Windsor Federal SAVINGS

Windsor Federal Savings recognizes a growing threat to businesses and offers the following information in an effort to assist in mitigating potential losses.

The Small Business Guide to Corporate Account Takeover

What is Corporate Account Takeover?

Corporate account takeover (also known as CATO) 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.

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

Online thieves target owners and employees through phishing, phone calls, and even social networks. It is common for thieves to send emails posing as a bank, a 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 criminals.

Employee Education is Essential, but is Missing the Mark

Ninety-two percent of respondents to a recent survey indicated employee education of small business employees was effective in reducing the threat of account takeover. However, nearly 80 percent of respondents to a small business survey said they had no formal internet security policy, with almost half indicating they provide no internet safety training to employees.

How do I protect myself and my small business?

The best way to protect against corporate account takeover is a strong partnership with Windsor Federal Savings. It's important to understand the security measures needed within the business and to establish safeguards 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:

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

- **Protect your online environment.** It is important to protect your online environment just as you would your cash and physical location. Do not use unprotected internet connections. Encrypt sensitive data and keep updated virus protections on your computer. Use complex passwords and change them periodically. Restrict the functions on the computer workstation that is used for online banking and bill payment. Use a dedicated PC that is not used for other online activity. Use/Install spam filters, anti-virus software and malware detection software.

- **Partner with Windsor Federal to prevent unauthorized transactions.** The Bank has programs that can help safeguard you from unauthorized transactions. We offer services such as call backs, out of band authentication, device authentication, multi-person approval processes and batch limits to help protect you from fraud.

- **Pay attention to suspicious activity and react quickly.** Look out for unexplained account or network activity, pop ups, and suspicious emails. Be wary of unsolicited email messages (spam) and the links contained in them. If detected, immediately contact the Bank to review your account history with a representative, stop all online activity and remove any systems from the network that may have been compromised. Keep records of what happened.

- **Understand your responsibilities and liabilities.** Our Deposit Account Agreement's **Security** section, as well as other service agreements such as ACH, RDC and Wire Transfer, details what commercially reasonable security measures are required. It is critical that you understand and implement security safeguards. Failure to do so may result in losses stemming from a takeover.

FBI Releases Warning to Businesses (January 2015)

The FBI's Internet Crime Complaint Center issued a public service announcement regarding an increase in phishing scams targeting businesses that work with foreign suppliers and perform regular wire transfer payments. Visit http://www.ic3.gov/MEDIA/2015/150122.ASPX to access the public service announcement for more information including various versions of the scam, characteristics of the complaints received and recommended mitigation tips.

We'd like to stress the importance of educating yourself and your employees on the security of your information. Your physical and online presence need to be safeguarded against unauthorized access. If you have any questions, please contact your Account Manager or Customer Service.