CLEAR LAKE BANK & TRUST COMPANY

Internet Banking Customer Awareness & Education Program
For Individuals

CLEAR LAKE BANK & TRUST CO.
A FULL SERVICE BANK MEMBER FDIC
EQUAL HOUSING LENDER

Introduction

Clear Lake Bank & Trust Company is committed to protecting your personal and confidential information which you have entrusted in our care. We take the trust you have placed in us very seriously and have created this Internet Banking Customer Awareness & Education Program to inform you of important information to assist you in keeping your information safe.

Requests for Information

Clear Lake Bank & Trust Company will never request personal & confidential information from you by telephone, mail, email, or text message. This includes requests for your account number, Social Security number, personal identification number (PIN), debit card number, etc. Requests for this information by anyone should be considered suspicious. Please contact us immediately at (641) 357-7121 if someone claiming to be from Clear Lake Bank & Trust Company requests personal and confidential information from you.

We will contact you on an unsolicited basis for the following reasons:

- Suspicious activity on your account.
- Suspicious activity on your debit card.
- Unclaimed property or a dormant account.
- Past due loan payments or fees due.
- To confirm changes on your account or contact information.

Credit Reports

You have the right to request one free copy of your credit report from each of the credit reporting agencies once per year. Contact all three of the major credit reporting agencies below to request your free report. Consider rotating the requests by ordering one report every fourth months instead of contacting all three credit reporting agencies at the same time.

- Equifax: 1-800-685-1111
- Experian: 1-888-397-3742
- Trans Union: 1-800-916-8800

Social Engineering

In terms of information security, social engineering is a broad term used to describe tools and techniques that criminals use to learn more information about an individual or a business, and the technology they use. It relies heavily on human interaction and often involves tricking people to breaking normal security procedures, thus providing the criminal with important information that can be used to commit fraud.

Social engineering can take on many different forms. Some examples of social engineering include, but are not limited to:

- Emails
    - With viruses/malware/spyware attached or that includes a link to viruses/malware/spyware.
    - That notifies the recipient of a suspended debit/credit card that requests a card number, PIN, or other information.
    - Claiming the recipient has won a lottery or is listed as an heir in a will.

- Phone Calls
    - Pretending to be a representative of their financial institution and requesting personal and confidential information, such as Social Security number, account number, personal identification number (PIN), etc.
    - Pretending to be a lottery representative or Publishers Clearing House employee who notifies you that you have won money in a lottery or drawing.
    - Pretending to be your grandchild who is in a foreign country and needs money wired for a problem they have encountered. The caller typically asks the grandparent not to contact "mom or dad" because they will be mad about the situation. The caller often sounds like the grandchild and uses sympathy as means of convincing the grandparent to wire money.
    - For any reason, asks you to send a wire transfer from a non-bank. Bank employees are trained to recognize fraud and criminals know a wire is more likely to be completed when a bank is not involved.
    - Automated phone call (also known as a robocall) notification of some sort of problem with your bank account or debit/credit card, and asks you to enter your PIN or card number.
    - Asking you to make payment with gift cards. At no time should you remit payment via a prepaid debit card.

- Text Messages
    - Claiming your debit/credit card is suspended or that fraud has been detected, and asks you to reply with your card number, PIN, or other confidential information.

- Dumpster Diving
    - The criminal goes through your garbage when placed outside for collection, looking for confidential information about you or your family.

- Media Drop
    - Criminal leaves flash drives or CDs in a public area hoping someone picks up the item and uses their computer to see what is on the media. Simply using the media loads a virus, malware, or spyware on your PC.

Security Tips

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, account numbers, etc.). If sensitive data is stored, enable encryption to secure it.
- **Keep your mobile device's software up-to-date.** These 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. Only download apps from trusted app stores (Apple, Google Play).
- **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.
- **Utilize antivirus software** where applicable (i.e. Android, Windows, etc.).
- **Do not jailbreak** or otherwise circumvent security controls.

Online Security

- **Never click on suspicious links** in emails, tweets, posts, or 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 submit sensitive information to websites using encryption** to ensure 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.

- **If you download anything from the Internet** (such as music, pictures, videos, software, etc.), make sure you download only from a trusted source. Downloaded files can contain harmful threats to your PC, such as viruses, malware, spyware, etc.
- **Make online purchases only from trusted web sites.** Research unknown companies before making an initial purchase. The Better Business Bureau is a good resource.

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.
- **Keep your computer's operating system up-to-date** with the latest security patches provided by the operating system vendor. Turn on automatic updates and keep your firewall on at all times.
- **Take immediate action if you see signs of spyware** on your PC. This includes pop-up ads, icons on your desktop, error messages, sluggish/slow PC performance.

Passwords

- **Create a unique password for all the different systems/websites you use.** Otherwise, 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 14 characters. Every additional character exponentially strengthens a password. Passphrases are most effective. A passphrase is a short sentence and generally easier to remember.
- **Avoid using obvious passwords** such as:
    - Names (your name, family member names, business name, user name, etc.)
    - Dates (birthdays, anniversaries, etc.)
    - 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.

Email Security

- **Scrutinize emails carefully** before clicking on links or opening attachments in emails, even if they appear to be from someone you know. Many times, these emails will appear to be authentic and claim to be from your bank, credit card company, or another trusted source. They may ask you to verify information about your account. DO NOT respond to these emails, DO NOT click on links in these emails, and DO NOT open attachments in these emails.
- **Do not call phone numbers** provided in a suspicious email. It is likely a "fake" phone number monitored by a criminal. Always contact your bank, credit card company, or other trusted business using a phone number provided on their published website or other trusted source.
- **Email is not secure,** and you should never send an email to your bank that contains confidential information. If you need to send secure information to Clear Lake Bank & Trust Company, please contact us and we will provide additional information.

Other Tips

- **Balance your bank account on a monthly basis** to ensure all transactions that appear on your account are legitimate. Remember, you only have 60 days after receiving your statement to report and recover unauthorized charges on your account.
- **Sign up for text message alerts** to receive notification when your balance falls below a certain level or when items post to your account.
- **Sign up for Internet banking** so you can check your account activity from your PC or mobile device at any time.
- **Don't use your mail box for outgoing mail** as criminals often monitor mailboxes in an effort to steal important information, bills, or checks you are sending via mail.
- **Use a cross-cut paper shredder** to destroy all documents that contain personal and/or confidential information. Straight line cut paper shredders are less effective than cross-cut paper shredders.
- **Don't write your PIN anywhere on your debit card** or keep your PIN in your wallet or purse.
- **Place your garbage out for collection in the morning** instead of at night. This reduces opportunities for "dumpster divers" to steal information that may be in your garbage.

Regulation E: Electronic Funds Transfer

Regulation E protects individual consumers engaging in electronic fund transfers (EFT). Non-consumer (or business) accounts are not protected by Regulation E. The term "electronic funds transfers" or "EFT", generally refers to the electronic exchange or transfer of money from one account to another, either within a single financial institution or across multiple institutions initiated through electronic-based systems. EFT transactions include, but are not limited, to:

- Point-of-sale transfers
- Automated Teller Machine transfers (ATM)
- Direct deposits or withdrawal of funds
- Transfers initiated by telephone
- Transfers resulting from debit card transactions, whether or not initiated through an electronic terminal
- Transfers initiated through internet banking/bill pay
- Electronic check conversion, whereby you may authorize a merchant or other payee to make a one-time electronic payment from your checking account using information from your check to pay for purchases or pay bills
- Electronic returned check charge, whereby you authorize a merchant or other payee to initiate an electronic fund transfer to collect a charge in the event a check is returned for insufficient funds.

The term EFT does not include:

- *Checks* – Any transfer of funds originated by check, draft or similar paper instrument or any payment made by check, draft or similar paper instrument at an electronic terminal
- *Check Guarantee or Authorization* – Any transfer of funds that guarantees payment or authorizes acceptance of a check, draft or similar paper instrument but does not directly result in a debit or credit to a consumer's account
- *Wire or other similar transfers* – Any transfer of funds through a wire transfer system that is used primarily for transfers between financial institutions or between businesses
- *Securities and Commodities Transfers* – Any transfer of funds for the primary purpose of the purchase or sale of a security or commodity, if the security or commodity is:
    - Regulated by the Securities and Exchange Commission or the Commodity Futures Trading
    - Purchased or sold through a broker-dealer regulated by the Securities and Exchange Commission or through a futures commission merchant regulated by the Commodity Futures Trading Commission
    - Held in Book-entry form by a Federal Reserve Bank or federal agency
- *Automatic transfers by account-holding institution* – Any transfer of funds under an agreement between a consumer and a financial institution which provides that the institution will initiate individual transfers without a specific request from the consumer:
    - Between a consumer's accounts within the financial institution

    - From a consumer's account to an account of a member of the consumer's family held in the same financial institution
    - Between a consumer's account and an account of the financial institution, except that these transfers remain subject to § 205.10(e) regarding compulsory use and sections 915 and 916 of the act regarding civil and criminal liability. (Refer to "Coverage in Detail" section below for a detail explanation of protections provided under Regulation E)
- *Telephone-initiated transfers* - Any transfer of funds that:
    - Is initiated by a telephone communication between a consumer and financial institution making the transfer; and
    - Does not take place under a telephone bill-payment or other written plan in which periodic or recurring transfers are contemplated.
- *Small institutions.* Any preauthorized transfer to or from an account if the assets of the account-holding financial institution were $100 million or less on the preceding December 31. If assets of the account-holding institution subsequently exceed $100 million, the institution's exemption for preauthorized transfers terminates one year from the end of the calendar year in which the assets exceed $100 million. . (Refer to "Coverage in Detail" section below for a detail explanation of protections provided under Regulation E)

If you believe an unauthorized EFT has been made on your account, contact us immediately. If you notify us within two (2) business days after you learn of the unauthorized transaction, the most you can lose is $50. Failure to notify the bank within two (2) business days may result in additional losses.

Unlimited loss to a consumer account can occur if the periodic statement reflects an unauthorized transfer of money from your account, and you fail to report the unauthorized transfer to the bank within 60 days after we mailed your first statement in which the problem or error appeared.

Contact Information

If you notice suspicious activity on your account or experience information security-related events, please contact us immediately at (641) 355-2217.

Individuals responsible for bank information security and electronic banking activities are:

Matt Ritter
Chief Operating Officer
(641) 355-2203

Sarah Thein
Assistant Vice President, Operations
(641) 355-2251

Resources

FDIC – Electronic Funds Transfers (Regulation E)
http://www.fdic.gov/regulations/laws/rules/6500-3100.html

FDIC Consumer Protection
http://www.fdic.gov/consumers/

FTC Complaint Assistant
https://www.ftccomplaintassistant.gov/#crnt&panel1-1

ID Theft

http://www.ftc.gov/bcp/edu/microsites/idtheft/

US Department of Homeland Security
http://www.us-cert.gov/home-and-business/

Federal Communication Commission - Business Cyber-planner:
http://www.fcc.gov/cyberplanner

On Guard Online:
http://www.OnGuardOnline.gov

Stay Safe Online:
http://www.StaySafeOnline.org

Better Business Bureau
http://www.BBB.org/Data-Security

United States Computer Emergency Readiness Team:
http://www.US-CERT.gov