Hacked! Business bank accounts vulnerable to cybercriminals

March 3 2016, by Joyce M. Rosenberg

In this Wednesday, March 2, 2016, photo, Sandy Marsico, owner of Sandstorm Design, poses for a portrait at her Chicago-based marketing company. Small businesses like Marsico's, who had company bank accounts broken into twice by cybercriminals, are vulnerable to having money stolen by criminals who use technology to hack into their bank accounts. (AP Photo/Charles Rex Arbogast)

It's a chilling moment when a small business owner discovers hackers

have stolen thousands of dollars from the company checking account.

Cybercriminals took an average $32,000 from small business accounts, according to a December survey of owners by the advocacy group National Small Business Association. And businesses don't have the same legal protection from bank account fraud consumers have.

The Electronic Funds Transfer Act, passed in 1978, states that it's intended to protect individual consumers from bank account theft, but makes no mention of businesses. Whether a business is protected depends on the agreement it signs with a bank, says Doug Johnson, a senior vice president with the American Bankers Association, an industry group. If the business hasn't complied with any security measures required by the agreement, it could be liable for the stolen money, he says.

Any business is vulnerable, but small companies are less likely to have security departments and procedures to guard against online theft than big corporations do. They also don't have big revenue streams that are better able to absorb losses from a theft. And even if they get the money back, they still have to spend time and money dealing with the hassles of closing accounts and opening new ones.

In this Wednesday, March 2, 2016, photo, Sandy Marsico, owner of Sandstorm Design, poses for a portrait at her Chicago based office. Small businesses like Marsico's, who had company bank accounts broken into twice by cybercriminals, are vulnerable to having money stolen by criminals who use technology to hack into their accounts. (AP Photo/Charles Rex Arbogast)

Sandy Marsico's company accounts were attacked—twice. Her bank contacted her in December 2014, saying a transfer of over $50,000 to Mexico had been requested from her checking account. The thieves had obtained the account information; Marsico, owner of Sandstorm Design, a Chicago-based marketing company, still doesn't know how. The bank did an investigation but didn't share its findings with her.

Marsico didn't approve the transfer, the account was closed and a new one opened. But the following November, someone began withdrawing

money from the new account in increments ranging from $1,000 to $4,000, a total of $20,000 in the course of a month. Marsico didn't discover it until she got her monthly statement.

"My stomach dropped when I wasn't able to identify these as our charges," Marsico says.

The bank, which again did an investigation but didn't tell Marsico the results, again reimbursed Sandstorm. Marsico has since moved some of her accounts to another bank.

HOW IT HAPPENS

Cybercriminals are creative, changing methods as companies and banks find ways to prevent attacks.

Thieves are increasingly using realistic-looking emails to trick companies into transferring money from their accounts with what's known as wire transfers, says Avivah Litan, a security analyst with the research company Gartner. Often, an employee receives an email purportedly from a company executive asking them to transfer the money from the company's account into a specific external account. If employees don't check to be sure the request is legitimate, they might go ahead and authorize a withdrawal.

The first attack on Marsico's account was a wire transfer attempt but didn't use an email to her company.

In this Wednesday, March 2, 2016, photo, Sandy Marsico, owner of Sandstorm Design, poses for a portrait at her Chicago based office. Small businesses like Marsico's, who had company bank accounts broken into twice by cybercriminals, are vulnerable to having money stolen by criminals who use technology to hack into their accounts. (AP Photo/Charles Rex Arbogast)

The FBI reported last August that more than 7,000 U.S. companies of all sizes had been victimized in emailed attacks since late 2013, with losses of more than $740 million. The government said the number of identified victims had surged 270 percent between January and August

of last year. Most of the thieves are believed to be in organized crime groups in Eastern Europe, the Middle East and Africa, the FBI said.

Criminals can also operate by planting malicious software known as malware on a company computer, often via an email that has a link or attachment. If the computer is used to log into a bank account, the malware can record the login and password and send it back to the criminals, who then withdraw funds. But many banks have procedures designed to protect against stolen logins. If bank computers don't recognize a device trying to log in, the bank will send a one-time access code to the account holder on a separate device like a phone. Without that code, a fraudster can't log in.

Using a computer or smartphone in a public place that has a Wi-Fi environment can also be risky, says Kevin Watson, CEO of Netsurion, a Houston-based company that provides cybersecurity for small businesses. Some Wi-Fi spots may have weak security, and savvy hackers know how to steal information that someone keys into their device.

And some thieves do it the old-fashioned way, simply by copying account numbers and routing information from checks and then printing phony checks and depositing them. One thief made two withdrawals from the checking account at Mark Waring Ventures two months ago, one for $800 and another for $1,000.

"Someone can just look at a check and they're a good part of the way to hacking into your account," says Dave Waring, managing partner of the New York-based company that provides financial and other services to small businesses.

The bank reimbursed Waring, the account was closed and he now makes payments electronically.

At Neil Palache's company, the culprit used a counterfeit debit card. Two thefts totaling $1,400 happened while Palache was online, looking at his account, and the card was immediately canceled. The bank refunded his money and Palache got a new card.

"I was thinking, 'they're going to wipe me out of this keeps going,'" says Palache, owner of The Wealth Creator Co. for Women, a Westlake Village, California, company that teaches women how to manage their money.

WHAT CAN YOU DO?

Business accounts are safer at banks that use what's known as two-factor authentication, requiring unfamiliar account users or devices to supply additional information like one-time access codes, says Timothy Ryan, a managing director with the security company Kroll in New York. Sophisticated banks also have software that flags emails or attempted logins from unfamiliar Internet service providers, he says.

Additional steps owners can take:

—Everyone in the company must be hypervigilant about emails, being wary about clicking on links and attachments and checking the addresses that emails came from. Criminals may create email addresses that look familiar but that might have an extra letter like an "I" or "i" not apparent at first glance.

—In the case of wire transfers, put procedures in place so several managers must sign off before a transfer can made.

—Keep a close eye on accounts. If you can't check your balance daily, get text alerts whenever there's a withdrawal.

— Don't log into your bank from an airport, hotel lobby, coffee shop or other public space that offers free Wi-Fi. Resist the temptation to log in until you're home or in your office.

"It's a simple protection for a complex problem, but it takes discipline and that's where people fall down," says Watson, the Netsurion CEO.