DON'T TAKE THE BAIT

Inside today's phishing attacks and
the social engineering behind them

THIS MONTH'S TOPICS:

Phishing scams continue to be one of the most common and effective cyber threats because they exploit human trust rather than technical flaws. From convincing emails and messages to fake Wi-Fi networks designed to steal sensitive data, attackers are constantly refining their tactics.

This month's newsletter explores real-life phishing scams and their impact, breaks down the social engineering techniques behind them, and outlines the critical steps to take if you ever fall victim—so you can recognize threats faster and respond with confidence.

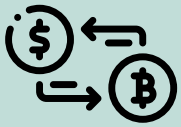
REAL WORLD PHISHING SCAMS AND THEIR IMPACT

Phishing is a real threat with real consequences for everyday people and organizations. Scammers are constantly evolving their tactics, exploiting trust, urgency, and emotions to deceive victims into handing over sensitive information or transferring funds. Understanding real incidents helps underscore why vigilance matters.

In one high-profile example from 2025, a New York City property management firm (Milford Entities/Management) allegedly lost nearly $19 million after employees were tricked by a single phishing email impersonating the Battery Park City Authority. The fraudulent message convinced staff to transfer large ground-lease and tax payments into a bogus bank account, prompting a multi-agency investigation by the Department of Homeland Security.

Back in 2020, Twitter suffered a major security breach when attackers successfully used spear phishing and social engineering to compromise employee login credentials and gain access to internal administrative tools. Once inside Twitter's internal systems, the hackers used the stolen access to take control of about 130 high-profile Twitter accounts, including those of celebrities, politicians, and major brands.

In Beaver County, Pennsylvania, a woman lost $87,000 after falling for a phishing scam that began with a fake Apple security alert on her computer. The pop-up prompted her to call a phone number, where scammers posing as Apple support claimed her computer and bank accounts were compromised. They convinced her to withdraw large sums of cash and deposit the money into a Bitcoin ATM.



Social Engineering

Tricks Scammers Use to Manipulate Humans

Urgency

Scammers create pressure by claiming an account will be locked, a payment is overdue, or immediate action is required. When people feel rushed, they're more likely to click links, share information, or bypass normal verification steps.

Authority Impersonation

Attackers pose as trusted figures—IT support, executives, banks, healthcare providers, or government agencies—to gain instant credibility. When a message appears to come from someone "important," victims may comply without questioning it.

Fear/Reassurance

A message might warn that your data has been compromised, followed by a promise to "fix" the problem if you act quickly. This emotional rollercoaster keeps victims focused on resolving the issue rather than spotting red flags.

Familiarity/Trust

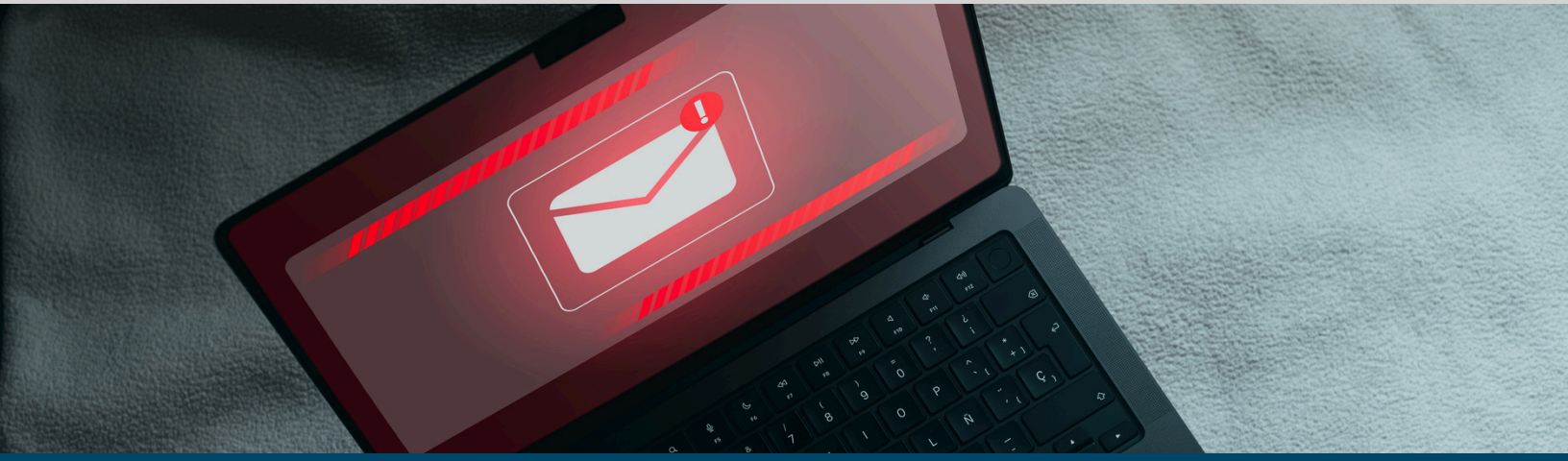
Phishing messages may reference coworkers, brands, or routine activities to appear legitimate. In some cases, attackers even hijack real accounts, making fraudulent messages look completely authentic.

SCAM OF THE MONTH: EVIL TWIN SCAMS

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

Emma stopped at her favorite coffee shop before work and opened her laptop to check email. When she searched for Wi-Fi, she saw two similar network names and connected to what she assumed was the café's guest network. A familiar login page appeared, asking her to re-enter her email and password, and she didn't think twice.

Unbeknownst to Emma, the network was an Evil Twin hotspot created by a scammer sitting nearby. Designed to look legitimate, the fake network captured her credentials the moment she entered them. Later that day, Emma received alerts that her email password had been changed. Attackers used the compromised account to attempt access to other services, turning a quick coffee break into hours of account recovery and security checks. Evil Twin scams can lead to stolen credentials, account takeovers, and long-lasting damage to both personal and workplace security—all without victims realizing they were ever under attack.



DID YOU SPOT THE RED FLAGS?

- Seeing more than one network that looks like the official café Wi-Fi is a common sign of an Evil Twin hotspot.
- Legitimate public networks rarely ask users to re-enter email passwords—especially personal or work credentials—just to access the internet.

HOW TO PROTECT YOURSELF

- Ask a staff member for the exact network name and avoid connecting to similarly named or unfamiliar Wi-Fi networks.
- Never log in to email, banking, or work accounts on public networks unless you're using a trusted VPN or your mobile hotspot.

Act Fast After a Phish

IMMEDIATE STEPS TO TAKE AFTER AN ATTACK

Stop engaging immediately.

Immediately stop interacting with the message. Close the email or text, avoid clicking additional links or attachments, and disconnect from the internet if directed by your IT or security team.

Change your passwords right away.

Update passwords for any accounts that may have been affected, starting with email accounts. Make sure new passwords are strong and unique, and enable multi-factor authentication where available.

Report the incident.

Notify your IT department, security team, or supervisor as soon as possible. Early reporting helps organizations investigate the threat, block similar messages, and protect others from falling victim to the same scam.

Monitor your accounts closely.

Watch for unexpected password reset emails, login alerts, or unusual activity on financial, work, and personal accounts. The sooner suspicious behavior is caught, the easier it is to contain.

Learn from the experience.

Use the incident as a learning opportunity to recognize what went wrong—whether it was urgency, impersonation, or a convincing message—and apply that awareness moving forward.