Phishing and Internet Fraud

A common type of scam is called "phishing" (pronounced "fishing"). Phishing usually involves a spammed email message, phone call, voice mail, or text message being sent with the intent of illegally capturing the recipient's personal information such as Social Security number, online banking user identification number, debit and credit card account numbers, and passwords. The messages are "spoofed," which means they appear to have been sent from legitimate companies such as banks, credit card companies, or Internet Service Providers (ISPs).

Do you think you can spot a phishing message a mile away? Think again. These types of messages are not always easy to spot. The criminals behind them have become quite sophisticated in how they create them. For instance, the message may request that you click on a link, or it may provide an Internet address that takes you to a fraudulent web site that appears legitimate. In reality, they are trying to get you to enter some kind of personal, financial or account information.

If you receive a suspicious message, do not click on any links, open any file attachments, return phone calls, or use an Internet address provided in a text message.

Tips for spotting fraudulent email, phone, or text messages:

Urgent or threatening tone

Often, these messages will claim that your account may close if you do not confirm or authenticate your personal information immediately.

Note: Key will never send email requests to any of our clients for personal information if there are problems with online banking, debit or credit card accounts, potential fraud, or any other information pertaining to accounts. We will never attach unexpected files to emails sent to clients.

Request for personal or financial information

A fraudulent email, text message, phone call, or voice mail may claim that the bank has lost important security information that needs to be updated. It may also request that you update this information online and provide you a link or Internet address to a counterfeit web site to do so.

Misspellings and poor grammar

These messages may contain errors. Be on the look out for improper grammar and misspellings.

Suspicious email messages

If you receive a suspicious email message that appears to come from Key*, take the following steps:

1. Do not respond to the fraudulent email message
2. Forward the email message to emailfraud@keybank.com. *Note: this mailbox is for reporting suspicious email messages only. Please call 800-539-1539 for help with specific questions.*
3. Then delete the message from your personal email inbox

If you did respond to the fraudulent email, please call us at 800-539-1539.

Protect yourself

To help protect you from "phishing" and other online fraud, we strongly recommend the following:

- Do not open suspicious email messages; delete them. If you do open it, do not open any attachments or click on any links within the message.
- Never log in to your account through a link or Internet address provided in an email or text message; even if it looks like it is coming from Key or a company you deal with regularly. Instead, open a new browser and manually type the known Internet address in the address bar.
- Do not click on links or launch email attachments from suspicious or unknown senders.
- If you receive an unexpected message from a known sender, do not launch an attachment without checking with the sender first 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, or worm.
- Be selective when providing your email address to sources you are unsure of. Sharing your email address to random sources can increase your chances of receiving fraudulent emails.
- If you are a victim of fraud, it's important that you report it to the proper law enforcement. Many acts of fraud go unreported due to shame, guilty feelings, or embarrassment.
- There is no computer that is 100% secure. Always be sure to backup important files and disconnect from the Internet when you aren't online.
- Do business with companies you know and trust.
- Only enter your credit card information on sites that have the "lock" icon at the bottom of the browser and "https" preceding the URL. The "s" stands for secure.