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? Unfortunately, online criminals are using increasingly sophisticated techniques to commit payments fraud against commercial business accounts. Let's take a closer look at corporate account takeover, how federal regulators and financial institutions are collaborating to help you to prevent it from happening to your business, and finally your responsibility to protect yourself.

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.

Regulation E
Consumer bank accounts enjoy a certain level of protection that business bank accounts do not. Under Regulation E, there are liability limitations for unauthorized electronic fund transfers affecting consumer bank accounts. Business bank accounts do not get this kind or protection. So when business accounts are compromised, they often lose all or at least some of their money.

Customer vs. Bank
A good example of this is the court case between Patco Construction Company and their financial institution Ocean Bank. Patco computers had become infected with malware allowing fraudsters to make six wire transfers using the Automated Clearing House (ACH) transfer system amounting to more than $588,000. Only $243,000 of the stolen money was recovered. What ensued was a three-year court battle between the company and their financial institution to decide who was at fault. In the end, both were losers. Businesses and banks aren't only losing millions to fraud; they are losing millions more in legal costs, productivity losses and negative PR. The only winners in these cases are the cybercriminals.

What regulators & banks are doing to prevent corporate account takeover
In an effort to protect both consumers and businesses from financial fraud, the Federal Financial Institutions Examination Council (FFIEC) has implemented and will continue to establish new security guidelines for financial institutions. These guidelines enforce the implementation of a layered security approach, risk assessments and customer security education and awareness. You can learn more about this from your financial institution.

Who's responsible?

The question remains, "In light of the increasing and more sophisticated cyber threats, who is ultimately responsible for ensuring the security of your bank account?" The financial institution must protect their online banking technology and ensure the security of online transactions, but what responsibility does the customer have to protect their own computing systems against attack? Today security is a shared responsibility between the financial institution and the customer.

As in the case of Patco Construction, corporate account takeover attacks today are typically perpetrated quietly by the introduction of malware through a simple phishing email, a deceptive social engineering ploy, or an infected website. For a business that has low resistance to such methods of attack, the malware introduced onto its system may remain undetected for weeks or even months.

How do I protect myself and my business?

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 to 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:

- **Develop a security plan.** Each business should evaluate its Corporate Account Takeover risk profile and develop a security plan that includes sound business practices.
- **Protect your online environment.** Protect your cyber environment 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 will detail what commercially reasonable security measures are required in your business. You need to 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 any questions about your responsibilities.

- **Educate all employees** about cybercrimes so they understand that even one infected computer can lead to an account takeover. An employee whose computer becomes infected can infect the entire network. For example, if an employee takes a laptop home and accidentally downloads malware, criminals could gain access to the business's entire network when the employee connects again at work. All employees, even those with no financial responsibilities, should be educated about these threats.

Stay informed about defenses to Corporate Account Takeover. Since cyber threats change rapidly, it's imperative that you stay informed about evolving threats and adjust your security measures accordingly.

You and your employees are the first line of defense against corporate account takeover. A strong security program along with employee education about the warning signs, safe practices, and responses to a suspected takeover are essential to protecting your company and customers.

These helpful tips are reprinted from My Security Awareness and were originally provided by InfoSight, Inc., an information security consultancy working to help ensure the privacy and security of your corporate, personal and financial information.