How to prevent Identity Theft and Cybercrime

At Bank of Commerce, the security of your personal and account information is very important to us. By practicing good security habits, you can keep your private information private.

To successfully prevent an attack you must understand what criminals are trying to do over the internet.

Most attacks fall into the following categories:

Fraudulent emails appearing to be from your bank or a trusted source sends you to a fictitious site that looks like the real site. At that site you are instructed to provide personal information, such as user names and passwords. This type of attack is called **Phishing** and is used to obtain information that can be used to hijack your accounts and your identity.

Internet traffic is redirected to a fraudulent site. At that site you are instructed to provide personal information such as user names and passwords. This type of attack is called **Pharming or Domain Spoofing** and is used to obtain information that can be used to hijack your accounts and your identity.

Malicious software is installed on your computer to infiltrate or damage a computer system without the owner's knowledge. This type of attack is called **Malware** and is used to disrupt computer operations, gather sensitive information, or to gain access to the computer system.

Someone is posing as someone else to gain confidential information such as an account number, credit/debit card number, password, and/or social security number. This type of attack is called **Social Engineering** and is used to obtain information that can be used to hijack your accounts and your identity.

The bank has implemented safeguards to increase security for our customers. Our security controls include multi-factor authentication, including security questions, image recognition, and passwords, and layers of security software and hardware. However, as an end-user you play an important role in ensuring that you are protected when you use the internet.

To stay safe online, follow these security tips:

Protect and Strengthen Passwords

Never share your password and never reply to phishing e-mails with your password or other sensitive information. Change your password regularly and use a different password for each account. The strongest passwords are those that cannot be attributable to you. Use a password that is difficult to guess and consists of a combination of numbers, letters (both upper and lower case), punctuation, and special characters. If you have to write down your password, store it in a secure, private place. When prompted by the browser to “remember” password, select NO. This may seem like a timesaver to accessing your accounts, but it also allows hackers easy access to your accounts.

Enhance Your Computer Security and Keep it Current

Virus protection and firewalls provide additional layers of security and are available for purchase online or at reputable stores nationwide. Once installed, these programs need to be kept up-to-date. Most virus software updates are free once you have paid the annual fee for the software. Make sure the computer has the latest software security patch provided by your operating system vendor. These patches are free and can be setup to automatically download and install to your computer. Review your program files and make sure there aren’t unknown programs running on your PC. If using a wireless router, make sure to secure it with a password required to connect and by changing the default password on the router.

Always disconnect from the internet when not in use

Always click on the “log out” button to terminate your online session. Select the ‘exit’ button to close the browser. Do not leave sessions open when the computer is not in use. As an additional precaution, if the PC will be idle for long lengths of time it should be shutdown.

Use Your Own Computer when accessing secure sites

Avoid accessing secure sites (sites that require a password) from shared computers. Shared computers may contain viruses or spyware and can save “temporary internet files” or “history” files that contain information about the sites you have accessed.

Monitor Your Account Activity Regularly

Using Online Banking you can monitor your account regularly. If you see something suspicious, contact the bank immediately.

Don't Respond to Emails requesting personal information

Bank of Commerce will never request personal information or passwords by email. Emails that ask for PIN numbers, passwords, bank account, or your credit card information are called ‘Phishing’ emails. These emails are designed to fool customers into believing the request is legitimate and may also link a customer to a site that looks legitimate. NEVER respond to these emails. Legitimate companies will never request this information by a non-secure means, such as email.

Don’t Respond to telephone calls requesting personal information

Bank of Commerce will never call and request personal information about your accounts. If you receive a telephone call from anyone who claims to be a bank employee and you are pressured to divulge sensitive data or personal account information, do not answer. Instead, ask them for their name and tell them you will call them back. Contact us immediately at 620-431-1400.

If you receive a call from someone requesting your Check Card Number/PIN or Bank Account Number, do not give them this information. If you accidentally provide this information, contact us immediately at 620-431-1400.

Understand What You Download

Virus and spyware can be hidden in email attachments, pop-up windows, or downloads. When you download a file from an unknown source you risk installing malicious software programs onto your computer or providing confidential information to a cyber-thief. Think before you click on a pop-up advertisement, download a “free” game, or open an email attachment.

Think before using "Open" Wireless Connections

Some wireless connections provided at cafes, coffee shops, libraries, airports, or hotels are considered “hot spots” and are made readily accessible by eliminating the use of a logon. Accessing secure sites, such as banking sites, should be avoided. The lack of security increases your risk when using these unsecured connections.

What to do if you suspect fraudulent activity on your Bank of Commerce account.

Contact the bank immediately at:

- 620-431-1400 M-F 8:30 am – 5:00 pm
- 620-431-7349 M-F 5:00 pm – 6:30 pm, Saturdays 8:30 am – 4:00 pm
- If suspicious card activity and it is after hours, call 1-800-554-8969 to block the card.

What to do if you suspect identity theft.

1) Contact the fraud department at any one of the 3 consumer reporting companies to place a fraud alert on your credit report.
    - www.equifax.com or 800-525-6285
    - www.experian.com or 888-397-3742
    - www.transunion.com or 800-680-7289

2) Close the accounts that you know or believe have been tampered with or opened fraudulently.

3) File a report with your local police or the police in the community where the identity theft took place. Get a copy of the report or the number of the report to submit to your creditors and others that may require proof of the crime.

4) File your complaint with the Federal Trade Commission (FTC) as www.ftc.gov or 1-877-438-4338. The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations.

**For additional information about Identity Theft, visit www.boc-ks.com and select the Identity Theft link at the bottom of the home page.

In addition, you should periodically verify that Bank of Commerce has your best contact information. This includes mailing address, home phone, work phone, cell phone, and email address.