Social Engineering

In a **social engineering attack**, an attacker uses human interaction to manipulate a person into providing them information. People have a natural tendency to trust. Social engineering attacks attempt to exploit this tendency in order to steal your information. Once the information has been stolen it can be used to commit **fraud** or **identity theft**.

Criminals use a variety of social engineering attacks to attempt to steal information, including:

- **Website spoofing**
- **Phishing**

This brochure explains the meaning of these common attacks and provides tips you can use to avoid being a victim.

To learn more about information security, visit any of the following websites:

- OnGuardOnline.gov
- StaySafeOnline.org
- BBB.org/Data-Security
- US-CERT.gov

Commerce Bank Texas
www.commercebanktx.com
830-996-3125

COMMERCE BANK TEXAS

Avoiding Social Engineering Attacks

www.commercebanktx.com

Common Attacks

❖ **Website spoofing** is the act of creating a fake website to mislead individuals into sharing sensitive information. Spoof websites are typically made to look exactly like a legitimate website published by a trusted organization.

Prevention Tips:

- Pay attention to the web address (URL) of websites. A website may look legitimate, but the URL may have a variation in spelling or use a different domain.
- If you are suspicious of a website, close it and contact the company directly.
- Do not click links on social networking sites, pop-up windows, or non-trusted websites. Links can take you to a different website than their labels indicate. Typing an address in your browser is a safer alternative. Only give sensitive information to websites using a secure connection. Verify the web address begins with "https://" (the "s" is for secure) rather than just "http://".
- Avoid using websites when your browser displays certificate errors or warnings.

❖ **Phishing** is when an attacker attempts to acquire information by masquerading as a trustworthy entity in an electronic communication. Phishing messages often direct the recipient to a spoof website. Phishing attacks are typically carried out through email, instant messaging, telephone calls, and text messages (SMS).

Prevention Tips:

- Delete email and text messages that ask you to confirm or provide sensitive information. Legitimate companies don't ask for sensitive information through email or text messages.
- Beware of visiting website addresses sent to you in an unsolicited message.
- Even if you feel the message is legitimate, type web addresses into your browser or use bookmarks instead of clicking links contained in messages.
- Try to independently verify any details given in the message directly with the company.
- Utilize anti-phishing features available in your email client and/or web browser.
- Utilize an email SPAM filtering solution to help prevent phishing emails from being delivered.
- Do not open attachments received from unknown senders or unexpected attachments from known senders.
- Be cautious of the amount of personal information you make publicly available through social networking sites and other methods. The more information publicly available about you, the easier it is for attackers to craft more convincing phishing messages.

Report Fraudulent or Suspicious Activity

Contact us immediately if you suspect you have fallen victim to a social engineering attack and have disclosed information concerning your Commerce Bank Texas accounts.

Call us at 830-996-3125 or visit your local Commerce Bank Texas branch location.

Regularly monitoring your account activity is a good way to detect fraudulent activity. If you notice unauthorized transactions under your account, notify Commerce Bank Texas immediately.

Passwords

- **Create a unique password for all the different systems you use.** If you don't, then one breach leaves all your accounts vulnerable.
- **Never share your password over the phone, in texts, by email, or in person.** If you are asked for your password, it's probably a scam.
- **Use unpredictable passwords** with a combination of lowercase letters, capital letters, numbers, and special characters.
- **The longer the password, the tougher it is to crack.** Use a password with at least 8 characters. Every additional character exponentially strengthens a password.
- **Avoid using obvious passwords** such as:
  - your name
  - your business name
  - family member names
  - your user name
  - birthdates
  - dictionary words
- **Choose a password you can remember without writing it down.** If you do choose to write it down, store it in a secure location.

To learn more about information security, visit any of the following websites:

- OnGuardOnline.gov
- StaySafeOnline.org
- BBB.org/Data-Security
- US-CERT.gov

Commerce Bank Texas
www.commercebanktx.com
830-996-3125

COMMERCE BANK TEXAS

Online Banking Security Tips

www.commercebanktx.com

Mobile Device Security

- **Configure your device to require a passcode to gain access** if this feature is supported in your device.
- **Avoid storing sensitive information.** Mobile devices have a high likelihood of being lost or stolen so you should avoid using them to store sensitive information (e.g. passwords, bank account numbers, etc.). If sensitive data is stored then encryption should be used to secure it.
- **Keep your mobile device's software up-to-date.** Mobile devices are small computers running software that needs to be updated just as you would update your PC. Use the automatic update option if one is available.
- **Review the privacy policy and data access of any applications (apps)** before installing them.
- **Disable features not actively in use such as Bluetooth, Wi-Fi, and infrared.** Set Bluetooth-enabled devices to "non-discoverable" when Bluetooth is enabled.
- **Delete all information stored on a device before the device changes ownership.** Use a "hard factory reset" to permanently erase all content and settings stored on the device.
- **"Sign out" or "Log off" when finished with an app** rather than just closing it.

Online Security

- **Never click on suspicious links** in emails, tweets, posts, nor online advertising**.** Links can take you to a different website than their labels indicate. Typing an address in your browser instead of clicking a link in an email is a safer alternative.
- **Only give sensitive information to websites using encryption** so your information is protected as it travels across the Internet. Verify the web address begins with "https://" (the "s" is for secure) rather than just "http://". Some browsers also display a closed padlock.
- **Do not trust sites with certificate warnings or errors.** These messages could be caused by your connection being intercepted or the web server misrepresenting its identity.
- **Avoid using public computers or public wireless access points** for online banking and other activities involving sensitive information when possible.
- **Always "sign out" or "log off"** of password protected websites when finished to prevent unauthorized access. Simply closing the browser window may not actually end your session.
- **Be cautious of unsolicited phone calls, emails, or texts** directing you to a website or requesting information.

General PC Security

- **Maintain active and up-to-date antivirus protection** provided by a reputable vendor. Schedule regular scans of your computer in addition to real-time scanning.
- **Update your software frequently** to ensure you have the latest security patches**.** This includes your computer's operating system and other installed software (e.g. Web Browsers, Adobe Flash Player, Adobe Reader, Java, Microsoft Office, etc.).
- **Automate software updates,** when the software supports it, to ensure it's not overlooked.
- **If you suspect your computer is infected with malware,** discontinue using it for banking, shopping, or other activities involving sensitive information. Use security software and/or professional help to find and remove malware.
- **Use firewalls** on your local network to add another layer of protection for all the devices that connect through the firewall (e.g. PCs, smart phones, and tablets).
- **Require a password to gain access.** Log off or lock your computer when not in use.
- **Use a cable lock to physically secure laptops**, when the device is stored in an untrusted location.