# Fraud Awareness & Risk Management:

## Fending Off Phishing, Business Email Compromise, and Fraud

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 Business Email Compromise (BEC) aka 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.

In 2023 the FBI received **21,489 BEC complaints,** amounting to $2.9 billion in reported losses.[1]

### Types of Phishing

- **Business Email Compromise (BEC) or CEO/CFO Fraud**

  BEC is a sophisticated **scam compromising legitimate 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.

- **Vishing**

  Vishing, short for “voice phishing,” is a type of **fraud attempt over the phone**, often using the same interactive voice response (IVR) technology used by financial institutions. Attackers typically send a message disguised as coming from a bank, government institution, or another trustworthy entity requesting a callback. The callback number pushes the victim to the attacker’s IVR technology, which prompts them to enter their account information and/or PIN, putting their sensitive information in the hands of the cybercriminal.

continue >

- **Smishing**

  Smishing is a **fraud attempt 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.

- **Clone Phishing**

  With "clone phishing," **a fraudster replicates a previous message** between an employer and employee with one key difference — the cloned email includes an attachment embedded with malware.

  Because the sender's email address and the style and substance of the email text match the original message, recipients have no reason to doubt the legitimacy. So, they're more likely to fall for the attacker's trap and click on the malicious attachment.

- **Spear Phishing**

  Unlike regular phishing, which casts a wide net, **spear phishing zeroes in on a specific organization or group of entities**, e.g., a government agent from one country targeting another country to learn sensitive intel. Attackers research their victims and tailor their messages accordingly so the bait appears more credible.

- **Whaling**

  Like phishing, whaling uses email and website spoofing to trick individuals — but with an added social engineering element. Masquerading as influential leaders in an organization, **attackers target other key individuals**, like the CEO or finance manager, in hopes of gaining access to computer systems or stealing money or sensitive data. The tactic presumes staff are more likely to divulge information or follow along when the request comes from another "big fish" or "whale" in the organization.

## How Can You Avoid Phishing?

### Coach employees to trust but verify emails

- 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 offline

- 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.

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

[1] https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf



COM-WP 06/24