Fraud Awareness Tips & Techniques

Security Techniques

- **Install a security software suite from a reputable vendor that provides detection and remediation for cybersecurity threats such as viruses, spyware, malware and email phishing.. Keep the software up-to-date through an automatic update feature and configure it to perform recurring, automated complete system scans on a routine basis.**
- **Protect your passwords. Never have password information written down. Do not share user IDs, or passwords.**
- **Utilize Multi-Factor Authentication (MFA) whenever possible to better safeguard access to data and applications. When MFA is enabled, every time you login to online banking, you will be prompted to validate your credentials via the MFA software. If for any reason you login and are not asked for this validation, it may indicate you have been redirected to a malicious website. Please close your browser and contact us immediately.**
- **Utilize IP Restrict when available to limit access to online banking resources only from approved internet protocol (IP) addresses.**
- **Midwest BankCentre utilizes online credentials protection that provides an additional layer of end user security by encrypting each keystroke as user IDs and passwords are entered. This helps ensure that end-user credentials cannot be harvested via browser-based malware.**
- **Do not allow your computer or web browser to save your login names or passwords.**
- **Be suspicious of emails and text messages purporting to come from Midwest BankCentre or government agencies requesting verification of information. Do not click on any links provided, always type in**
- **https://www.MidwestBankCentre.com/ in your internet browser address bar to access our site.**
- **Utilize a security expert to test your network or run security software that will aid you in detecting and remediating known vulnerabilities.**
- **Be aware of changes to the look of your online banking login screens. If the screens are unfamiliar or you are prompted multiple times for a security code, contact us immediately.**
- **Always use dual control when processing any payment entries; one individual to initiate the entry and a second individual to approve the entry.**
- **Educate users on good cybersecurity practices to include how to avoid having malware maliciously installed on a computer.**

Continued ▸

- **Monitor and reconcile your accounts daily. Keep all account information secure.**
- **Ultimately the best way to insulate your business against fraudulent online banking transactions is to use a dedicated PC that is not used for other online activity. Implement white listing methods to prevent the system from going to any site/address that does not have a documented business need. This would include, web browsing, social networking and most importantly email.**
- **Purchase Insurance - While there are many precautions you can take, no measure is foolproof. Consider getting an insurance policy that specifically protects against fraud.**
- **Always make a call back verification when a business/consumer is requesting to change their banking information. Do not call the number on the email/fax, call the number in your file.**
- **How to discover a bad email – hover over the email address to verify the email address matches your records.**

ACH Payment Awareness

- **Always set up dual control for any outgoing payments, one user to initiate the ACH and a second user to approve the ACH.**
- **Review user permissions and limits periodically. Administrators should set user permissions and limits based off your company's historical transmissions.**
- **Obtain written authorizations from all ACH participants. Any time you set up a new participant to either send money to or receive money from, you are required to have them sign an authorization agreement. You must keep these on file for at least 2 years after the revocation of the authorization.**
- **Take action immediately to correct an ACH participant's banking information when a Notice of Return or Correction is received. For changes to routing or account number, you are required to receive a new authorization form from the participant.**

Wire Payment Awareness

- **Wire transfers pose one of the single greatest risks of loss to a company because of the speed with which losses can occur, the potential size of such losses, and the inability to recover the funds once they are transferred to the destination institution.**
- **Always send wire payments out using dual control, one user to initiate the wire and a second user to approve the wire.**
- **Administrators should set reasonable wire transfer limits for all users.**
- **Monitor and reconcile your accounts daily.**
- **Never access your online banking to send a payment from a public computer at a hotel, library or public wireless access point.**
- **Never share user IDs or passwords.**