CYBER SECURITY AWARENESS

The following list of information security practices is being provided for your convenience in an effort to help your business protect itself against breaches of security. This list is not intended to be comprehensive nor is it customized for any individual member's circumstances. This document was created to provide examples of common practices that may help reduce the likelihood that you become the victim of fraud.

BEST PRACTICES: GENERAL SECURITY

SECURE LOCATION: Computers used for everyday business transactions should be placed in a secure location. Keep these computers away from public areas and beware of scenarios where unauthorized individuals might view login credentials or transactional activity on the screen.

PHYSICAL SECURITY: To protect your information, securely dispose of sensitive documents in designated shred bins and destroy all hard drives on electronic devices.

WORKSPACE SECURITY: Sometimes unauthorized individuals may bypass security and gain access to your building. To protect against these types of threats, always lock up any sensitive documents and lock your computer screen when you will be away from your desk.

DATA SECURITY: A great deal of security focuses on keeping systems updated and secure. To ensure your data remains secure, take the following steps whenever handling any sensitive information:

- Only use or access systems authorized by your organization to process or transmit sensitive information. Do not copy anything to an unauthorized system or account such as your personal computer or email account.
- Keep your systems secure by only using authorized and licensed software. Using or installing unauthorized software creates risk for our systems and data.
- Should someone call or email asking for sensitive information, always authenticate the person first using procedures approved by your organization.
- If working with a third-party vendor, verify your data is protected before it's shared. A contract and evaluation of their security controls is recommended before allowing access to or sharing of information.

USING MOBILE DEVICES MORE SECURELY: Mobile devices, such as your smartphone and tablet, store a tremendous amount of personal and sensitive information, including your contacts, photos, text messages, and online activity. As such, mobile devices are frequent targets of cyber criminals. The following are best practices when conducting business/financial transactions from a mobile device:

- Conduct business transactions from devices that are compliant with your organization's security policies.
- Do not enable Bluetooth until you need it. This protects your device against unauthorized 'Bluesnarfing.' Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, exposing email, calendars, contact lists, text messages and potentially pictures and videos stored on your device.
- Add a screen lock to mobile devices, adding protection in case of loss or theft.
- If you lose or have any work-related mobile devices stolen, report it immediately and reset passwords for any app or website used on that device.
- Set auto-updates to keep your device operating system and any mobile apps current.
- Before installing any apps, do a safety check: Are the reviews positive? Are there many downloads? What permissions does the app require for installation? Is the app regularly updated?
- Do not access banking accounts from any Wi-Fi hotspots. Using a Virtual Private Network (VPN) app on your mobile device provides an additional layer of security when using any Wi-Fi connection.
- Ensure encryption is turned on for your mobile device.
- Securely delete the data from your mobile device before trading in or disposing of it.
- Only download applications from your device's trusted App Store.
- Phone numbers can be impersonated. A strange call or text from a known contact should be challenged before taking any action.

PHISHING/SPOOFING EMAIL COMPROMISE: Phishing is when a cyber attacker uses email to trick you into taking an action, such as clicking on a link, sending sensitive data, or opening an infected email attachment. Spoofing generally refers to an email which is drafted to appear as though it was sent by someone other than the actual source. It is not uncommon to have a cyber attacker spoof an email communication from an executive to initiate unauthorized wire transfers. Protect your organization by having processes and procedures for wire transfers and being alert to these signs of types of cyber attacks:

- Messages directed to "Dear Customer" or other generic greeting.
- Messages requiring immediate action or creating a sense of urgency, such as threatening to close down your account.
- Messages claiming to be from an official organization but having grammar or spelling mistakes or using a personal email address, such as Gmail, Yahoo, and Hotmail.
- Messages pressuring you to bypass your organization's security procedures. These types of attacks often happen when a cyber attacker is pretending to be your supervisor or co-worker.
- Messages requesting highly sensitive information, such as your business debit or credit card number.
- If you receive a message from someone you know, but the tone or message just does not sound like him or her, be suspicious. Call the sender on a trusted phone number to verify they sent it.
- Before you click on a link, hover your mouse cursor over it. This will display the true destination of where it will take you. Confirm that the destination displayed matches the destination in the email and make sure it is going to the organization's legitimate website. Even better, type the proper website address into your browser.
- Only open attachments you were expecting. Infected email attachments are a very common attack method and may not be detected or blocked by anti-virus.

ANTI-VIRUS AND ANTI-SPYWARE: Use anti-virus software, firewall and anti-spyware programs and use the most updated version available.

PASSWORD PROTECTION: Your passwords are one of the keys to securing your systems, accounts and organization as a whole. Cyber attackers have developed sophisticated methods to guess passwords and they're constantly getting better at it. Keep the following in mind when developing your organization's password policy and/or procedures:

- Make sure each password is long and strong. The more characters in your password, the stronger it is.
- Change your passwords frequently (at least every 90 days).
- Use a different, unique password for your systems and applications. That way, if one is compromised your other passwords are still safe.
- Use multiple, uncommon words to create a pass phrase, such as "Dontforget2walk!" or "stopping-highway-windy50MPH." Note that hackers often use dictionaries of previously compromised passwords from other attacks.
- Keep passwords a secret. Never share them with anyone, including a supervisor or someone claiming to be from CommunityAmerica.
- Consider using a password manager. This is a special program that securely stores all of your unique passwords.
- Never store your username or passwords on devices.
- Use Multi-Factor Authentication (MFA) on any application or website that offers it.
- Browser Security: Protect against attacks by using the latest versions of operating systems and applying any recent patches. Updated operating systems and applications (ex. Microsoft Office, Word, Google Chrome, etc.) are much harder for cyber attackers to compromise using vulnerabilities or weaknesses. Most applications and systems have the ability to automatically update themselves and warn you when an update is required.

Continued on back

BEST PRACTICES: COMMUNITYAMERICA ONLINE BANKING SECURITY

DEDICATED PC: CommunityAmerica strongly recommends that your organization have dedicated computers for facilitating online financial transactions. In addition, only authorized online banking users should have access to these dedicated computers.

SYSTEM ADMINISTRATOR DESIGNATION: Within online banking, Community America strongly recommends that you designate an individual or staff as your System Administrator(s). This separation of duties can help mitigate the risk for internal losses due to fraud within online banking. System Administrators should build authorized online banking users and determine their access controls and restrictions. In addition, the System Administrator(s) can determine which authorized user has approval and/or draft rights on each account with Dual Control enabled. In a Dual Control environment, one authorized user creates an ACH or wire payment and a second authorized user authorizes the release of the payment.

ONLINE BANKING USER ACCESS: Assign authorized online banking users' access to accounts and permissions within the account that are required for his or her specific job function. Immediately delete users upon employee termination and update user permissions/account access upon position changes within the organization. Review user access on a regular basis to ensure the following:

- Authorized users have not been granted unnecessary or unapproved permissions.
- User transaction limits are appropriate based on user role or specific job function.
- Unauthorized users have not been added to the system.

USER LOGOUT IN ONLINE BANKING: CommunityAmerica recommends that users log off at the conclusion of each online banking session in order to best protect your online banking account from unauthorized access. Do not simply close the web browser.

UTILIZE THE CONTROLS WITHIN COMMUNITYAMERICA ONLINE BANKING: CommunityAmerica's online banking solution provides several controls to limit your organization's exposure. These controls are vital to the security of your financial transactions and we strongly encourage your organization to incorporate them into your standard operational procedures. Controls available to help reduce your risk of fraud in online banking include the following:

- Establish Transaction Limits: Daily, monthly and per transaction limits for various types of payment transactions. These transaction limits can be enforced systematically to limit your exposure and allow for each employee to have appropriate limits based on his or her job function.
- Dual Approval/Multi-Factor Authentication: Review of payment transactions, such as ACH and wire, by a second authorized user. Under Dual Control, one authorized user drafts the ACH or wire payment and a second user authorizes the release of the payment. Next, the user authorizing the payment will go through Multi-Factor Authentication, a method in which a user is granted access after successfully entering a randomly generated code from the online banking system.
- User/User Role Permissions: The System Administrator(s) has access to all features, accounts and enabled transaction types allowed by your organization. CommunityAmerica strongly encourages each System Administrator to manage all authorized user's entitlements and account access as they're created in online banking. The Manage User/User Role function within CommunityAmerica's online banking platform can assist in this process. It allows System Administrators to manage user features which includes adding additional authorized users, accessing remote deposit capture and managing other entities within the organization using online banking.

Important Note: We will never ask for your password or send a message from anything other than a CommunityAmerica account.

BEST PRACTICES: OPERATIONAL PROCEDURES

TRANSACTION VERIFICATION: CommunityAmerica strongly encourages you to always thoroughly verify payment transactions for authenticity and promptly reconcile accounts. If you receive a request from a vendor to change routing information for an ACH or wire payment, you should authenticate the request by performing a call-back to a number you have on file for the vendor.

DUAL CONTROL: CommunityAmerica requires Dual Control on ACH and wire transactions as part of its standard security requirement. We strongly encourage that Dual Control approvals are completed from separate computers. Some malware is designed to capture multiple users' credentials on the same PC.

SEPARATION OF DUTIES: CommunityAmerica recommends a separation of duties between individuals drafting ACH or wire payments and the staff responsible for verifying and approving these transactions.

For questions about security, please
contact our Commercial Member Support
at TMServices@cacu.com.

BEST PRACTICES FOR COMMERCIAL BANKING

CommunityAmerica®
CREDIT UNION

CommunityAmerica.com