

## ★ INTERNET SECURITY

# Hacking and identity theft—the lowdown

Q&A with Ryan Penn, president of **ituitive Business Technologies**



### What types of threats do cyber criminals use on businesses and everyday computer users?

Very high threats, especially to SMEs and home-based businesses. Most large businesses understand these threats and have spent time and effort to protect the business and maintain back ups. Many small businesses that have a Web commerce site have a double threat—to their online commerce and to their office systems. This has become a significant problem of late, as so many businesses are on permanent high-speed connections and have poor or no firewall or security protection.

### Who are targets for hack attacks?

Anyone really. Hacks can range from Trojans or Zombies that do not affect day-to-day functionality, all the way to data theft, and systems and network shutdown.

### Have you seen more of these issues in 2005 than in 2004?

More and more clients are becoming concerned. Each week there are reports of hacks, theft, Trojans, etc. A lot of this can come from countries where there is no real enforcement.

### What is the most common kind of hack attack?

Trojans or Zombies. They lie dormant waiting from commands from their master to attack a given site or IP address. Doctors, Lawyers, Accountants, and other professionals that hold personal and private information, need to be especially vigilant. They can be held liable and accountable if they do not take the necessary steps to guard and back up their data.

### What kind of damage is being done to businesses as well as personal computers?

Trading accounts, trade secrets, erasing debt, blackmail, you name it. If someone can get in and use your computer to their advantage, it will be done and it's getting worse.

### How many hackers can attack a network at one time?

One to over 50,000. With Web-based extortion, you could get hit with denial of service by tens of thousands of Zombies.

### What is the cost to businesses?

It's the cost of being down, the cost of being sued, the cost of losing business, not getting your e-mail, losing customers and patients if they find out you have been compromised.

### Where do you see these cyber crimes going if they are not stopped?

Well, a smart kid in Russia brought down websites doing millions of dollars in business. Some pay, some do not. If a doctor is compromised, will he tell the authorities? Most likely not—it could cost him his practice.

### What can be done to stop these cyber criminals from hacking into personal and confidential information?

The best practices in system and network hardening to prevent hackers are: logging traffic, closing ports, restricting VPN, creating internal policies for people. Most hackers use “social engineering” to gain simple access. Doing a full security audit from both an external and internal perspective will greatly reduce the risk. This would include an application audit if the company is running a Web-based business. Although we are talking about the *external* hacker, most damage and security breaches are caused by *internal* sources like employees, contractors, and suppliers.

### How can they fix these attacks?

One way is by performing a comprehensive penetration attack (with permission) and providing the customer with a full report and recommendation. Many times, we actually break in and leave a file behind to show the clients their vulnerabilities.

### What is the most serious hack attack that your company helped to fix?

We have had clients that have had attempts made against them to gain access; most of our clients were set up by us. Of course, if someone really wants to get you—and they have enough motivation and money—they might. The key is to lock the doors with good locks and check on them all the time.

### Are companies such as ituitive able to work with clients anywhere in Canada?

Anywhere in the world—the Internet is everywhere and so are hackers. **E**

*Ryan brings over 14 years experience to Internet service, application and marketing initiatives, overall technology strategy, end user usability studies, Internet filtering applications, new service/product development and privacy issues. Contact info: Ituitive Business Technologies, e-mail: rpenn@ituitive.com*