

Salisbury Bank is committed to helping your business and protecting your accounts. One way we do this is by keeping you informed about important news that affects your online security.

Protect your Business from Online Fraud

Electronic fraud is a multi-billion dollar industry that can silently rob your business of all its cash assets without you even knowing it. In one common scenario cyber thieves plant keylogging spyware on computers that pirates sensitive information about bank accounts. The spyware is then used to steal money from the accounts. According to a 2010 report by the Anti-Phishing Working Group, this type of crime continues to climb.

Online cash management customers at banks across the country have been targeted. This type of fraud takes advantage of compromised computer security, poor treasury management practices, and weak authentication. It has happened with ACH payments as well as wire transfers. Here's how it works:

- 1.** Keylogging spyware infects corporate treasury workstations or company computers used to log on to online banking. This is usually accomplished in one of two ways. It may come in emails pretending to be from legitimate businesses, financial institutions or government agencies. Or it can be planted on a computer when users surf the Internet and go to sites with lax security measures. The victim is tricked into running software, opening a harmful attachment or visiting a malicious website that allows criminals to install keylogging software. This spyware records the company's online banking credentials, such as User IDs and passwords, when employees log on to online banking. The software then sends this information back to the perpetrator.
- 2.** The perpetrator uses the company's credentials to log on to the company's account and initiates money transfers out of the account, either via ACH credits or wire transfers, routing funds to deposit accounts at various financial institutions. These accounts may have been opened by the perpetrator or by unknowing individuals or willing associates recruited by the perpetrator.
- 3.** These account owners immediately wire the funds overseas, at which point the money cannot be recovered by the company or its bank.

You can help to prevent this type of fraud from happening to your company by taking critical steps to protect your bank accounts, including:

- Use best practices for online cash management services, including authentication for authorizing transactions online and / or dual confirmation of outbound transfers.
- Keep your SecurID token and serial number in a secure place.
- Utilize security features such as IP Restrict and Time Restrict.
- Review account activity periodically throughout the day and at wire / ACH deadlines to verify transactions. Immediately report any questionable transactions to Salisbury Bank by calling our Deposit Services Department at 860-435-9801.
- Reconcile accounts daily.
- Use best practices for computer security, including security of hardware, software and employee identity management. One of the best ways to protect your data and your accounts is to install anti-virus software, set up daily updates, and schedule virus scans at least weekly.

This document is designed to provide informative material and is distributed with the understanding that it does not constitute legal or other professional advice. We suggest that you consult with your systems administrator, IT consultant, technical advisor or attorney with regard to your business' particular situation. Opinions expressed herein are subject to change without notice. Information has been obtained from sources believed to be reliable, but its accuracy and interpretation are not guaranteed.

Salisbury Bank and Trust Company

5 Bissell Street
Post Office Box 1868

Lakeville, Connecticut
06039-1868

t: 860.435.9801
t: 800.222.9801

www.salisburybank.com

© Salisbury Bank and Trust Company Member FDIC