Buckeye
State Bank

Online Banking Best Practices

Buckeye State Bank strives to offer online banking products that are fast, secure and easy to use. Since Buckeye State Bank does not implement, oversee or monitor the computer security infrastructure for bank client computers/networks, we are providing a partial list of things you can do to protect your accounts and information from fraudulent activity.

- Never share User identifications, passwords, PINs, security tokens, etc., with anyone, and do not leave any such information or items in an area that is not secured. Use a unique login identification and password for online banking than any other website or software. Passwords should not contain predictable terms or numbers.
- Never leave a computer unattended when using any online banking or financial services, and always lock your computer when you have logged off such sites and are leaving the computer unattended. Never access your financial institution's online banking website from a public computer (hotel, library, etc…)
- Monitor & reconcile your accounts frequently. Immediately review wire transfer, ACH or other electronic account transactions. Immediately report any suspicious activity on your accounts to Bank personnel.
- Do NOT click on a link in any email purported to be sent from the Bank. Be suspicious of any emails purporting to be from any financial institution, federal, state or local government departments or agencies or taxing authorities that request account information. If you provide financial information and passwords for financial services in response to unfamiliar or suspicious websites, emails, text messages, telephone calls, mobile phone applications or social media messages, you should change your password immediately.
- Use caution when opening email attachments from unknown senders. These attachments can exposure your computer to malicious code or malware that will be installed on your computer.
- Install antivirus, anti-malware, anti-spyware and a firewall and maintain the software with the most recent updates. In addition, operating system updates (also referred to as "patches") should be accepted, downloaded, installed and run promptly, and as recommended.
- Limit or eliminate unnecessary Internet use and email activity on computers used for online banking. Use caution when utilizing a Wi-Fi network as most do not encrypt information and are not secure.
- Verify use of a secure session (https:// and not "http ://) and avoid saving passwords to a computer. Verify a website's privacy policy is easily found and understood.

In addition commercial clients should:

- Implement a system of dual control and approval for ACH and wire transfers where dual approval is required before a transaction is initiated. One employee should be responsible for originating/initiating the transaction and a second employee must authorize the transaction prior to it being processed. Dual approvers should access and approve from different machines and utilize the Multifactor Authentication (MFA) token provided by the Bank.
- Develop internal Internet and information security practices and train personnel. These practices may include: limiting Internet access to websites approved for business use and blocking all other websites; discouraging password-sharing among employees; preventing or discouraging employee use of laptops and tablet devices to access sensitive information over unsecured Wi-Fi systems; and limiting access to established business hours only.
- Regularly review employees with access to online banking for user approval, access rights and terminated employees or employees no longer responsible for online banking transactions.

Use Mobile Phones, Mobile Banking and Mobile Payments Securely

- Mobile phone applications, text messages, instant messages and calls from unfamiliar or suspicious sources that request personal financial information and passwords should be declined and, when appropriate, promptly deleted.
- Mobile phones should be set to logoff automatically after a short period of non-use, with a password required to log back into the phone. Mobile Phones should be locked up when not in use and not left in visible, unsecured locations. Lost or stolen phones should be reported to the carrier promptly.

Use Social Media Securely

- The highest available level of privacy and security settings should be selected and activated on any social media site. No information that can be used to compromise information security should be viewable on any social media site. Such information includes the names of financial institutions, card companies, commerce websites, Internet service providers, utilities and wireless carriers with which you have accounts. This also includes personal financial information, passwords, phone numbers, email addresses, addresses and dates of significance.
- Accept only known and trusted individuals into your social network. Do not allow social media sites to scan your address book.

Use ATM, Credit, Debit and Prepaid Cards Securely

- Card numbers should only be used in secure transactions and should not be provided in response to unfamiliar or suspicious websites, emails, text messages, telephone calls, mobile phone applications or social media messages.
- As applicable, cards should be signed as soon as they arrive. Cards should not be left in visible or unsecured locations. Lost or stolen cards should be promptly reported to the card issuer. Cards that are unused, have been canceled or have been replaced by a new card should be securely eliminated.

Use Statements and E-Statements, Bills and E-Bills, and Transaction Receipts Securely

- Statements, e-statements, bills and e-bills should be reviewed promptly upon receipt and verified with transaction receipts to ensure all transactions were made by authorized parties; any unauthorized transactions should be reported to the appropriate financial institution, card issuer or biller.
- Transaction receipts should be saved and compared to states
- Financial institutions, card issuers and billers should be notified in advance of a change of address.
- Statements, bills and transactions receipts that are to be discarded should be securely eliminated.

Monitor Credit Accounts

- Credit accounts and reports should be monitored regularly. Any unauthorized or suspicious activity should be promptly reported to the appropriate financial institution, card issuer, local law enforcement agency and the Federal Trade Commission (877-438-4338, or online at www.consumer.gov).
- As a precaution, you may choose to place a fraud alert on your credit file. A fraud alert will notify you before unauthorized third parties open new accounts in your name or charge existing accounts in your name. This can be done at no charge to you. To receive fraud alerts, contact Equifax® (800-525-6285), Experian® (888-397-3742) or TransUnion® (800-680-7289)

DISCLAIMER: Buckeye State Bank does not provide any express or implied warranty, guarantee or promise concerning the content, completeness, accuracy or value of the above information. All persons or entities should confirm the accuracy as it applies to them specifically or their business or system. These "online banking best practices" are provided as information only and Buckeye State Bank will have no liability to a client or any other person or entity, for any direct, indirect, incidental, special or consequential damages arising out of the information above.