Exchange

Security Best Practices

Don’t Go Phishing

- **NEVER** click on a link in an email from an unknown source.
- **NEVER** respond to emails claiming to be from ANY Financial Institution regarding your online banking status and asking for credentials.
- **ALWAYS** be suspicious of emails claiming to be from governmental entities or regulatory agency groups that are requesting credentials such as usernames, passwords, PIN codes and similar sensitive authentication information.
- **ALWAYS** be cautious about opening file attachments on emails from unknown sources or attachments on suspicious emails.

Avoid Crimeware

- **UPDATE** your anti-virus software.
- **UPDATE** your operating system, Web browser, and e-mail program on a regular basis
- **NEVER** interact with any suspicious attempt(s) to gain secret codes or information. Be aware of how each online banking system for your company’s banking relationships utilizes tools to combat fraud.
- **EDUCATE** employees.
- **CONSIDER** using a dedicated PC for doing your online business banking.

Exchange

- Any Token Serial Number on screen requests should be reported to BOK Financial Treasury Client Services immediately.
- **ONLY** enter your one-time or token passcode as instructed in the Quick Reference Guides located on the Exchange Resource Center. **NEVER** enter it directly on the login page.
- **NEVER** enter a Secure token SERIAL NUMBER on the Exchange site.
- **NEVER** respond to an Exchange authentication request for any services other than those listed below:
  - Login (triggered after you input your credentials and hitting “Log in”)
  - Approving Wire Payments
  - Approving ACH Payments
  - Forgot Password
  - User Administration Changes
- Users sharing a job for your company should **NEVER** share Exchange user credentials.

Exchange Separation of Permissions & Duties

- Require different users for transaction entry versus transaction approval.
  - A setting is applied at ACH Company level in Exchange automatically requiring a different user to initiate the payment versus approve the payment. Requiring two different approvers is also available.
  - This separation of permissions makes it much more difficult to be compromised since multiple users’ workstations would be required to become infected for the fraud to be successful.
- Require different individuals to be responsible for payments versus reconcilement of all banking accounts.
- Require a different user to create payment templates and for approving them for use. This would also require dual control for any payment template additions or changes.

Mobile Security

- Choose devices carefully. Use mobile devices that have the best possible control and security.
- Use a password/lock code. Enable password/PIN and create passwords that are difficult for others to guess and change them often.
  - Set the screen time-out to five minutes or less.
  - Avoid using auto-complete features that remember names or passwords.
- **ALWAYS** remember multi factor authentication is required/requested when approving an ACH or Wire Payment within Exchange Mobile.
- Use secure wireless connections.
  - Avoid public WiFi hotspots (use cell phone network instead of insecure WiFi).
  - Keep optional network connections (i.e. WiFi and Bluetooth) turned off except when you are using them.
  - Don’t access personal or financial data with public WiFi.
  - Turn off GPS tracking services for non-essential applications.
  - Enable GPS tracking services for any application that helps you locate the device if it is lost or stolen.

Mobile Security (continued)

- Physical Security. Follow these best practices for physically securing your mobile device:
  - Do not leave your device unattended. Keep it with you at all times, or leave it in a secure location. This not only prevents against malicious access to your data, but also against inadvertent or accidental loss or damage of your data, such as when a child finds it and attempts to use it.
  - Be particularly cautious about keeping your device safe in airports and other public places.
  - Be inconspicuous. Carry your smartphone, tablet or laptop in a way that does not attract the attention of someone who might want to steal it.
  - Label your property. Put a sticker on your phone with your name and contact information. This low-tech, practical step enables someone to contact you if they found your lost phone, even if the battery is dead.
  - Keep records of your device's identifying information such as serial number, MAC address, etc.; and the data and place of purchase. This information can help authorities track or identify a lost or stolen device.
- Once you have finished your online or mobile banking session, always log off before visiting other sites on the internet.
- Shore Up Bluetooth. Bluetooth capabilities on today's smartphones may make it easy to talk on hands-free headset, but they're also a target for hackers, who can take advantage of its default always-on, always-discoverable settings to launch attacks. In order to limit your exposure, US CERT recommends that users disable Bluetooth when it is not actively transmitting information. It also suggests switching Bluetooth devices to hidden mode.
- Manage your applications wisely.
  - Download apps only from trustworthy sources.
  - Don't install a new app until it has established a good reputation.
  - Keep applications updated. Remove applications you no longer use.
  - Don't "root" or "jailbreak" your device or install third-party firmware.
- Lost or stolen device.
  - If your mobile device is lost or stolen, call your Treasury Client Services Representative to deactivate your mobile device.

ALWAYS REMEMBER...

Immediately escalate any suspicious transaction activity to a BOK Financial Treasury Client Services Professional or any Financial Institution that is used by your company. There is a limited recovery window for commercial transactions and immediate escalation may prevent losses.