Fraud Protection

Over the years, there has been a significant increase in fraud schemes. Scams to obtain personal information can occur through many different means, such as emails, telephone calls and even text messages. A common method used by fraudsters is called "phishing." While phishing has typically been associated with unsolicited emails, there are a variety of scams that use a combination of phone messages and toll-free numbers.

The Federal Financial Institutions Examination Council (FFIEC) issued supervisory guidance designed to assist consumers and businesses with enhanced security for online transactions. With an ever-increasing threat environment, scams and hacking techniques are becoming highly sophisticated. Both domestic and international crime groups are continually developing new threats.

The guidance means you may begin to see new security features on the websites you visit. Online products have built-in security features which are continually enhanced in response to changing threats. Some of these enhancements are visible to you, the user, but others occur behind the scenes. You may see more information on how you, as a user of online services, can take action to help keep your identity, financial information and funds secure.

Below we have provided a few tips to help you protect your personal information from telephone or email phishing scams are listed below:

Computer Security Tips:

- Protect your computer with anti-virus software and firewall(s).
- When banking online, always make sure your browser address reads https://www.commerceonebank.com before you begin the login process.
- Never respond to an email requesting that you provide personal information to verify an account or to re-activate that account or service.
- Remember, CommerceOne Bank does not contact clients via email requesting personal information or personal account security information, such as a PIN or passwords.
- Keep PC operating system security up to date by applying patches and updates.

Telephone Security Tips:

- If you receive a suspicious phone message or email requesting that you call CommerceOne Bank at a particular number, you may verify the number is legitimate by visiting the Contact Us page on our website. You may also call our main number (205-719-5750) for expert support and assistance.
- Note: Sophisticated scammers can make your caller ID indicate that they are calling from CommerceOne Bank or another legitimate phone number, even if they are not. This is called "spoofing." If someone asks you to provide sensitive personal or account information on a call you did not initiate or request, hang up and call 205-719-5750 or visit our location.
- Do not provide your personal secure information to an unsolicited caller. Remember, CommerceOne Bank will not initiate a call asking you to provide your full account number, online/mobile banking passwords, PINs or complete Social Security number over the phone.
- Never respond to a phone call or voice mail service asking you to verify account information or reactivate a bank service, even if the caller recites some of your account information to you. They may have obtained the information from another source and are enticing you to provide additional details that would help them access your accounts.
- Please be aware that legitimate calls from CommerceOne Bank, such as calls from the Fraud Center, are made often, but the agents only ask for confirmation of certain activity on a credit or debit card. No sensitive information is requested.

Access Credentials:

- CommerceOne Bank will never call, e-mail or otherwise contact you to request your access ID, password or other access credentials for the online services we offer.

- Never give out personal account access information in response to an unsolicited call, e-mail or text message. If you receive such a request, do not provide any information. Contact us immediately at 205-719-5750 to report an incident.
- Do not share your user ID(s) or password(s) with another person or provide them to others.
- Safeguard your user ID and password information – never leave the information in an unsecured location.
- Create a unique user ID and password for each site or service.
- Do not use the same identifying information on multiple websites.
- Do not use information that can be associated with your personal identification including your social security number, address, date of birth, children and/or pet names.
- Your passwords should be memorized instead of written down.
- Create strong user IDs and passwords using upper- and lower-case letters, numbers, and special characters. Many websites force password changes (i.e. every 60 days). If a website does not do so, take the initiative and change your password on a regular basis.

Website Security Tips:

- Frequently monitor account activity.
- Review account activity online compared to periodic account statements and reconcile them to your personal records at least monthly.
- Never leave your computer unattended during an internet banking or bill pay session.
- Log off from a website; do not just close the page or "X" out, as a browser may leave you logged in for perceived convenience.
- Secure websites have a web address that includes an "s" (https rather than http). If this is lacking, the site does not contain additional security enhancements. We do not recommend conducting business on the site.
- If a website displays a security monitor, verify it has the current date. If it does not, do not use the site; it may be spoofed or hijacked.
- When completing financial transactions, verify encryption and other security methods are in place, protecting your account and personal information.

Resources:

Web Resources – Learn more and do more to protect yourself online:

Consumer alerts and online security tips on the FTC website: www.consumer.ftc.gov

Scams and fraud and tips to avoid being a victim – Go to the FBI website at: www.fbi.gov

Reporting Suspicious Activity:

If you see suspicious activity on your account(s) or have received a suspicious call, e-mail, letter or other similar contact regarding your relationship to CommerceOne Bank, call 205-719-5750.

Consumer Protection – Regulation E:

The Electronic Funds Transfer Act - Regulation E provides consumers with protections for error resolution and unauthorized transactions for electronic fund transfers. It sets forth liability limits which are tied to the timeliness of your detection and reporting of the transactions. Therefore, we encourage you to immediately review periodic account statements as soon as they are received and to regularly monitor your account activity online and through our mobile banking app.

The "Electronic Fund Transfers" disclosure provided to you at the time of account opening contains detailed information regarding your rights. Upon request, we will provide a free printed copy of this disclosure. In general, these protections are extended to consumers and consumer accounts.

Commercial Clients Offering Online Services:

Business transactions can be at greater risk for fraud then consumer transactions. Reports indicate potential risk reduction when enhancements in controls over administrative access and functions related to business accounts are in place. In addition, layered security using multiple and independent controls help to reduce these types of crime.

The Federal Financial Institution Examination Council (FFIEC) has recommended the completion of a periodic risk assessment along with an evaluation of the effectiveness of the controls in-place to help minimize risk associated with online transaction processing. The tips and controls provided for in this document can assist in providing a starting point and resource for completing the risk assessment and control review. In addition, the FTC Business Center has a great deal of information for businesses at www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security

Important note about requests from CommerceOne Bank to verify/update personal information:

If CommerceOne Bank asks you to verify or update personal information for our records, we will do so through a secure channel like online banking and/or we will provide an option that makes it easy for you to confirm that the request is legitimate (for example, calling us directly at 205-719-5750 or visiting a branch).

If you believe you are a victim of fraud or have been the recipient of suspicious communication, call or contact CommerceOne Bank immediately at 205-719-5750. CommerceOne Bank clients can also forward any suspicious email to client.services@commerceonebank.com.