# Are You Secure?

Published October 1, 2011 | By Beau Denton



When hackers broke into Sony's PlayStation Network this past spring, they stole the personal information, including thousands of credit card numbers, of 77 million customers, a breach that cost the company a reported $171 million. But small businesses—not large corporations—are the most likely target of cybercrime in the commercial arena, says Dr. Cihan Cobanoglu, an expert in computer security and the dean of the School of Hotel and Restaurant Management at the University of South Florida Sarasota-Manatee.

From everywhere in the world, he says, computer hackers scan 24/7 for open doors in computer networks and can easily retrieve customers' private information, leaving businesses thousands to millions of dollars in damage. The hospitality industry is a frequent target. "Fortunately, there are some simple steps small business can take to protect themselves," says Cobanoglu, who recently served on President Obama's Secure Online Transactions Strategy Initiative.

Who are the hackers?

I put cyber criminals in three categories. The first is innocent—high school and even middle school students trying to break into websites just because they can. They don't steal or harm. The second are terrorists. They want to harm a particular country or business, but the purpose is not commercial; they'd like to manipulate transportation and military systems. The third type is the commercial hacker, and this is organized crime, done to make money. These people steal credit card information and private information. Their main target is the credit card numbers of consumers so they can be replicated and sold.

Is cybercrime increasing?

In the last decade, the intensity has increased significantly because everyone has Internet access now. Commercial hacking is the worst in terms of dollars and waste. Hackers sniff the cloud. Whenever they detect a 16-digit [credit card] code, they can grab it. The good news is that the ability to protect against the first and third types of cybercrime is not difficult.

Who is most likely to get hacked?

Organized hackers want to steal a bunch of credit cards at one time. More than half of all commercial hackings happen in small businesses, and 55 percent are in the hospitality industry—hotels, restaurants, travel agencies, casinos, theme parks.

What do hackers do with the credit cards?

Once the cards are stolen, they're replicated by a credit card encoder, a device you can buy online for about $900. The actual cards—the plastic magnetic stripe cards—are 5 cents to 10 cents. You buy empty cards, put them in the encoder machine and add the numbers—the expiration date, the CVC code, even the PIN number, which is stored in the magnetic stripe. Then [the criminals] start buying items and sell them on outlets like eBay for much less.

Given how sophisticated hackers are and how quickly new techniques develop, can you ever protect yourself against hacking?

If someone wants to hack you and is determined and persistent, he will do it. The FBI, the CIA, the White House have been hacked, and if they can be hacked, anybody can. But hackers must have a very good reason to get into a [business].

And what is that good reason?

We work with companies that do audits after a server has been breached. We find that the majority of servers breached don't comply with the most basic security guidelines. I use this analogy: When you go on vacation, you lock your doors, close the curtains, stop deliveries and leave the lights on. It's just common sense, right? Business leaves all the doors open and then tells everyone, "We're on vacation for 15 days. So, hey, enjoy yourself."

So what should businesses be doing to protect themselves?

If a business accepts credit cards or holds private, confidential information, they need to be PCI DSS—Payment Card Industry Data Security Standards (pcisecuritystandards.org)—compliant. It is a not-for-profit organization and a great resource for small business because it outlines what you have to do to be secure. It's created by the major credit card companies. The PCI Council teaches businesses 12 basics so they are not vulnerable. It's a requirement to be compliant if you accept credit cards.

What are some of the standards?

First, use updated antivirus software and make sure it updates once a day. When we did research, only 70 percent of small businesses use this in the hospitality industry. Second, install a firewall to block traffic from the outside. We use a honey pot in our research. That means you install a new server into your organization, attach it to your network, but purposefully put nothing into the server. Then don't protect it. Within one minute you will get the first attack. Three, encrypt sensitive data like credit card numbers and Social Security numbers.

What happens if a business is hacked and credit card numbers are stolen? Is the business financially responsible?

The consequences are very severe now. If you are breached and not PCI compliant, you can be denied [the privilege of accepting] credit cards. There's also a hefty fine that comes from the credit card companies. Merchants also have to pay for all the theft. If somebody bought $2,000 in merchandise, the merchant is responsible for that. Merchants are also responsible for changing all the credit card numbers that have been stolen, which can be $50 per consumer. T.J. Maxx was breached a couple of years ago. Forty million credit cards were stolen. It cost T.J. Maxx millions.

Is identity theft different?

The motives are different. Instead of targeting businesses, now I'm targeting you. I want to be you. I want to apply for a

credit card, steal your identity. In commercial hacking, once credit cards are stolen, these people will not use them long-term because the minute that they buy a $2,000-$3,000 computer you will detect and close your account and the credit card companies are alerted to find out which cards were stolen.

What should consumers do?

Check your statements at least once a month. Hackers check to see if a person checks their balance. They'll charge a very small amount—say $2—because if you don't detect, they will start using your card for larger amounts, and it can affect your credit.

Your advice to business?

Don't take the chance that you're a needle in the haystack and no one will find you.

Special event
Biz(941) and USF's Institute for Public Policy and Leadership are presenting "Cybercrime 101: How Businesses Can Protect Against Hacking." The event is free and open to the public. RSVP to http://sarasota.usf.edu/ippl, or contact Holly Lundgren at hlundgre@sar.usf.edu or (941) 359-4774.

Poll

**Are you in favor of the Florida Water and Land Conservation Initiative on the November ballot to acquire and restore Florida conservation and recreation lands?**

- Yes
- No

Vote

View Results Polldaddy.com

Search Local Businesses

Search

Popular Searches

Powered by Local.com

Categories

— any —

Tags

— any —

Submit Reset