TRUXTON TRUST

A PRIVATE BANK

Best Practices:

Corporate Online Banking Security

These Best Practices assume that your organization has a commercially-reasonable security infrastructure in place. These Best Practices are not comprehensive or all-encompassing nor are they customized for any individual organization's circumstances. In addition, cyber threats are continuously evolving and new threats are constantly emerging; therefore, any best practices list will be, to a large extent, compiled in response to previously attempted cybercrimes. Thus, this document should not be the only method of an organization's ongoing education regarding corporate banking online security. These Best Practices do not provide any guarantee against cyber threats, but rather, some commonly-accepted practices that may help reduce the likelihood of a successful cybercrime. Further research should be conducted on each topic.

Table of Contents

General Internet Security

- **Antivirus and Anti-Spyware Software:** Install and use commercial antivirus and anti-spyware programs. Ensure this software is always up-to-date.

- **Business Email Compromise:** Business Email Compromise is a sophisticated and increasingly common scam in which legitimate business email accounts are compromised in order to initiate unauthorized wire transfers. It is important that individuals be cognizant of and on the alert for Business Email Compromise scams. All organizations should evaluate their processes for transfers of funds. Some recommendations to avoid becoming a victim include:
  - Call to verify the transfer request. Call the requestor directly using a phone number that is already on file. Do not call any number contained within the email and do not reply to the email.
  - Train employees to identify these scams.
  - Verify changes in vendor payment location and confirm requests for transfer of funds.
  - Be suspicious of requests for secrecy or pressure to take action quickly.
  - Register all internet domains that are slightly different from your actual company domain, if possible. Be aware that domains may still be spoofed.

  While Business Email Compromise scams are most commonly geared toward wire transfer transactions, consider these same recommendations when receiving payment instruction changes for any type of payment.

- **Email Security:** Always be aware of an email asking for personal or login information. Train employees to recognize phishing and how to identify potential threats in email and instant messages. Train employees to think before they click. Although fraudulent email can be difficult to recognize, be aware of emails that:
  - Request a link is clicked which may lead to a spoofed website – website spoofing is the act of creating a website, as a hoax, with the intention of misleading readers to believe it is a legitimate website. Since a fraudulent email and websites may use images and messaging from the real company it is spoofing, it can be difficult to identify a spoofed email and website.
  - Ask for a confirmation or update to any personal information, such as Social Security numbers, usernames, passwords, PINs, or account numbers. Even if personal data is not entered, clicking a link in a fraudulent email may download tracking software or a virus that tracks keystrokes to gain personal information. *Truxton Trust will never ask for personal or account information through email.*
  - Use pop-up windows for entering or confirming personal data.
  - Have a sense of urgency asking for information immediately, citing a specific event that might happen if a response is not granted. For example, the email may state that an account may be closed or temporarily suspended if action is not taken as soon as possible.
  - Contain spelling errors and/or bad grammar.

If a suspicious email is received, do not open any attachments or click on any links in the email. *If you believe to have encountered a fraudulent email, contact Truxton Trust immediately at 615-515-1700.*

In addition to education and awareness, an organization may take additional steps to decrease the risk of becoming victim to email fraud. Automate antivirus scanning of email attachments. Implement spam filtering on inbound email to block unsolicited email that may contain malicious code. Spam filtering should validate that the sender has a valid email address and domain name before delivering the email. Implement email validation technologies, such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-Based Message Authentication, Reporting and Conformance (DMARC).

- **Encrypted Applications:** When using applications that require login credentials or process sensitive data, such as online banking and remote deposit, ensure a Secure Sockets Layer (SSL) connection. SSL is the standard security technology for establishing an encrypted link between a web server and a browser and can typically be identified if the URL contains https:// - an "s" after the "p". Certain browsers will also denote if the connection is secure. Truxton Trust employs SSL on truxtontrust.com as well as any account access platforms.

- **Internet Browsers:** Always sign out then close the browser when finished using online applications. Do not click "Remember Me," especially on a public computer. Use the most current version of a recommended browser that supports Secure Sockets Layer (SSL) and 256-bit encryption. Install any updates to a computer's operating system and browser as often as they are made available. Contact Truxton Trust for details regarding browser compatibility with Truxton Trust products.

- **Mobile Devices:** Mobile devices are becoming more common targets of cybercrime. The following are best practices when conducting financial transactions from a mobile device:
    - Conduct business financial transactions from devices that are in compliance with your organization's security policies, enforced through an enterprise mobile security management solution.
    - Do not access bank accounts from public wi-fi or hotspots.
    - Do not circumvent security features or "jailbreak" your mobile device.
    - Ensure encryption is turned on for your mobile device.
    - Keep your mobile devices with you at all times or store them in a secured location when not in use.
    - Mobile devices should be password protected and auto lockout should be enabled. The password should block all access to the device until a valid password is enabled.
    - Ensure your device has current antivirus software and all operating system and application updates and patches. Firewalls should be enabled, if possible.
    - Wireless access, such as Bluetooth and wi-fi to the mobile device should be disabled when not in use to prevent unauthorized wireless access to the device.
    - Only download applications from trusted app stores.
    - Wipe or securely delete data from your mobile device before you dispose of it.

- **Patch Management Policy:** Ensure your organization has an established Patch Management Policy that covers third-party software such as Adobe, Flash, and Java. Ensure that all third party software is updated with the latest security patches. Install new security patches as soon as your operating system and internet browser manufacturers make them available.

- **Secure Locations:** Position computers used to transact business in a secure location. Try to keep computers away from public areas and beware of opportunities for "shoulder surfing" where unauthorized persons might view transactional activity on a computer screen. Consider using privacy screen filters on computer monitors that may be visible to the public.

- **Technology Solutions:** Continue to evaluate and implement technology that attempts to detect threats to which the organization may be susceptible, such as technology that will detect drive-by downloads and zero-day threats. A drive-by download is an unintentional download of software from the internet. A zero-day threat is an undisclosed software vulnerability that hackers can exploit. Zero-day attacks are severe threats and are named as such because the vulnerability is exploited before it is released to the public or sometimes before it is even discovered by the software owner or author.

- **Timeout and Automatic Computer Lock:** Utilize the timeout feature available. Set the computer to lock and show a screensaver after a specified number of minutes of inactivity and require a password to log in. Never leave computers unattended while using any type of online banking service. It is a good habit to lock a computer anytime it is unattended.

- **Whitelisting and Web Monitoring:** Consider deploying "whitelisting" software that only allows approved applications to run on company computers. Implement a Host Intrusion Prevention System (HIPS). Deploy web monitoring and filtering capabilities and block web browsing to non-business related sites, especially those at greater risk of hosting malware.

ID and Password Security

- **Dedicated Computer:** It is recommended that an organization have dedicated computers for online financial transactions, with all email and other web browser capabilities blocked from those dedicated computers.

- **Password Protection:** Remind authorized users to maintain strict confidentiality of login credentials, IDs, and passwords. We recommend changing passwords frequently and using a unique password for each critical system. *A Truxton Trust representative will never request login credentials via phone, email, or text.* Do not respond to a request to disclose this information. Do not share login credentials. Stay away from "guessable" passwords. It is best to stay away from dictionary words. A strong password should be at least 12 characters and include a lowercase letter, uppercase letter, number, and symbol. Do not allow your browser or other systems to remember your password.

- **User Access Restriction:** Assign users access to only the applications and accounts required by their specific job functions. Review user access on a regular basis to ensure unauthorized users have not been added to any system. Notify Truxton Trust of any employee whose employment has been terminated if they have access to online banking or remote deposit so that their access will be revoked.

- **Security Information Available from Truxton Trust:** Truxton Trust will periodically provide important information relating to data security and cyber threats via email, website, and at times US Postal Service. We strongly advise these messages be considered to enhance awareness.

Operations

- **Dual Controls:** Although Truxton Trust does not require dual control, we recommend utilizing dual control for ACH and wire transfers. Dual control is when one person creates or drafts the transaction and a second person authorizes the release of the payment. Truxton Trust recommends that each dual control approval is completed from a separate computer. Known malware is designed to capture multiple users' credentials on the same computer. For information on updating your controls, please contact Truxton Trust at 615-515-1700.

- **Protection of Sensitive Data:** It is recommended to establish and implement appropriate procedures to safeguard the confidentiality and integrity of protected information. Protected information not only includes financial information such as checks received and deposited through remote deposit or mobile deposit, but also sensitive non-financial personal information that may be incorporated into an entry or transaction, such as name and Social Security number. The protection of this data is mandatory to defend against unauthorized use of information that could result in a severe cyber-attack. Keep non-public personal information secure and have a procedure to destroy any such information properly, such as shredding.

- **Separation of Duties:** A separation of duties between the individual(s) verifying activity and reconciling accounts and the individual(s) with authority to originate transactions is recommended. The verifier/reconciler should not be given system authority to originate transactions.

- **Transaction Verification:** Always carefully and thoroughly verify transactions for authenticity and promptly reconcile accounts. If you receive a request from a vendor to change routing information for an ACH or wire transfer, you should authenticate the request to ensure it is legitimate by calling a number already on file, as phone numbers and email addresses can be spoofed. Truxton Trust online banking offers same-day reporting of your transactions and encourages companies to verify activity as quickly as possible during the banking day. *If you believe any transactions are in error or were unauthorized, please contact Truxton Trust at 615-515-1700 immediately.*

Questions on Online Security?

Please contact Kris Long, AAP, at 615-515-1718
or your dedicated Truxton Trust officer.

These Best Practices should not be any organization's only means of protection against cybercrime. These Best Practices should be considered as part of a more comprehensive program to identify and mitigate potential risk from fraud. Even if complied with in its entirety, these Best Practices herein are not a guarantee against becoming a victim of cybercrime or any fraudulent attempt. Truxton Trust makes no guarantee, warranty, or representation as to the results that may be achieved as a result of following these Best Practices and disclaims any liability related thereto. The term "Best Practices" does not mean or imply that these practices are a definitive, all-encompassing, or a uniformly-accepted compilation of optimal security practices.