

Playing It Safe

Protecting your business from cybercrime and scams.

BY SHARI HELD

Target. Home Depot. UPS. JP Morgan Chase. They've all made the headlines lately—and not in a good way. They've been hacked! And confidential information was compromised.

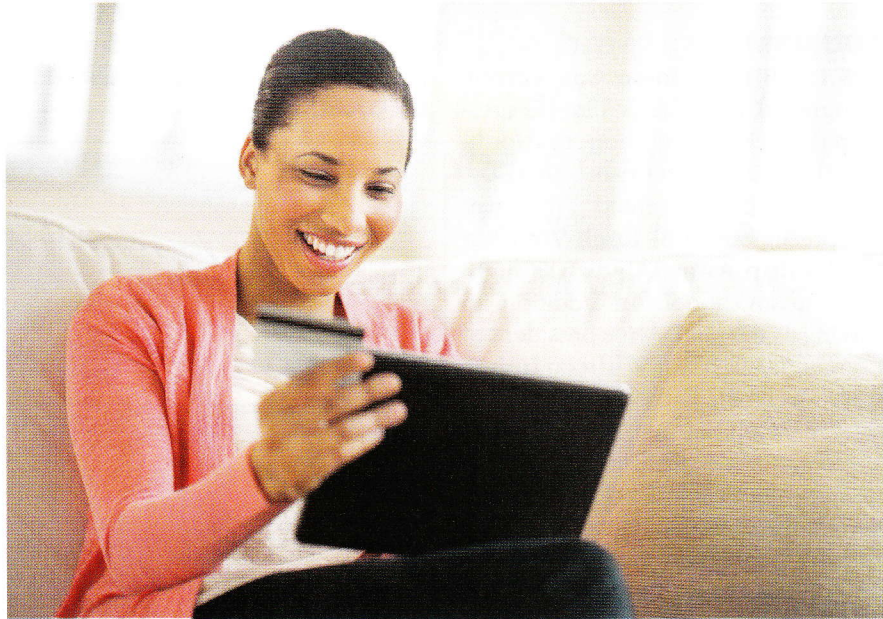
“The threat is very real, and pretty much a weekly occurrence,” says Tanya Buerger, senior vice president and chief information and technology officer for Peoples Bank in Munster. “It’s the new reality we’re forced to deal with.”

And it’s one that has many small business owners wondering how safe their information and money really are.

“Small business owners think, if Target, JP Morgan Chase, Goodwill and Home Depot can get compromised, what if they come after me?” says Andrea Smiddy-Schlagel, vice president and cash management services manager for 1st Source Bank in South Bend. “I don’t have the IT staff those big companies have. They want to know where’s the next threat going to come from. If we all had a crystal ball, we’d all know. But we don’t.”

Cybercriminals have many avenues for attack—viruses, retail or credit card fraud, account takeover and social engineering such as phishing emails (those emails that often look like they come from your bank or other official institution) are but a few. The one thing they all have in common: The bad guys gain access to your sensitive information so they can make off with your money! (See onguardonline.gov for a comprehensive list of scams and Internet fraud.)

“These are truly sophisticated people,” Buerger says. “There’s a lot of money to be made, so they are going to be creative. You can’t protect yourself 100 percent, but there are things you can do to help lessen the risk.”



RIGOROUS CONTROLS Cybercriminals have many avenues for attack, and banks are fighting back.

THE LAYERED APPROACH

Financial institutions began putting more rigorous controls in place several years ago when a rash of bank account takeovers took place, with business accounts as the primary target.

“If the bank has the proper controls in place, essentially it’s made it tougher for business accounts to be compromised,” says Clyde Hague, CISM, CISSP, information security office and assistant vice president for First Merchants Bank.

One such control is out-of-band authentication. In addition to supplying an ID and password when conducting a business transaction, business clients must enter a special code that is sent over another “band,” such as a cell phone, before the transaction is approved. It works because the hacker won’t have that last piece of information needed to finalize the transaction.

Financial institutions may also issue tokens, a hardware device that

can be carried on a keychain, to business customers. The password on the device changes frequently to make hacking more difficult.

“If customers are doing riskier transactions such as a wire transfer or ACH transaction, they’ll have an added layer of protection with a token,” says Bob Buhle, senior partner, Centier Bank, a family-owned bank serving Northwest Indiana.

Behavioral analytics is instrumental in helping banks better protect customers by understanding how they use their accounts. When does a customer typically do their banking? What are their normal deposit and withdrawal amounts? To whom do they normally transfer money?

“All those things over time create a unique fingerprint or profile for each of our clients that the system constantly evaluates against the activity that is occurring in real time,” says Chris Hart, operational risk director at First Financial Bank Cincinnati headquarters. Deviations from the histori-

cal behavioral pattern raise a flag that may stop the transaction until it can be identified as being legitimate.

Many financial institutions require customers to register their computers so their systems will recognize them. Accessing your online banking account from a different machine raises the risk level.

“Once a customer’s risk score reaches a particular level, we will ask them to authenticate through some challenge questions,” Hart says. “That gives us the confidence you are who you say you are.”

Hart encourages customers to take advantage of alerting capabilities, especially when it comes to online banking. Customers can receive a variety of alerts ranging from anytime someone successfully logs into the account, to anytime there’s a transaction out of the account, or anytime there’s a bad password entered to the account.

“We highly recommend that our clients go through those alert mes-

sages and select the ones that make the most sense for them,” he says.

Dual controls, especially when it comes to payment origination, provide yet another layer of safety for business customers. Smiddy-Schlagel often convinces customers, who wouldn’t implement dual controls on their own, to hunker down and do it. “It’s not necessarily easy, Smiddy-Schlagel says. “But we try to make it more difficult for customers to be compromised.”

This checks and balances system typically requires two people to originate payments. But if the bookkeeper is the only person in a small business that performs payroll, the bookkeeper will establish the payroll information (employees’ account numbers, etc.) and then the bank will lock the information down. The bookkeeper can originate payroll to employee accounts, but is not authorized to change account numbers or add additional employees without

going outside the system to do so. In the event the payroll computer is compromised, hackers won’t be able to create bogus accounts or add additional employees.

KEEPING A STEP AHEAD OF RETAIL FRAUD

The banking industry is a highly regulated industry that has many controls in place to keep customer accounts secure. But the retail industry isn’t as highly regulated. The PCI Security Standards Council, founded in 2006, issues guidelines for Payment Card Industry compliance in an effort to protect customers, which is a good starting point, but today it still isn’t a robust system.

“It’s just a snapshot at one point in time,” Hague says, “not a continual assessment. And it doesn’t guarantee that a company that was PCI-compliant three months ago is secure now.”

Meanwhile, credit card fraud is running rampant. One tool financial



EXTRA PROTECTION Centier Bank can give business customers a “token” that provides changing passwords to foil hackers.

institutions use to protect customers from breaches and credit card fraud is a monitoring service. These services access reports on breaches from MasterCard and other organizations to identify cards that may have been compromised.

“Sometimes we’re able to get a step ahead of things,” Buhle says. “With the Target breach we were literally

able to identify all our cardholders who used their cards at Target during the time of the compromise. And we began reissuing those cards the evening the breach was announced on the news.”

PARTNERING TO COMBAT CYBERCRIME

Banks provide education on how

business customers can protect themselves from breaches of confidential information in the form of fact sheets, email alerts, and even actual face-to-face training. But banks can only do so much. Businesses have to do their part as well.

“What we’re seeing in the industry is a partnership of the banks and their customers working together to battle the bad guys,” Hague says. “And that’s the way it should be.”

Businesses need to implement protective measures—firewalls, anti-virus and spyware detection, timely installation of software and hardware patches and other system measures—but one of the most important and effective measures they can take is to educate employees about the risks, how to recognize them and what to do if they suspect a computer or information has been compromised.

“People are historically the first line of defense,” Buerger says. “The more knowledgeable they are, the less likely something is going to happen.

Training can be very helpful in combating phishing emails asking recipients to enter sensitive data, open an attachment or click on an embedded link.

“Just delete them,” Hague says, “or call the person or business back and see if it’s real. You can have all the controls in place but human beings are your weakest link.”

Another way cybercriminals gain control of a computer is through contaminated Internet links on trending topics accessed through Google or other search engines. Click on a contaminated link, and your computer is compromised by malware or a virus. If your computer is networked, it’s possible the other computers in your business are as well. The best policy is to only visit websites you are familiar with or know that they are legitimate.

“Many people don’t take the time to look at the URL before they click on a link,” Hart says. “And we know the bad guys are taking advantage of that.”

Essentially it comes down to the basics: Use complex passwords. Use

Community businesses need a community bank.

**Are your revenues in excess of \$100 million a year? No?
Then why use a bank that caters to those businesses?**

Make a decision to bank with a financial institution that’s as down-to-earth as you are. Work with a bank that specializes in community-based business relationships. Partner with someone who actually wants your business. We’re standing by to help you with all your business borrowing needs like:

Refinance your existing commercial real estate

Traditional operating Lines of Credit

Construction financing for commercial building

Equipment loans – to modernize your operation

Asset-based financing alternative to factoring

**Call our Lending Center at
(219) 365-6700 to set up a
meeting with a business specialist.**

Ask about special incentives for businesses owned by women, minorities and veterans!



A REAL COMMUNITY BANK... Not just a branch in your community.

www.amsavings.com MUNSTER HAMMOND DYER SCHERERVILLE

8230 Hohman Ave. 4521 Hohman Ave. 1001 Main Street 7880 Wicker Ave.
219.836.5870 219.931.1015 219.322.5005 219.365.6700

MEMBER FDIC ©2014 MIDS amb40614

unique passwords for online banking. Change all passwords routinely. Download information from only trusted websites. Don't immediately react to threatening emails—we're going to shut down your account if you don't provide this information—or other requests that require your information or interaction.

And when installing wifi, be sure to change the default passwords. Smiddy-Schlagel has heard too many stories about businesses that ran all their systems off wifi without changing the default password.

"You're basically opening all the doors and windows and letting everyone come in," she says.

USING ALL THE TOOLS IN YOUR TOOLBOX

Some businesses may try to protect themselves by not doing their banking online. But waiting for statements to be mailed to them on a monthly basis isn't such a good idea.

"Small business owners think, if Target, JP Morgan Chase, Goodwill and Home Depot can get compromised, what if they come after me?"

—Andrea Smiddy-Schlagel, 1st Source Bank


"Online banking is a good option for staying on top of things," Buerger says. "You can look at your accounts periodically so you're aware of what's transpiring."

Caution and vigilance go hand-in-hand with enjoying the convenience the latest technology provides.

"We can't be afraid to use these wonderful electronic devices or tools that we have," Buhle says. "They're wonderful tools and they're a great way to improve efficiency and ease of doing business. We just have to have a heightened awareness of

what we can do to make our environment more secure. That's the direction we're all taking."

Cybercrime is an issue we'll have to live with, and the key for combating it is to be informed and prepared.

"We have to look to the future to determine what controls we'll need next," Hague says. "We can't sit still. We may not need them today, but we'll need to implement them tomorrow to protect our customers, because the bad guys are constantly trying to get around the controls we put in place." 



**A SMARTER SOLUTION.
WE MADE IT HAPPEN.**

Kevin Lhotak
PRESIDENT, RELIABLE TRANSPORTATION SPECIALISTS
CHESTERTON, INDIANA

My trucking company has seen a fair share of bank mergers. And I've been bogged down by busywork and disappointed by customer service afterward, too. Not only was my transition to First Merchants the smoothest I've ever had, but their expanded services can only help my business. My goal was a seamless transition to create new opportunities. First Merchants helped make it happen.

It's your goal. We make it happen.
At First Merchants, we see beyond the numbers by using powerful financial resources, prompt local decisions, and personal attention.

First Merchants Bank

See how our commercial banking solutions make it happen for you. firstmerchants.com

THE STRENGTH OF BIG THE SERVICE OF SMALL | firstmerchants.com | 800.205.3464

FDIC 