## Protecting Your Information is Our Priority

Threats to information security are increasingly part of everyday life for the customers we serve. Today more than ever, you need to know how to protect yourself against Internet and e-mail hazards like phishing, spyware, viruses, spam and more. Below, you will find useful information and education on ways you can take control to safeguard your identity, money, privacy and property.

## If You Suspect Fraud

If you suspect fraudulent activity related to your accounts, contact your local community office or visit our webpage for the nearest branch locations and contact information. https://www.cnbthebankonline.com/home/contact/locations

## Security Topics

During times of turmoil some people may use this as an opportunity to take advantage of others. If you need assistance with your finances, please contact us at the number on your account statement, or on written correspondence from us. Please know that we will not contact you via phone or text messaging to request sensitive personal information such as your Social Security Number, Account Number, Debit Card Number, Personal Identification Numbers (PIN), or passwords.

Commercial Bank & Trust of PA recommends following the guidance from the Department of Homeland Security and Infrastructure Security Agency (CISA) https://www.cisa.gov/

## Social Engineering Schemes

Commercial Bank & Trust of PA has observed an increase in social engineering fraud attempts. In these phishing scams, you may be called, emailed or texted by someone pretending to be from an organization you are likely to engage with, including popular retailers, government agencies or technology providers. The scammer may claim false information about a product or service to trick you into sharing account access or other personal information. For example, he or she may tell you that a payment error has occurred and an account number is needed for reimbursement, that funds need to be mailed or transferred at once or that you need to purchase gift cards and provide him or her with the numbers.

If you receive a similar call, email or text, be aware of the following best practices:

- Always use caution and never provide personal information to an unknown contact.

- Confirm the authenticity of the message by using publicly available email addresses or phone numbers for the organization the individual claims to represent.
- Do not purchase gift cards unless they are intended as gifts for family and friends.
- Never send funds to unknown recipients via person-to-person payments (for example, Zelle®), cash or wire payments.
- Use online and mobile banking tools to check your account regularly for unauthorized activity.

If you believe that you have been the victim of a phishing scheme or if you identify potential fraudulent activity on your account, notify local law enforcement immediately and contact your local community office.

## Caller ID Spoofing

Please be aware of spoofing scams in which a caller intentionally falsifies or disguises a caller ID to appear as someone they are not. Scammers may act or say they are with a legitimate organization, including as a representative of a financial institution, to get you to respond with personal information they can then use to engage in fraudulent activity such as stealing your identity or money.

Commercial Bank & Trust of PA will never call, email or text you to request personal information such as Personal Identification Numbers (PIN numbers) or passwords.

Use caution at all times and never answer calls from unknown numbers, respond to questions or provide personal information of any kind. If you suspect the call might be a spoofing scam, hang up immediately and call the company or government agency the caller claimed to represent to verify the authenticity of the call/request.

## Text and Email Scams

Be aware of phony text and email messages appearing to come from Commercial Bank & Trust of PA. These messages often reference irregular/unauthorized account activity, or inform you that your profile has been accessed from a different device. These messages also request that you review/update your profile and include a link to enter personal information. These texts and emails are not legitimate Commercial Bank & Trust of PA communications. Commercial Bank & Trust of PA will never request personal or confidential data such as account numbers or passwords via email or text. Recipients should not respond to these types of messages or click any links contained in them.

## Update Your Operating System and Web Browser

For the optimal and most secure Online and Mobile Banking user experience, remember to always use the most up-to-date version of your operating system or browser.

## COVID-19 Phishing Scheme

The FBI's Internet Crime Complaint Center (IC3) has warned of a phishing campaign delivering spam that uses fake government economic stimulus checks as bait to steal personal information from potential victims.

Be on the lookout for phishing emails asking to verify personal information in order to receive an economic stimulus check from the government. Government agencies are not sending unsolicited emails seeking private information in order to send money.

Similar campaigns might ask potential victims for donations to various charities, promise general financial relief and airline carrier refunds, as well as try to push fake COVID-19 cures, vaccines and testing kits.

Other active phishing attacks are taking advantage of the COVID-19 pandemic to infect victims with malware and harvest their personal information through spam impersonating the Centers for Disease Control and Prevention (CDC) and other similar organizations, such as the World Health Organization (WHO).

The FBI adds that scammers are trying to sell products claiming to prevent, treat, diagnose or cure the COVID-19 disease, as well counterfeit sanitizing products and personal protective equipment, including but not limited to N95 respirator masks, gloves, protective gowns, goggles and full-face shields.

Possible COVID-19-themed scams and attacks as highlighted by U.S. Attorney Andrew Murray include:

- Individuals or businesses selling fake cures for COVID-19.
- Online offers for vaccinations and test kits.
- Phishing emails or texts from entities posing as the World Health Organization (WHO) or the Centers for Disease Control and Prevention (CDC).
- Malware inserted in mobile apps designed to track the spread of COVID-19 that can steal information stored on devices.
- Malicious COVID-19 websites and apps that can gain and lock access to devices until a ransom payment is made. Solicitations for donations to fake charities or crowdfunding sites.

Commercial Bank & Trust of PA

To report COVID-19 Fraud, contact the Disaster Fraud Hotline 866-720-5721 or email disaster@leo.gov. You can find more information on the National Center for Disaster Fraud webpage.

## Beware of identity theft scam involving unemployment benefits

The IRS is warning taxpayers of an identity theft scam involving fraudulent claims for state unemployment benefits. Identity thieves are reportedly using stolen personal information to file for and receive unemployment benefits. This scam has proliferated during the COVID-19 pandemic as unemployment claims in general have skyrocketed.

In response, the IRS says taxpayers who receive Forms 1099-G, *Certain Government Payments*, reporting unemployment benefits they did not receive should contact the state unemployment agency and get a corrected form saying they did not receive those benefits (IR-2021-24).

The IRS told taxpayers who are unable to obtain a timely, corrected form that they should still file an accurate income tax return, reporting only the income they received. A corrected Form 1099-G showing zero unemployment benefits when taxpayers have been victims of identity theft will help them avoid being hit with an unexpected federal tax bill for unreported income, an especially unwelcome occurrence when they are unemployed.

The IRS stated that if payments are made due to identity theft and are mistakenly reported on Form 1099-G in the name of the identity theft victim, a corrected Form 1099-G reporting $0 should be issued to the identity theft victim and filed with the IRS as soon as possible after the error is discovered.

The IRS explained that taxpayers who have been victims of this scam do not need to file a Form 14039, *Identity Theft Affidavit*, with the IRS reporting an incorrect Form 1099-G. The identity theft affidavit is used only if the taxpayer's e-filed return is rejected because a return using the same Social Security number already has been filed.

The IRS also told taxpayers they can protect themselves from federal tax return identity theft by requesting an identity protection PIN (IP PIN) from the IRS, which is now available to all taxpayers. An IP PIN is a six-digit number the IRS issues that prevents an identity thief from filing a tax return using a taxpayer's Social Security number. Because only the taxpayer and the IRS know the number, an IP PIN helps the Service verify the taxpayer's identity when the taxpayer files his or her paper or e-filed tax return.

Commercial Bank & Trust of PA

For your convenience, Commercial Bank & Trust of PA provides links to third party service providers. By clicking this link you agree to leave Commercial Bank & Trust of PA‘s website and will be routed to a third party site outside the control of Commercial Bank & Trust of PA. Commercial Bank & Trust of PA does not provide, and is not responsible for, the products, services, or overall website content available at a third-party site. Commercial Bank & Trust of PA does not endorse or guarantee the product, information or service on any third party’s website. Commercial Bank & Trust of PA’s privacy policy does not apply to the linked website; we encourage you to read and evaluate the privacy and security policies of the site you are entering.