Corporate Account Takeover |
Busey offers tips to small businesses for combating fraud.

Cybercriminals are increasingly targeting small businesses to transfer funds from accounts and steal private information, a fraud referred to as "corporate account takeover." Criminals use spoofed emails, malicious software and online social networks to obtain login credentials to businesses' accounts, which they then use to make illicit transactions. Small businesses are a growing target for account takeover, but a partnership with Busey will give you the tools needed to shield yourself from this attack.

Combating account takeover is a *shared responsibility* between businesses and financial institutions. *Your banker* can explain the safeguards small businesses need and the numerous programs available that help ensure fund transfers, payroll requests and withdrawals are legitimate and accurate. *You can* train employees about safe internet use and the warning signs of this fraud, as they are the first line of defense. ***Together, Busey and our customers are far more effective at combating account takeover than going at it alone.***

Here are a few tips to help prevent account takeover:

- **Protect your online environment.** It is important to protect your cyber environment just as you would your physical location. Do not use unprotected internet connections. Apply operating system and application updates (patches) regularly. Ensure anti-virus/spyware software is installed, functional and updated to the most current version. Encrypt sensitive data and use host-based firewall software. Change passwords from the default to something complex, including at point-of-sale terminals.

- **Partner with your bank for payment authentication.** Talk to your banker about services that offer call backs, device authentication, multi-person approval processes, batch limits and other tools that help protect you from unauthorized transactions.

- **Pay attention to suspicious activity and react quickly.** Put your employees on alert. Watch for strange network activity, do not open suspicious emails and never share account information. If you suspect a problem, disconnect the compromised computer from your network and contact your banker. Keep records of what happened. Monitor and reconcile accounts daily to catch fraudulent activity early. Businesses that do not reconcile their accounts daily may not recognize fraudulent activity until it is too late to take action.

- **Understand your responsibilities and liabilities.** The account agreement with your financial institution will detail what commercially reasonable security measures are required in your business. It is critical you understand and implement the security safeguards in the agreement. If you don't, you could be liable for losses resulting from a takeover. Talk to your banker if you have questions about your responsibilities.