KeyBank


# Fraud and the workplace: Getting employees involved

There are many steps a business can take to prevent fraud, but it can't be done without its employees. The following are various ways staff can help protect their company—and themselves.

## Prevention at a glance

### Be aware and be safe

- Monitor accounts daily and closely.
- Be suspicious of any unsolicited emails, phone calls or text messages with an urgent request for personal or company financial information, from both known and unknown senders.
- Never log in to online banking accounts via a link or Internet address provided in an email or text message.
- Never use "favorites" to access a website where you plan to disclose private information—type the URL into your browser's address bar.
- Only enter financial or account information on sites that have the lock icon displayed in the browser and https preceding the URL.

### Be vigilant with emails

- Do not open unsolicited, suspicious emails or emails from unknown senders—delete them. If one is opened, never click on links or open attachments.
- When receiving a message from a known sender, do not open an attachment before checking with them through a known phone number/email address for validity.
- Email appearing to come from a trusted source could be fraudulent and contain a virus, Trojan horse, worm or other malware.
- Do not share your email address with random sources.
- Never provide personal information requested via pop-up windows or email.

## Remember: It can happen to anyone

Fraud is a threat for all businesses, but smart policies and consistent employee training can help companies stay a step ahead of perpetrators.

### When in doubt, delete

Employees should 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"

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 familiar that is unexpected or appears unprofessional and requests sensitive information.

### Keep passwords strong—and secret

Email and online account passwords should be complex, with a mix of uppercase and lowercase letters, numbers and symbols, and employees should change them yearly or when suspected fraud has occurred. 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 electronic payments—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.

**If you suspect you are a victim of fraud or malware, call Key's Fraud and Disputes Hotline directly at 1-800-433-0124. Then contact your Relationship Manager to make them aware of the issue.**

**To learn more, contact your Relationship Manager, or visit key.com/security.**