

PROTECTING YOURSELF AGAINST EMAIL AND ONLINE FRAUD

Phony e-mail messages sent to you for the purpose of stealing personal and financial information are among the most common types of e-mail fraud.

Disguised as legitimate e-mail and claiming to be from sources you trust, these messages attempt to entice you to provide various types of personal and confidential information, including online IDs and passcodes, Social Security numbers and account numbers.

Also known as phishing or spoofing, the practice of e-mail fraud is commonly used by criminals to gain access to your existing accounts or to use your personal and financial information to open new accounts.

Please note: S&T will never ask you for your Log-in ID, password, account number or Social Security number in email. In addition, we will not contact you via telephone or email for the purpose of updating customer account information.

If you receive a suspicious email or telephone call asking for confidential information, please contact us at 800.325.2265.

Recognizing e-mail fraud

Spotting phony e-mail messages is not always easy. And the criminals who use them are becoming more sophisticated about creating them.

Phony e-mail messages may ask you to reply directly or click on a link that takes you to a fraudulent Web site that appears legitimate. In either case, they will generally ask you to provide sensitive personal, financial or account information.

Here are some tips for spotting phony e-mails:

- **Urgent appeals.** Frequently, these e-mails claim that your account may be closed if you fail to confirm, verify or authenticate your personal information immediately.
- **Requests for security information.** Fraudulent e-mails often claim that the bank has lost important security information that needs to be updated. They also may request that the user visit and update this information online.
- **Typos and other errors.** Fraudulent e-mails or Web sites may contain typographical or grammatical errors. The writing may also be awkward, stilted or inappropriate. The visual or design quality may be poor.

Protecting yourself against e-mail or online fraud (continued)

- Make sure the security features of your computer software, including your Web browser, are up-to-date. Software companies continuously provide security updates to their products.
- Don't take anything for granted. Always keep in mind that forging e-mails and creating fraudulent Web sites is not difficult.
- Confirm the validity of all requests for sensitive personal, financial or account information, particularly if they are made with an urgent or threatening tone.
- Call the company directly to confirm requests for updating or verifying personal or account information.
- Confirm requests for personal or account information by going to the company Web site directly. Open a new browser window, type the Web address and check to see if you must actually perform any activity that an e-mail may be asking you to do, such as change a passcode.
- Do not share your IDs or passcodes with anyone. Choose passcodes that are difficult for others to guess and use a different passcode for each of your online accounts. Use both letters and numbers and a combination of lowercase and capital letters if the passcodes or personal identification numbers (PINs) are case sensitive. Change your passcode often.
- If you think you may have provided personal or account information in response to a fraudulent e-mail or Web site, report the fraud immediately, change your passcodes and monitor your account activity frequently.
- Always sign off Web sites or secure areas of Web sites (for example, Online Banking) for which you use an ID and passcode to enter.
- When your computer is not in use, shut it down or disconnect it from the Internet.
- Be careful and selective before providing your e-mail address to a questionable Web site. Sharing your e-mail address makes you more likely to receive fraudulent e-mails.
- Review your monthly credit card and bank account statements thoroughly. Investigate suspicious items immediately to head off any possible fraud before it occurs.