Cybersecurity

Understanding these social engineering attacks and mitigating the risks

FIFTH THIRD BANK

	Business Email Compromise (BEC)	Spoofing	Ransomware	Phishing
What is it?	An email attack, sometimes referred to as CEO Fraud, using a compromised executive's email account or the compromised email account of a supplier with a longstanding relationship. Often sent to employees with access to finances, payroll data and other personally identifiable information.	An attack (email, caller ID or website) in which the attacker pretends to be someone else by falsifying data (sender address, phone number, URL).	A type of malware that prevents users from accessing their system or files and demands a ransom payment to regain access. Paying the ransom does not guarantee access.	Email campaigns crafted specifically for a target that often contain links directing recipients to malicious sites or attachments infected with malware, and often include a sense of urgency.
Goals	Defraud the company, its employees, customers or partners	• Gain the victim's confidence • Get access to systems • Steal data • Steal money • Spread malware	Financial gain by: • Scaring the user • Threatening the user • Encrypting files	• Financial gain • Steal intellectual property • Disrupt business • Damage reputation
How users can protect your organization	• Exercise caution when reviewing emails, especially unexpected emails from executives or suppliers • Be wary of emails with sense of urgency • Always follow standard company verification procedures and processes • Contact the executive or supplier to confirm the request	• Exercise caution when reviewing emails or phone calls • Carefully check the sender address and the accuracy of the spelling of the sender's name • For questionable emails or phone calls, contact the sender directly, using a known email or phone number to confirm the request	Prevent it from happening to begin with by: • Exercising caution when reviewing emails • Avoid clicking links • Be wary of attachments	• Exercise caution when reviewing emails • Avoid clicking links—hover over them to review the real URL • Be wary of attachments—never open from unknown senders • Right click on the From address for more details about the sender
What can organizations do?	• Backup systems regularly • Invest in good cybersecurity technology • Patch & update software regularly • Educate users			

Continued ▶

Business Checklist

Effective actions businesses can take to protect their own network, company and clients.

Protect the Money

- □ Monitor accounts regularly—leverage push notifications
- □ Utilize two-factor authentication sign on
- □ If you're a small business, consider adhering to an FBI recommendation to dedicate one computer to handle online banking activity

Encourage Users to Secure Communications

- □ Create secure passwords
  - Don't reuse passwords
  - Use a unique password for each account
  - Avoid sharing
  - Create passwords that are long and strong
- □ Avoid public Wi-Fi networks
- □ Do not use personal email for business
- □ Surf safely
- □ Never enter personal or customer-specific information into a public computer

Be Prepared—It's Not a Matter of "If"

- □ Retain an expert cybersecurity firm that can:
  - Provide initial diagnostics of risks and provide regular checkups
  - Perform "white hat" simulated cyber attack tests to identify weak points
- □ Consider cyber insurance coverage to cover:
  - Breach Response
  - Cyber Extortion
  - Network Interruption
  - Data Restoration
  - IT Forensics
- □ Adopt an Incident Response Plan
- □ Take a data inventory
- □ Identify the operation's "crown jewels"
- □ Establish a procedure employees should use if they think their computer may be infected
- □ Make sure all employees use good security habits and establish a security awareness and education program
- □ Regularly check for external accounts imitating the company or people within the company

Practice Security Hygiene

- □ Use an up-to-date browser and apply patches regularly*
- □ Install and regularly update security tools (anti-virus, anti-spyware, firewalls, etc.)*
- □ If your company has internet sites, incorporate intrusion detection and vulnerability management tools
- □ Turn off and remove services that are not needed, like USB drives*
- □ Use a mail service that blocks or removes email file attachments commonly used to spread viruses
- □ Ensure only approved company applications are deployed and keep them patched*
- □ Install pop-up blockers on your system
- □ Make sure your networking equipment and computers are supported by the manufacturer
- □ Dispose of your network, computer and mobile devices safely

Implement Security Measures

- □ Restrict access to information
  - Individuals with access to personal information should have the minimum access necessary to perform duties
- □ Regularly back up critical data
- □ Implement procedures for verifying urgent wire transfer orders
- □ Minimize the number of individuals who can approve or conduct wire
- □ Be aware of third-party risk— you're only as strong as your weakest third party

Fifth Third Bank

For more information on how Fifth Third protects you, visit 53.com/privacy-security

*Indicates basic system hygiene

Fifth Third Bank, National Association. Member FDIC.