Commercial Bank & Trust of PA

Protect Yourself from Fraudulent Emails

What is a Fraudulent Email?

A Fraudulent (spoof) e-mail pretends to be from a well-known company. Many times the person, who is sending the fraudulent e-mail, portrays the e-mail to be from a financial institution, credit card company, and so forth. The sender who sends the spoof email hopes to acquire your information, such as account numbers and passwords, to commit identity theft.

How can you prevent spoof email from affecting you?

Spoof, or "phishing", emails and the spoof websites often associated with them are deceptive in appearance. However, they may contain subject matter that reveals they are false. The most important thing you can do to protect yourself is being able to spot the misleading content.

Detect a spoof when you see it.

Frequently, a fraudulent or spoof email may contain the following:

- **Generic greetings or subject matter.**
  Many spoof emails begin with items in the subject line such as: "Detected Online User Violation", "Account Alert", or something of that nature. If you do not see your first and last name, be suspicious and do not click on any links or attachments.
- **A fake senders address.**
  A spoof email may contain a forged e-mail address in the "From" field. This field can be easily altered.
- **False sense of urgency.**
  Another tactic used by senders who send spoof emails is to try and deceive the person receiving the email with a threat to your account access. They will threaten your account access by informing you your account access has been suspended or an unauthorized transaction has occurred. A spoof email may also inform you that the financial institution is updating their records and needs your information fast.
- **Fake Links.**
  Many times spoof emails will contain instructions or an attachment that will send you to a spoof address. The text in the link may look valid, when in actuality it is not. A user can check the source of the link by moving their mouse over it and looking at the URL in the browser or email status bar. If there is any suspicion to the link, do not click on it. Be aware that the link may even contain verbiage referring to the financial institution.
- **Emails that appear to be websites.** Some emails may appear to be like a website in order to get you to enter your personal information. **Commercial Bank & Trust of PA** will never ask for personal information in an email.
- **Unsafe sites.** The term "https" should always precede any website address where personal information is entered. The "s" stands for secure. If you do not see "https", you are not in a secure web session, and data should not be entered. Many financial institution websites contain the "VeriSign Secured" site verification seal. Users can verify the site by clicking on the seal for verification.

Questions Commercial Bank & Trust of PA will never ask you in an email

- Account numbers
- Passwords
- Drivers License numbers
- Social Security card numbers

Commercial Bank & Trust of PA

Steps to take to prevent spoof from affecting you

- **Monitor your account.** Check your account periodically to see if there has been any suspicious activity.
- **Change your password often.** If you think your security or password has been compromised, create a new password immediately.
- **Take Action.** If you think your account information has been compromised contact Commercial Bank & Trust of PA at once.

We are dedicated to protecting you

Commercial Bank & Trust of PA works hard to educate you on the best ways to recognize and fight spoof.