicks.
- **Report suspicious emails.** Flagging them early helps protect the whole organization.
- **Update regularly.** Keeping software, apps, and devices patched helps businesses of all sizes close known vulnerabilities.
- **Back up your data.** Regular backups mean you won't be stuck paying a ransom if files are encrypted.

Key Takeaway:
No company is immune to cyber threats.

MYTH #3: PUBLIC WI-FI IS ALWAYS SAFE.

Fact: Even if a public Wi-Fi network is password protected, that doesn't mean it's safe. Everyone who connects to that network shares the same access point, which allows hackers to intercept traffic, launch man-in-the-middle attacks, or set up fake "look-alike" hotspots.

Example: A traveler connected to "Airport_Free_WiFi," not realizing it was a fake hotspot. The attacker captured their email login immediately.

What You Should Do:

- **Use a VPN.** It encrypts your internet traffic, even on unsecured networks.
- **Rely on your mobile hotspot.** Cellular connections are safer than shared Wi-Fi.
- **Verify the network.** Ask staff for the exact Wi-Fi name before connecting to avoid "evil twin" hotspots.
- **Turn off auto-connect.** Disable settings that automatically join open Wi-Fi networks.
- **Avoid sensitive activity.** Don't log into bank or work accounts unless you're on a trusted, secure connection.

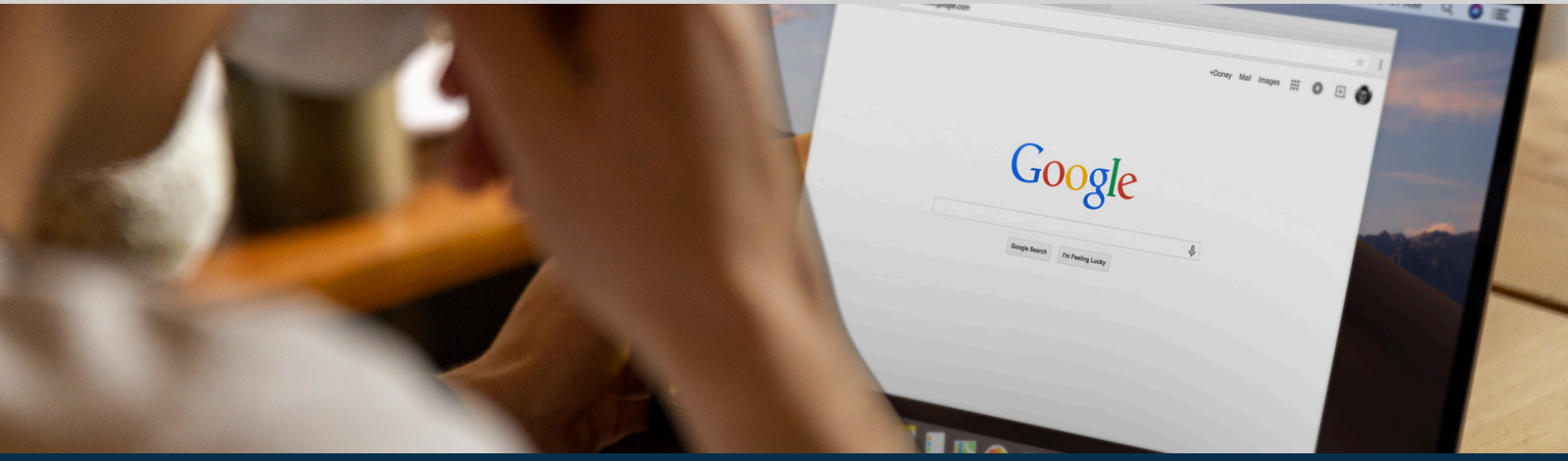
Key Takeaway:
Public Wi-Fi is risky. Use a VPN or mobile hotspot instead.

SCAM OF THE MONTH: BRUSHING SCAMS

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

Last month, Carla started receiving small packages on her doorstep—things she had never ordered, like cheap phone cases and a pair of novelty sunglasses. At first, she thought it was a shipping mistake and tried to return them, but there was no sender information. More packages arrived over the next two weeks, and it became clear something strange was going on.

What Carla didn't realize is that she was caught in a brushing scam. Fraudulent sellers had created fake accounts in her name and used her address to "prove" deliveries were made. This allowed them to post glowing reviews under her identity, boosting their products online. While the items seemed harmless, the scam meant her personal information was exposed and being misused without her consent.



DID YOU SPOT THE RED FLAGS?

- Receiving packages you didn't order is a red flag. Unexpected deliveries with no clear sender are a major warning sign.
- Lack of return information or suspiciously cheap items. Scam products are usually low-value goods with no way to trace the source.

STAY SAFE

HOW TO PROTECT YOURSELF

- Report the packages to the retailer or platform (like Amazon, Walmart, etc.) so they can investigate and shut down fraudulent sellers.
- Monitor your accounts and credit reports to ensure your personal information hasn't been stolen or misused elsewhere.