Business Fraud Prevention Best Practices

In today's fast-paced business environment, you need to be able to protect your business's assets. Let our Fraud Prevention Best Practices provide you with tips to shield your business from fraud and scams.

USER ID AND PASSWORD GUIDELINES

- Create a "strong" password with at least 12 characters that includes a combination of mixed case letters, numbers, and special characters.
- Implement Multifactor Authentication (MFA) where available.
- Change your password frequently.
- Never share username, password, or token information with anyone, including third-party providers.
- Avoid using an automatic login feature that saves usernames and passwords.

EBUSINESS SOLUTIONS GUIDELINES

- Do not use public or other unsecured computers for logging into eBusiness Solutions.
- Users should check the last login date/time every time they log in. Last login date/time is displayed on the Welcome Page.
- Review account balances and detailed transactions on a daily basis to confirm payment and other transaction data and immediately report any suspicious transactions to us. Review historical and audit reports regularly to confirm user access and transaction activity.
- Take advantage of and regularly view system alerts. Examples include:
  - ACH Alerts
  - Wire Alerts
  - Security Notification Alerts
- Do not use account numbers, your Social Security number, Tax ID number, or other account or personal information when creating account nicknames or other titles.
- Use the historical reporting features of your online banking application on a regular basis to confirm payment and other transaction data.
- Never leave a computer unattended while using eBusiness Solutions.
- Never conduct banking transactions while multiple browsers are open on your computer.
- Change your password frequently.
- Enable a screen lockout after 15 minutes of inactivity to keep confidential data secure when you are not at your desk.
- An FBI-recommended best practice is that company users dedicate a PC solely for financial transactions (e.g., no web browsing, emails, or social media). This can effectively seal off threats that can come from visiting various websites, which could lead to becoming a target for hackers and Corporate Account Take Over (CATO).
- To maintain security best practices and mitigate risk, the company should periodically perform IT risk assessments on the business environment.
- Familiarize yourself with bankESB's Cash Management Master Agreement and Internet Banking Services Schedule. **Immediately escalate any suspicious activity or transactions to a bankESB representative by calling 855.527.4111.** *There is a very limited recovery window for unauthorized ACH debits or withdrawals and immediate escalation may prevent loss.*

ADMINISTRATIVE USERS

- Prohibit the use of "shared" usernames and passwords for eBusiness Solutions.
- Limit administrative rights on users' workstations to help prevent the inadvertent downloading of malware or other viruses.
- Dedicate and limit the number of computers used to complete online banking transactions; do not allow Internet browsing or email exchange, ensure these computers are fully up to date with system patching and are equipped with the latest versions and patches of anti-virus, anti-malware, and anti-spyware software.
- Delete online user IDs as part of the exit procedure when employees leave your company. Review and adjust user entitlements as access needs change and delete any inactive users.
- Use multiple approvals for monetary transactions and require separate entry and approval users.
- Establish transaction dollar limits for employees who initiate and approve online payments such as ACH batches, wire transfers, and account transfers.

TIPS TO PROTECT ONLINE PAYMENTS, ACH & WIRES

- Require dual control of ACH and wire transfer payments. Each transaction should be drafted by one employee and approved by another (dual control).
- Take advantage of transaction limits. Establish limits for monetary transactions at maximum daily limits and maximum per transaction limits.
- Use pre-notification transactions to verify that account numbers within your ACH payments are correct.
- When you have completed a transaction, ensure you log off to close the connection.
- Use separate accounts for electronic and paper transactions to simplify monitoring and tracking of any discrepancies.

TIPS TO AVOID PHISHING, SPYWARE & MALWARE

- Do not open email from unknown sources. Be suspicious of emails purporting to be from a financial institution, government department, or other agency requesting account information, account verification, or banking access credentials such as usernames, passwords, PIN codes, and similar information. Opening file attachments or clicking on web links in suspicious emails could expose your system to malicious code that could hijack your computer.
- Do not enter token codes into links that you clicked on in an email. Instead, type the URL of the reputable site to which you want to authenticate.
- Never respond to a suspicious email or click on any hyperlink embedded in a suspicious email. Call the purported source if you are unsure who sent an email. If an email claiming to be from us seems suspicious, checking with us is appropriate. **bankESB will never call you and ask for personal or business information over the telephone or request information via email.**
- Install commercial anti-virus, anti-malware, and spyware detection software on all computer systems. Update all of your computers regularly with the latest versions and patches of anti-virus, anti-malware, and anti-spyware software. Free software may not provide the level of protection against the latest threats that a licensed industry standard product can.
- Ensure computers are patched regularly and up to date, particularly operating systems, browsers, and key applications.
- Install a dedicated, actively managed firewall, especially if using a broadband or dedicated connection to the Internet, such as fiber or cable. A firewall limits the potential for unauthorized access to your network and computers.
- Check your settings and select, at least, a medium level of security for your browsers.
- Be advised that repeatedly being asked to enter your password/token code are signs of potentially harmful activity.

TIPS FOR WIRELESS NETWORK MANAGEMENT

Wireless networks can provide an unintended open door to your business network. Unless a valid business reason exists for wireless network use, it is recommended that all wireless networks be disabled. If a wireless network is to be used for legitimate business purposes, it is recommended that wireless networks be secured as follows:

- Change the wireless network hardware (router or access point) administrative password from the factory default to a complex password. Save the password in a secure location as it will be needed to make future changes to the device.
- Disable remote administration of the wireless network hardware (router or access point) and if possible, disable broadcasting of the network SSID.
- If your device offers WPA encryption, secure your wireless network by enabling WPA2 or higher encryption on the wireless network. If your device does not support WPA2 or higher encryption, enable WEP encryption.
- If only known computers will access the wireless network, consider enabling MAC filtering on the network hardware. Every computer network card is assigned a unique MAC address. MAC filtering will only allow computers with permitted MAC addresses access to the wireless network.

TIPS TO AVOID BUSINESS EMAIL COMPROMISE (BEC)

- Treat email with caution! Email is a gateway into your computer and personal information, so make sure you only open emails/attachments from known senders and, in general, be wary of emails with attachments and links. Stay vigilant and make sure everyone on your team stays alert.
- Check for spoofed (i.e., false and deceptive) domain names. This can help you identify if someone might be launching a Business Email Compromise (BEC) scam against your company.
- Limit publicly available information. Criminals use public information to target companies for BEC scams.
- Implement a formal process for money transfers and documentation requests and ensure there is a formal process for high-risk transactions such as wire transfers and requests for sensitive documentation.
- Require dual approval for high-risk transactions. Segregation of duties and including more than one individual in a transaction is a great way to help mitigate external and internal fraud.
- Use Forward instead of Reply. When receiving an email requesting a money transfer or for sensitive information, using forward and sending it back to the intended recipient can help you avoid falling victim to a BEC scam that utilizes a spoofed domain.
- Use Out of Band to Verify. Use a different channel to verify. If the request came in via email, use phone (and not the phone number that is in the email) and vice versa. Also be sure to verify the beneficiary bank and account number.
- Color code emails so that emails from employees or internal accounts are one color, and emails from non-employees or external accounts are another color.
- When adding new vendors, change vendor payment information by using phone verification as part of the two-factor authentication. When doing this, use previously known phone numbers, not the numbers provided in the email request.
- Don't get complacent and stay vigilant. Fraud is ever-changing, so keep your team and yourself up to date.

bankESB®

bankESB.com | 855.527.4111