RIVER BANK

We Bring Banking to You!

PROTECT YOUR BUSINESS FROM CORPORATE ACCOUNT TAKEOVER

What would you do if you suddenly noticed that huge chunks of money had been drained from your business account into overseas accounts? Online criminals are using increasingly sophisticated techniques to commit payments fraud against commercial business accounts.

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 new fake employees to payroll, and stealing sensitive customer information that may not be recoverable. Thousands of businesses have fallen victim to this type of fraud, and the losses have ranged from a few thousand to several million dollars.

What's more, business bank accounts are NOT protected under Regulation E, so when business accounts are compromised, they often lose all, or at least some of their money.

Today security is a shared responsibility between you and your financial institution. Corporate account takeover attacks today are typically perpetrated quietly by introducing malware through a simple phishing email, a deceptive social engineering ploy, or an infected website. For a business that has low resistance to attack, the may remain undetected for weeks or even months.

How do I protect my business?
The best way to protect your business is to develop a strong partnership with your financial institution and establish safeguards on your accounts to help the bank identify and prevent unauthorized access to your funds.

- **Develop a security plan.** Each business should evaluate its risk profile and develop a security plan that includes sound business practices.

- **Protect your online environment.** Protect your computers just as you would your cash. Use appropriate tools to prevent and deter unauthorized access to your network and make sure you keep them up to date. Encrypt sensitive data and use complex passwords and change them regularly.

- **Create a secure financial environment.** Dedicate one computer exclusively for online banking. This computer should not be connected to the business network, have email capability, or connect to the Internet for any purpose other than online banking.

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

- **Pay attention to suspicious activity and react quickly.** Watch for unexplained account or network activity, pop ups, and suspicious emails. If detected, immediately contact your financial institution, stop all online activity and remove any systems that may have been compromised. And keep records of what happened.

- **Understand your responsibilities and liabilities.** The account agreement with your bank explains what reasonable security measures are required in your business. You need to understand and implement these security safeguards. If you don't, you could be liable for any losses.

- **Educate all employees** about cybercrimes so they understand that even one infected computer can lead to an account takeover. One infected computer can compromise the entire network. All employees, even those with no financial responsibilities, should receive security awareness training.

Since cyber threats change rapidly, it's important that you stay informed about the evolving threats and adjust your security measures accordingly. You and your employees are the first line of defense against corporate account takeover.

MySECURITY
Awareness.com