You're an easy target, and that's why criminals like you

By Bob Russo, general manager, PCI Security Standards Council

Harold Hacker is scanning the Internet. No, he's not surfing to his favorite news and game sites. He's looking for systems that belong to restaurant and hotel chains. When he finds one, he'll enter the private section.

Passwords won't stop Harold, because in addition to knowing all the obvious ones, he also has a small program that hurls common logins and passwords at unsuspecting sites. He's aware that the most common password used in business today is Password1.

Fran Franchisee has invested her entire life's savings, her children's college fund, plus all the money and goodwill from every blood and marriage relative within miles to get her business up and running. She simply isn't thinking about resetting the password on the payment hardware she received from head office.

Harold doesn't consider himself a thief. He sees himself as an opportunist... the online version of someone who wanders around your neighborhood at 4am checking to see if your house, garage, and car doors are locked. If they're not, whatever is inside now belongs to him.

Fancying himself as particularly entrepreneurial, after he has his way with a franchisee site he'll advertise his findings for sale on websites frequented by criminal hackers. Soon thousands around the world will know how unsecure that network, especially its payment system hardware, is.

Fran is the opposite of a computer geek. In addition to being a manager, sometimes she's also a cook, a server, and cleaner. She's too busy serving customers and dealing with the everyday trials and tribulations of a franchisee... Friday her best server called in sick, Saturday her dishwasher didn't show up, and Sunday the vegetable delivery van broke down, leaving her to explain to every customer why there was no salad.

Fran is the first to admit she doesn't know much about computers. And she knows even less about securing them. Unfortunately Harold, his criminal colleagues, and everybody in the computer security industry know it too.

Franchise outlets like hotels and restaurant chains are a favorite place for cybercriminals to attack. To understand why, put yourself at Harold's keyboard and mouse for a moment.

You can search for individual computers to infect, wait for the owner to log into an online banking site, and steal one password at a time.

Or you can log into the bank and steal them all. Except banks can afford to buy expensive security software, along with the high salaried professionals to manage them.

So what's next? Well, you want credit card info. Where else is it used?
Ah ha, the hospitality industry. Indeed.

The very nature of repeatable systems is what makes franchises successful. So when a security hole exists within a specific system, it's duplicated among the entire franchise base.

In 2011 Cyber criminals took full advantage of this vulnerability, targeting specific franchised businesses and exploiting common points of failure across franchisee properties.[1]

Both the Trustwave Global Security Report and Verizon Data Breach Investigation Report indicated that for the second year in a row, the food and beverage industry had the highest percentage of breach investigations, at almost 44 percent and 54 percent, respectively.

While Harold Hacker isn't aware of the details, he knows Fran Franchisee is too busy to change the password on that payment processing hardware. So while she thinks she's locked the door on her equipment, by maintaining the original factory-inserted password Fran has done the equivalent of leaving spare keys under the doormat, above the doorframe, and in the mailbox.

Sadly, Fran is unaware that the knowledge for stopping these attacks already exists.

The Verizon report demonstrated that 96 percent of cyber victims subject to Payment Card Industry Data Security Standard (PCI DSS) had not yet reached compliance. Had existing simple or intermediate controls been in place, 97 percent of those breaches could not have occurred.

Consider for starters, two of many choices – Point-to-Point encryption (PTP) and EMV, both of which minimize payment card fraud. No, Fran doesn't *need* these technologies, however they make it harder for attackers to steal her and her customers' data.

She can also take courses like the PCI Security Standards Council Internal Security Assessor program to help her business achieve compliance faster. It's the same training Council Assessors receive – that course and several more are available online.

[1] Trustwave 2012 Global Security Report

If Fran truly sought to help, she'd join the Council as a Participating Organization. The benefits are numerous, including access to expert peers in her industry, and the chance to attend PCI Community Meetings.

At Community Meetings thousands of IT security professionals gather to assist business owners like Fran, with the latest methods of protecting businesses and customers from credit card fraud. She'd get even more out of the great networking opportunity by telling her stories and sharing experiences.

This year Community Meetings are in Orlando, FL on September 12-14, and Dublin, Ireland, October 22-24.

In addition to learning the latest fraud prevention techniques and meeting all kinds of people who can help her, traveling to one of the meetings is generally considered a business expense. So Fran can ask her accounting professional how much of it she can write off.

Join us, and together we'll reduce credit card fraud in the hospitality industry.