Email security isn’t just about company secrets—it’s the number one way cyber-criminals gain access to financial accounts. And if your company has fallen victim to a cyber-crime, you’re not alone. U.S. companies lose an average of $15.4 million per year to cyber-crime, according to research conducted by the Ponemon Institute of Cyber Crime and sponsored by Hewlett Packard Enterprise. Unfortunately in many cases, employees are unwitting accomplices—through common email practices and habits.

As email has become a standard mode of business communication, it has become a common starting point for online fraud and identity theft. Cyber-criminals constantly find new and ingenious ways to exploit email. Once an email account is compromised, the thief can fraudulently gain access to corporate or consumer cash, or simply disrupt daily business operations by disseminating malware and viruses.

Cyber-criminals understand how to fool unsuspecting employees into cooperation. Many perpetrators use sophisticated tools to research their victims and identify vulnerable points of access or manipulation. Perpetrators may be individuals or, increasingly, may belong to an organized group, whether domestic or international, that targets companies globally.

The Rise of Social Engineering

Many forms of online or offline business fraud are based on the concept of social engineering, in which the perpetrator psychologically manipulates an employee into taking action that will ultimately cost your company time and money.
Typical approaches are based on these well-intentioned actions:

- Transferring cash
- Divulging login data or account numbers
- Executing a wire transfer
- Downloading malicious software
- Allowing someone to remotely control the employee’s computer

In fact, social engineering preys on your employees’ good intentions. Most professionals, from rank-and-file to senior leadership, are motivated to help clients, solve problems quickly and protect their own positions. Faced with a seemingly legitimate request for assistance, a well-meaning employee will naturally respond to a carefully crafted fraudulent request without pausing to consider fraud risk.

**Phishing**

Have you ever received an email that seems to be from a well-known company—but something seems off? Phishing relies heavily on social engineering, often by exploiting the public trust in well-known corporate brand names. Phishing emails and websites can be very convincing and closely mimic legitimate brands.

First, the perpetrator sends an email message that appears to be from a legitimate, recognizable company, asking the recipient to verify their account or update their billing information by clicking a link. The link opens an online form or web page that appears genuine—but actually was created by the cyber-criminal to collect logins, account numbers or other sensitive data from gullible users.

Variations include spear phishing (targeting individuals), vishing (phishing via telephone or in a face-to-face encounter) and SMiShing (via SMS text messaging).

**Email Account Hijacking**

Even in our password-protected society, an email account hijacker is able to take control of an account and use it to send emails, often spreading malware or viruses.

Attackers may hijack hundreds of accounts at once, or target an individual user to gain control of their identity and access to confidential information. Cyber-criminals can also hijack online accounts, including those used for cloud-based services, or even an entire desktop computer or server.

**Business Email Compromise (BEC)**

Companies that regularly make wire transfer payments to foreign suppliers or other businesses are particularly at risk for BEC scams, in which an employee unwittingly authorizes a wire transfer or electronic check payment to a wrongdoer.

BEC attackers typically research their victims to target those in a position to execute large electronic cash transfers, and use phishing tactics and/or email hijacking to do their dirty work.

In a common scenario, someone masquerading as the CEO emails the corporate controller with an “urgent” request for a funds transfer to a particular trade account. Or, a “vendor” sends an urgent demand for payment to ensure continued delivery of goods or access to an account.

**What Can You Do? Train, Test, Repeat.**

While no one can predict every form of cyber-crime and fraud, every company can protect itself by training employees in ways to safeguard sensitive data and protect corporate resources. Most important, employees should understand—and always follow—company policies and practices regarding Internet safety.

One-time training is not enough. Ongoing awareness and periodic testing will help keep employees on the lookout for email intruders and imposters, and in compliance with security policies. Critical email policies include the following:

- **When in doubt, delete.**
  
  Advise employees to avoid downloading “.exe” attachments that may introduce malware or viruses, and possibly infect the computer—or even the entire corporate network. These emails should be deleted without opening.
• **Remember “stranger danger.”**
  Employees should never click on an unfamiliar link embedded in an email from an unknown or questionable source, or provide confidential information in response to an unsolicited email or SMS text message. Nor should employees trust an email from someone unfamiliar that is unexpected or appears unprofessional, and requests sensitive information.

• **Keep passwords strong—and secret.**
  Email and online account passwords should be long, with a mix of uppercase and lowercase letters, numbers and symbols, and employees should be prompted to change them regularly. All passwords should be kept private—not displayed on sticky notes around the computer monitor—and should never be provided via email.

• **Stay suspicious.**
  Employees should be especially mindful of emails requesting specific and significant cash transfers—especially if the CEO or CFO is on vacation. If an email requests an “urgent” electronic payment, the employee should contact the requesting person or organization directly via a trusted phone number to confirm whether the request is valid. Bear in mind that neither KeyBank nor any other responsible major corporation will ever send unsolicited requests for sensitive information.

• **Keep software up to date.**
  Employees should be reminded to keep software and security “patches” up to date on their work and personal computers.

---

**Cultivating Cyber-Crime Resistance**

Use periodic testing and other communications to maintain strong awareness of cyber-crime. For example, your IT team can create a mock phishing attack to test employee responses, with follow-up education about just how convincing email fraudsters can be.

Other steps include:

• Keep employees informed of new kinds of cyber-crime that might infiltrate their inboxes. Enlist your marketing and communications team to help keep your email compliance communications fresh and engaging.

• Provide a clear process through which employees can report suspicious activity in their email account and other potential cyber-crime threats.

• Monitor your accounts closely.

• Instill operational practices that help mitigate cyber-crime risk. For example, wire or check transfers over a certain amount should be a two-person task—one to approve the transfer and one to execute it.

• Ask your bank about possible tools for mitigating fraud risk.

Cyber-crime is a threat for all businesses, but smart policies and consistent employee training can help you stay a step ahead of the perpetrators.