KCB Bank
Best Practices for Business Banking

In today's world, we all know the importance of protecting sensitive financial information. Don't allow yourself or your business to be vulnerable to threats or hazards that would compromise your responsibility of security. We are providing this document to assist you in your efforts to protect the data used and transmitted by your business. This Best Practices document should not be your sole method of your ongoing education regarding financial protection. These Best Practices do not provide any guarantee against successful attacks, but rather, is an attempt to provide some commonly accepted practices that may help reduce the likelihood that you become the victim of fraud.

Best Practices: KCB Bank Cash Management

-Dedicated PC: KCB Bank strongly recommends that your company utilize dedicated computers for your online financial transactions. Email and other web browsing capabilities should be blocked from dedicated computers.

-User Access: Assign users access to only the functions and accounts they need for their specific job function. Modify authorities if an employee has a change in duties. Immediately delete an employee upon termination. Review user access on a regular basis to ensure authorized users have not been assigned unnecessary permissions and that no unauthorized users have been added.

-Password Protection: Remind users to maintain strict confidentiality of user IDs, passwords, and tokens. Do not share user IDs, passwords, or tokens. Disable automatic password save features in the browsers and software used to access the internet. A KCB Bank employee will never request your login credentials, whether by phone, through email, text, or any other method.

-Separation of Duties: Dual control is a feature that adds more security to Cash Management. It limits a user to only one half of a transaction. If the user creates the transaction, they are unable to process it. It requires a second user to approve and complete the transaction. This separation of duties can help mitigate the chance for internal losses due to fraud. KCB Bank strongly recommends the use of dual control to its Cash Management Users.

-Dual Control: KCB Bank strongly recommends the initiation of ACH and wire requests under dual control: one person creates the ACH or wire requests and a second person authorizes the release of the ACH batch or

wire. KCB Bank also strongly recommends that dual control approvals are completed on a separate computer. Known malware is designed to capture multiple users' credentials on the same computer.

Anti-Virus Protection: Install and use commercial anti-virus, firewall, and anti-spyware programs. Ensure your anti-virus receives daily updates.

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

Whitelisting and Web Monitoring:

-Install "whitelisting" software on computers that only allows approved applications to run. -Deploy host intrusion preventions for computers.
-Deploy web monitoring and filtering capabilities and block all non-business related sites.
-Businesses should especially block access to social networking sites, such as Facebook, YouTube, Twitter, etc. These sites can be havens for malware.

Risk Assessments: We recommend you perform risk assessments at least annually. You should also perform them upon the occurrence of any of the following situations.

- If you become aware of any increased risk of fraud
- If you experience or suspect actual or attempted fraud
- If you become aware of changes to your online banking environment

Technology Solutions: Be proactive in evaluating and implementing technology that detects threats to which your organization may be susceptible, such as technology that would detect drive-by-downloads and day-zero threats.

For more information, watch our online video on ***"ID Theft For Business."*** The video can be found in the **Education Center** link in the upper left hand corner of our homepage or through the link in **Helpful Videos** at the bottom of the homepage.