Security under threat

How to protect your online banking transactions from cybertheft

KRISTA DOBRONOS
Senior Vice President, Market Leader, Akron
Westfield Bank

(330) 668-6420
kristadobronos@westfieldgrp.com

WEBSITE: To learn more about Westfield Bank, visit www.westfield-bank.com.

INTERVIEWED BY ADAM BURROUGHS

Identity theft, viruses, malware, phishing and hacking can strike anyone, or any company, at any time. Downloading financial records using an unprotected system, for instance, can open the door to a man-in-the-middle attack in which a thief intercepts the signal between a device and a server. Other times, an individual can unknowingly login through a false portal at a hotel or coffee shop and have their bank account information, or their business's bank account information stolen.

"Many of the main threats against companies are direct hacking attacks," says Krista Dobronos, senior vice president, Market Leader, Akron, Westfield Bank. "But many more passive attacks are introduced in a company's systems through human error. In some cases, just opening an email could trigger a virus, especially if it has an attachment that's downloaded."

Smart Business spoke with Dobronos to learn more about how businesses can safely conduct their banking online.

How are banks protecting information exchanged through online banking systems?

Many, if not all, banking relationships include an online component that allows customers to complete transactions through a secure Web portal. The convenience of account balance review, electronic bill pay, remote check deposit and direct deposit must be balanced with security to ensure company and customer information is protected.

Information transferred through online banking is typically supported by the highest level of encryption, creating a secure environment for transfers between a browser and the online banking application. Banks continuously monitor these activities and layers of security are in place to make it more difficult for hackers to get customer information.

What internal controls should companies have in place to prevent cybertheft?

First and foremost, perform an evaluation on your existing internal controls and conduct periodic risk assessments to identify gaps and continuous improvement opportunities. It's also important to establish internal information security policies, such as acceptable uses of your information systems.

There are many ways to take steps internally to safeguard company information, a few of which are:

- Dedicate and restrict one computer to online banking transactions. Allow no Internet browsing or email exchange, ensure this computer has the latest security patches, and create unique and separate user IDs for every employee accessing the system.
- Segregate responsibilities among employees by maintenance, entry and approval.
- Assign dual system administrators for online cash management services.
- Establish transaction limits for employees who initiate and approve online payments.
- Create an escalated authorization process for high transaction limits.
- Monitor account activity and review all transactions on a daily basis.
- Never bank online using computers at kiosks, cafes, unsecured computers, or unsecured wireless networks.

Who should establish these protocols and who should enforce them?

It's a company's responsibility to protect its customers' data and information. For some companies, the law defines to what extent that must be done.

All companies are at risk for a security breach and should have internal controls to reduce their exposure. Companies with limited resources may want to engage with a consulting firm or an outsource partner to protect sensitive information.

If a company suspects it is the victim of a cybertheft, what should it do?

Immediately contact your financial institution regarding your suspicions. Exercise internal incident response procedures if they exist. If not, then see what options are available to you through your bank or insurance provider. You may also need to seek out a third-party that specializes in cybertheft mitigation.

Ultimately, it's getting to be good business practice to secure customer data. It may seem like an overhead expense, but it ensures the integrity of customer relationships, which is important because a breach of information is also a breach of trust. ●