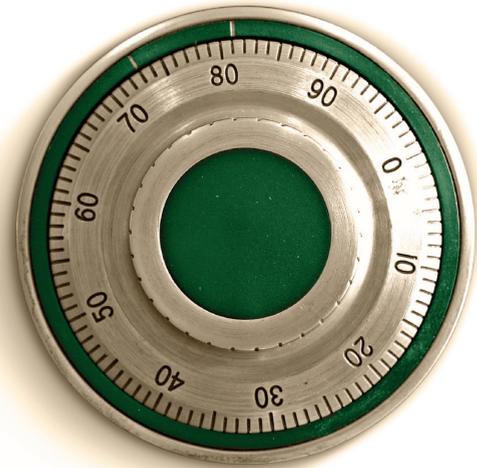




bibank.com

Come by any office

Call us at 877-865-5050



The security of personal information held by your company is very important to Bank Independent. We want to work with you to protect it.



Member
FDIC



Data Security Planning

Are you taking steps to protect personal information? A sound data security plan is built on five key principles:

- **Take Stock:** Know what personal information you have in your files and on your computers.
- **Scale Down:** Keep only what you need for your business.
- **Lock It:** Protect the information that you keep.
- **Pitch It:** Properly dispose of what you no longer need.
- **Plan Ahead:** Create a plan for responding to security incidents.

Corporate Account Takeover

Corporate Account Takeover is a form of identity theft in which criminals steal your online banking credentials. Attacks are usually stealthy. Malware introduced into your system may go undetected for long periods of time. Account-draining transfers using stolen credentials may happen at a time when they are not noticed. Protect yourself by following sound business practices:

- **Use Layered System Security:** Create layers of firewalls, anti-malware software and encryption. Install robust anti-malware programs on every file server, workstation and laptop, and keep them updated.
- **Use a Single, Dedicated Computer for Online Banking and Cash Management:** Do not connect this computer to your business network, use it to retrieve e-mail messages, or use it for any online purpose except banking.
- **Educate Your Employees About Cybercrimes:** Explain the risks of opening e-mail attachments or providing confidential information, and ensure that they understand that just one infected computer can lead to an account takeover.
- **Block Access to High-Risk Websites:** Prevent access to any website that features adult entertainment, online gaming, social networking and personal email that can inject files into your network.
- **Establish Separate User Accounts and Limit Administrative Rights for Employees Accessing Financial Information:** Many malware programs require administrative rights to the workstation and network in order to steal credentials.
- **Use Approval Tools in Cash Management:** Requiring two people to issue a payment – one to set up the transaction and a second to approve the transaction – doubles the chances of stopping a criminal from draining your account.

- **Review or Reconcile Accounts Online Daily:** The sooner you find suspicious transactions, the sooner the theft can be investigated.

Risk Assessment

We recommend that our business customers, especially those using Independent Deposit (remote deposit capture), ACH origination or wire transfer services, conduct a periodic risk assessment and controls evaluation. We provide a Small Business IT Risk Assessment template that may be used for this review.

Electronic Transaction Protection

Consumers are provided certain protections against unauthorized electronic transactions according to how soon they are reported. In general, *these protections are provided on consumer accounts only and do not apply to business accounts.*

Reporting Suspicious Activity

Contact Customer Service at 256-386-5000 or 877-865-5050 to report suspicious activity on your Bank Independent accounts or e-mails asking you to provide Bank Independent online IDs, passwords, or other account information. *We will never ask for your personal information through an e-mail.*

To learn more about identity protection, visit the Education Center at bibank.com or one of these websites*:

www.ftc.gov
www.usa.gov
www.stopfraud.gov
www.idtheft.gov
www.onguardonline.gov

If you have questions about identity protection, contact Customer Service at 256-386-5000 or 877-865-5050.

*Bank Independent neither endorses nor guarantees in any way the organizations, services or advice associated with these links and is not responsible for the accuracy of the content found on these sites.

