Fraud Awareness & Risk Management:
Fending Off Phishing Attacks

Cyber fraud remains a concern for business leaders, as the prevalence of cyberattacks continues to escalate. As businesses enhance their strategies, cybercriminals are equally enhancing their tactics, aiming to outwit established safeguards. This trend has led to businesses shouldering more of the responsibility to combat cybercrime.

What Is Phishing?

Phishing is a form of social engineering or scam where attackers deceive people into revealing sensitive information or installing malware such as ransomware. Phishing usually involves an attacker impersonating someone you know using a platform that you trust. Phishing most frequently comes in the form of an email, a Business Email Compromise (BEC) attack, from individuals outside the organization. Treasury and accounting staff discover the majority of payments fraud.

Types of Phishing

Business Email Compromise (BEC)

BEC is a sophisticated scam compromising legit email accounts, typically to fraudulently obtain funds, sensitive data, or intellectual property.

Spam filters defend us from a raft of suspicious emails, but occasionally a malicious email can sneak into our inbox sent from a hacked or impersonated account. A BEC can be challenging to detect and, as one of the most financially damaging cybercrimes, costly to resolve. Fortunately, security precautions and employee training can help prevent these crimes.

In 2022 the FBI received nearly 21,832 BEC complaints with adjusted losses over $2.7 billion.[1]

Smishing

Smishing is a cybersecurity attack using text messages to trick victims into clicking malicious links. “Smishing,” a clever portmanteau combining “SMS” (aka “texting”) and “phishing,” falls in the phishing category of scams. Victims receive text messages with malicious links that can download malware or redirect recipients to illegitimate websites that request sensitive information. Like BEC, smishing can wreak havoc for your business, but proactive measures can help prevent attacks.

continue >

How Can You Avoid Phishing?

Get employees up to speed on cybersecurity best practices

- Never open emails or attachments from unknown senders
- Watch for any changes in email addresses that mimic real ones
- Be cautious when clicking links

Be vigilant, and encourage employees with company-owned devices to do the same

- Be suspicious of unsolicited texts and emails
- Be wary of "urgent" messages and requests
- Avoid sending sensitive information — it's atypical a legitimate institution would even ask for such information

Opt to take the conversation off-line

- Contact the purported sender directly via phone to verify the source
- Block, don't respond — even requesting to UNSUBSCRIBE proves your phone number is real and active, inviting future attempts

Keeping up with the fast pace of emerging cyber fraud can feel overwhelming, but the right tools, tactics, and actions can help keep you in control. Webster is here with the guidance, products, and expertise to help protect your business against the risks of cyberattacks.

Received a fraudulent or suspicious email that appears to be from Webster Bank?

Contact a Webster Relationship Manager or call 888-932-2256.

Want more information on protecting your company from cyber threats?
Connect with Webster Bank.

[1] Source: FBI Internet Crime Report 2022.

COM-WP 0923