Commercial Bank & Trust of PA

Types of Fraud

Understanding the different types of fraud will help you avoid becoming a victim. Stay informed on the latest online fraud threats by reading below:

Phishing
Phishing involves fraudsters who send messages to lure personal information (credit card numbers, bank account information, Social Security number, passwords, or other sensitive information) from unsuspecting victims. Phishing may occur through fraudulent emails, text messages or direct phone calls claiming to be a financial institution, or another company you have a customer relationship with, asking you for your personal information. These types of attacks may also be referred to as SMishing or SMS phishing, or Vishing (Voice Phishing).

At no time will you ever receive a call or email from the bank asking you for your login credentials. If you receive a suspicious phone call or email asking you to provide your authentication credentials you should decline to do so and call us at 1-800-684-2440.

For more information about phishing visit the Consumer Financial Protection Bureau (CFPB) website at https://www.consumerfinance.gov/

Malware

Malware, short for "malicious software," includes viruses and spyware installed on your computer, phone, or mobile device without your consent. Malware can be used to steal personal information, send spam, and commit fraud. For more information about malware visit https://www.onguardonline.gov/.

Identity Theft

Identity theft occurs when someone uses your personally identifying information, such as your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes. The Federal Trade Commission has online guidance about the steps consumers can take to protect themselves against identity theft.

For more information about identity theft visit the Consumer Financial Protection Bureau (CFPB) website at https://www.consumerfinance.gov/ or the Federal Trade Commission Website at https://www.ftc.gov/

Personal and Account Protection Tips

- Do not use your Social Security number (SSN), in full or in part, for a password or PIN.

- Review your credit reports frequently to ensure the information is up to date and accurate. Work with the credit reporting agencies to have any inaccurate information removed.
- Store your Social Security card, other identification cards, checks and accounts statements in a safe and secure location.
- Carry your Social Security Card, passport or birth certificate with you only when absolutely needed.
- Do not share your personal or financial information over the phone or in person unless the information is absolutely necessary and you can confirm that the individual and company are legitimate.
- Frequently monitor your financial accounts and report any suspected fraudulent transaction immediately.
- Retrieve and review your mail promptly.
- Shred financial documents no longer needed, pre-approved credit offers, receipts and other documents that may contain financial and personal information.

Online Banking Security Tips

Step 1: Protect Your Computer

- Install and update your anti-virus and anti-spyware software frequently.
- Keep your computer's operating system up-to-date.
- Make sure to keep your web browser software up-to-date by installing the most recent version.
- If your computer's operating system has a firewall, enable it.

Step 2: Keep Your Information Secure

- If you do not recognize the sender of an email or have any doubts about the authenticity of an email, do not respond and delete it immediately.
- Do not open the email or click on links or attachments, especially if they tell you the problem is urgent or the attached file ends in ".exe".
- Don't give out personal information. Check a website's privacy policy before you give them your email address.
- Always use secure passwords. A secure password consists of upper and lower case letters, numbers, and special characters.
- Never share your password with anyone.
- Do not include personal or sensitive data in, or in response to, an email.
- Monitor your account activity closely and watch for unusual activity. You can use Commercial Bank & Trust of PA Online Banking to monitor account balances, 24/7.
- When you finish your online banking sessions, be sure to log out.
- Do not store financial or personal information on your laptop, phone, or other devices.

Commercial Bank & Trust of PA

Step 3: Practice Safe Web Browsing

- Only allow pop-ups from sites that you authorize.
- Do not give out personal information to blogs, forums and other social networking sites.
- Only make online purchases using secure sites that encrypt your information. To determine if a site encrypts your information look for the locked padlock icon in the browser and "https:" in the address line.
- Never access a website from a link in a suspicious email.
- Access online banking sites by typing the address directly into the browser's address bar.

Step 4: Protect Your Laptop, Phone, and other Devices

- Be suspicious when installing applications/programs that require you to provide information that has nothing to do with the application's purpose.
- If you use your laptop, phone or other devices to conduct online banking, and your device becomes lost or stolen, contact your financial institution and cell phone provider immediately.
- Never leave your laptop, phone or other devices logged in and/or unattended in public.
- Password protect and lock your laptop, phone or other devices when not in use.
- Do not store financial or personal information on your laptop, phone, or other devices.

Commercial Bank & Trust of PA

What is Card Skimming?

Card skimming is the illegal copying of information from the magnetic strip of a credit, debit or ATM card. Skimming devices can be placed on or near an ATM or any device in which you swipe your card to make a payment (commonly referred to as Point of Sale (POS) device) and can be difficult to spot.

ATM and Card Protection Tips

- Be cautious and always pay attention to your surroundings when using your credit, debit or ATM card at an ATM or Point of Sale device.
- When entering in your PIN, hide it from view so others nearby cannot see it.
- Do not use an ATM or Point of Sale device if you notice suspicious individuals or possible tampering of the machine or device, including scratches, marks, and adhesive or tape residues.
- Report any suspicious or fraudulent activity immediately to the owner of the ATM or Point of Sale device or local law enforcement.
- Be suspicious if a store employee takes your card out of your sight in order to process your transaction, asks you to swipe your card through more than one machine.
- Monitor your account or credit card statements for unusual or unauthorized transactions.

Unauthorized Transactions for Consumers

Notify us immediately if you believe your Card or Personal Identification Number (PIN), or both, has been lost, stolen or used to complete an Electronic Fund Transfer (EFT) without your permission. Examples of EFT transactions are: ATM withdrawals and transfers, POS purchases made with your debit or ATM card, online banking payments, and online transfers. These claims will be investigated in accordance with Federal Regulations and guidelines.

Here are some additional tips for commercial customers:

- Perform your own annual internal risk assessment & evaluation on all online accounts
- Establish internal policies regarding employee internet usage
- Ensure all company computers are equipped with up to date anti-virus protection software
- Ensure you have procedures for terminating access for former employees
- Inform employees to never write down Internet Banking passwords and leave them out in the open
- Ensure dual control or other checks and balances over individual access to online transaction capabilities

Commercial Bank & Trust of PA

FDIC Consumer Education

The FDIC offers an on-line tool to help educate consumers how to better protect their computers and themselves from identity theft, and steps to take if they have been victimized. The presentation: "**Don't Be an On-Line Victim: How to Guard Against Internet Thieves and Electronic Scams"** is on the FDIC's website and can be viewed at the following address:

https://www.fdic.gov/consumers/consumer/guard/

Links to More Resources:

https://ftc.gov/
https://onguardonline.gov/
https://www.stopfraud.gov
https://apwg.org/