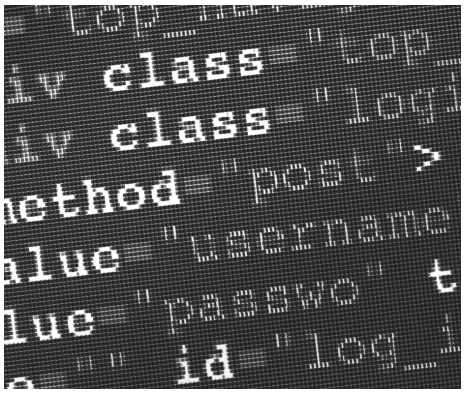
How to help protect your company from fraud

Technology is getting better – but so are the cyber-crooks

Fraud is as old as commerce itself. Today, the threat of fraud often centers on the continually evolving technologies used to conduct business and online banking. In the 2011 Association for Financial Professionals (AFP) Fraud and Control Survey, 71% of respondents said they had experienced attempted or actual payments fraud in 2010.*



Cyber criminals understand online banking and electronic payment transactions. They use these channels to defraud the organizations and businesses that drive our economy.

KeyBank is dedicated to helping you better understand how to protect your company from fraud and online security threats.

How fraud happens

One of the most common cyber-scams is “phishing” (pronounced “fishing”). Phishing usually involves a spammed email message, phone call, voice mail or text message sent by criminals who intend to capture the recipient’s personal information (e.g., Social Security numbers, credit card information, User IDs and passwords) and use it illegally.

Phishing emails are often “spoofed,” i.e., they appear to come from legitimate sources such as banks, credit card companies or Internet Service Providers (ISPs). These emails may also appear to come from official sources such as the FBI, FTC, NACHA, Federal Reserve, BBB, or a company you specifically do business with.

These scams or phishing emails often contain malware that can be installed on your computer when you or your employees take the action requested in the email. For example, an email may ask you to click on a Web link, open an attachment, or provide personal information. These emails may also attempt to steal your banking credentials or other personal information by asking you to confirm data.

Malware can cause a wide range of problems, from system disruptions to the loss of personal data or identity theft.

Your computer could also be infected when a user visits less-than-trustworthy websites (e.g., gambling, adult content), downloads and installs “free” software, visits a website that has been compromised, or responds to a malicious advertisement on a website.

KeyBank

*Association for Financial Professionals (AFP), 2011 AFP Payments Fraud Survey: Report of Survey Results, 2011.

How to help protect your company from fraud

Why these fraud attempts are so dangerous

They can give criminals access to your assets. If a phish contains a link and users click on it, they may be directed to a fraudulent website that often looks legitimate. If users enter the information requested, the cyber-criminal could then use it to log on to your account(s) and initiate fraudulent payments or purchase merchandise.

Some malware tracks and logs your keystrokes. This lets criminals continuously harvest information such as your passwords, account numbers, and much more.

New phishing tactics appear all the time. Scam artists continually develop new ways of using email and the Internet to gain access to personal or critical business information and use it for criminal purposes.

Electronic payments present opportunities for criminals. Automated Clearing House (ACH) and wire payments offer potentially lucrative opportunities for fraudsters and criminals who often try to leverage the speed of these payments.

If a phish contains a link and users click on it, they may be directed to a fraudulent website that often looks legitimate.

How to protect your accounts from fraud

These suggested best practices can help protect your computer and your associated banking accounts from inappropriate use.

Be vigilant

- First and foremost, you should closely and frequently monitor your accounts. You are your own best line of defense against fraud, because no one knows your spending patterns better than you, and no one can spot a problem more quickly. Be on the lookout for exceptions or transactions that may be fraudulent so you can take appropriate action to reduce the risk of losses.
- Be proactive and work with your IT/Security professionals to develop a plan for responding to fraud and virus/malware incidents before a problem occurs.
- Be alert to messages with improper grammar and misspellings – these are often seen in phishes.

Browse safely

- Never log in to your online banking account through a link or internet address provided in an email or text message – even if it appears to be coming from Key or a company you deal with regularly. Instead, open a new browser and manually type the known internet address directly into your internet browser address bar.
- Never use “favorites” to access a website where you plan to disclose private information. Rather, type the URL in your browser’s address bar when you want to access the site.
- Only enter your financial or account information on sites that have the “lock” icon displayed in the browser and “https” preceding the URL.

Consider a dedicated computer

- Consider using a dedicated computer for all banking transactions. Do not use the computer for email or to visit sites other than your banking websites.

Be suspicious

- Do not open any unsolicited, suspicious messages, or any emails from unknown senders. Delete them. If you do open one, do not open any attachments or click on any links within the message.
- If you receive an unexpected message from a known sender, do not launch an attachment before checking with the sender through a known phone number or email address. Even an email that appears to come from a trusted source could be fraudulent and contain a virus, Trojan horse, worm or other malware.
- Be very selective about giving your email address to sources you are not sure of. Sharing it with random sources can increase your chances of receiving fraudulent emails.
- Never provide personal information requested through pop-up windows or email.
- Read what consumer affairs reporters are writing. They often post alerts about new phishes and other electronic fraud or scams.
- Develop a forum in your company to routinely discuss security best practices. Engage internal partners by communicating concerns and sharing observations.

Safeguarding electronic payments such as wires

To help protect against fraudulent wire transactions, organizations need to carefully monitor all wire activity.

- Ensure you know who you are wiring funds to; never send funds to unknown individuals. Completely understand and verify the legitimacy of the requests, especially if they seem to be crisis or urgent situations.

KeyBank

How to help protect your company from fraud

- Many criminals send scam emails that try to manufacture "crisis situations" to evoke an emotional response. This increases the likelihood that an individual may wire funds, outside of your normal processes and controls, to an unknown or fraudulent source.
- If you receive an unexpected, urgent message from any known senders asking you to wire funds to them, call them at a trusted phone number to ensure that they truly sent the request. Criminals sometimes hack into emails to send these fraudulent requests for wires.
- When using your computer in any public area, whether at your place of work or elsewhere, if you have to leave your computer for any period of time ensure that you lock it. This will help prevent individuals from initiating unauthorized transactions while you are away.

What Key is doing about online fraud

Because phishing emails are not coming from Key or passing through any of Key's systems – even if they are good imitations that may look like they came from Key – there is nothing Key can do to stop you from receiving a phishing email. However, if we learn of a phish, we will work with the authorities to try to take down the fraudulent site. This makes it even more important for KeyBank customers to recognize fraud attempts and know how to protect themselves.

As part of our ongoing efforts to increase fraud awareness, Key alerts and educates clients and employees about phishing emails and methods. Those alerts are updated as new and changing frauds appear.

Key has various systems and procedures in place to monitor accounts and identify potential fraudulent transactions. However, Key's monitoring is an enhancement to – not a substitute for – your own monitoring.

Key is committed to continued investment in prevention and detection, using both technical and non-technical advancements. We are focused on new authentication advancements and behavioral analytics as well.

What to do if you suspect you are a victim of fraud or malware

- Call Key's Fraud Hotline directly at 1-**800-433-0124** for an analysis of the situation and further direction. After calling the Fraud Hotline, contact your Relationship Manager to ensure they are also aware of the issue.
- If you are unsure whether an email is an authentic message from Key, please call us right away to verify.

  Do not respond to the message. Instead, forward the message to **emailfraud@keybank.com**. You can also visit key.com/security for additional information on fraud protection.

  If you responded to the fraudulent email or have specific questions, call Key at 1-**800-433-0124**.
- If you have any security questions related to your use of Key Total Treasury,® please call our Key Total Treasury Security Support team at **1-800-539-9039**, and select option 1.

  If you suddenly do not have access to Key Total Treasury, please call Key immediately and inform us. This may be a result of malware or phishing attempts.
- If you have discovered malware on your computer, or clicked a link or opened an attachment and are not sure if your computer is safe, immediately disconnect your computer from the Internet and your company's network. Please contact Key to inform us of the malware concern and consult with a qualified IT professional to scan for and/or remove any malware and viruses.

  Unfortunately, depending on the type of malware, any networked computer is at risk of infection from any other computer on the same network. This is why removing the computer from the network and internet is so important.
- Remember, if you are a victim of fraud, it's important that you report it to the proper law enforcement authorities. Many acts of fraud go unreported due to shame, guilty feelings or embarrassment. Don't let that stop you.

Key has a variety of payment fraud protection solutions available.

Your Relationship Manager can provide more information about these services and help determine which solutions are right for you.

To learn more:
Visit key.com/phishing or key.com/security

KeyBank