The Clay City Banking Co

331 S. Main St
P.O. Box 465

Clay City, Illinois 62824
Ph: 618-676-1511

What is Corporate Account Takeover?

Corporate account takeover is a type of fraud where thieves gain access to a business' finances to make unauthorized transactions, including transferring funds from the company, creating and adding fake new employees to payroll, and stealing sensitive customer information that may not be recoverable.

Corporate account takeover is a growing threat for small businesses. It is important that businesses understand and prepare for this risk.

Cyber thieves target employees through phishing, phone calls, and even social networks. It is common for thieves to send emails posing as a bank, delivery company, court or the Better Business Bureau. Once the email is opened, malware is loaded on the computer which then records login credentials and passcodes and reports them back to the criminal.

The best way to protect against corporate account takeover is a strong partnership with your financial institution. Work with your bank to understand security measures needed within the business and establish safeguards on the accounts that can help the bank identify and prevent unauthorized access to your funds.

A shared responsibility between the bank and the business is the most effective way to prevent corporate account takeover. Consider these tips to ensure your business is well prepared:

o Educate your employees. Strong security programs paired with employee education about the warning signs, safe practices, and responses to a suspected takeover are essential to protecting your company and customers.

o Protect your online environment. Do not use unprotected internet connections. Encrypt sensitive data and keep updated virus protections on your computer. Use complex passwords and change them periodically.

o Partner with your bank to prevent unauthorized transactions. Talk to your bank about programs to safeguard you from unauthorized transactions.

o Pay attention to suspicious activity and react quickly. Look out for unexplained network activity, pop ups, and suspicious emails.