

How to protect yourself from the hackers

NAOMI CARNIOL
Special To The Star

With computer fraud becoming a growing concern in Canada, online investors can never be too careful. Individual investors who don't protect their computer systems risk losing thousands of dollars, experts say.

In the past six months, at least 14 online accounts of Canadian individual investors have been broken into, says Alex Popovic, vice-president of enforcement for the Investment Dealers Association of Canada. Hackers use a variety of techniques to obtain online passwords. With that information in hand, the goal is simple get cash out of the online investing account.

But it's not as easy as draining a bank account once you've got a PIN, or personal identification number, Popovic says.

"You can't buy anything else other than securities using that account."

Hackers tend to use two strategies to make money. They'll sell the account's valuable stocks and then make the account buy penny stocks at two or three or 100 times what the hackers paid.

Or they'll create a public company and sell its shares to several online investors' accounts. Then the thieves walk away from the company and let it fail.

"It's something we've seen in the past," Popovic says.

As hackers grow more sophisticated and find more ways to invade PCs, online investors need a multi-layered approach to ensure that private information stays private, says Amit Sahni, vice-president of technical services at Markham's Evron Computer Systems Corp.

With that in mind, here are some tips for securing your computer.

- Don't choose an easy password. That means don't use your birthday, street address, child's name or spouse's name. Use a password that has some numbers, some letters and a few special characters.
- Install a firewall. That will prevent others from getting into your computer, and keep the firewall up-to-date. "Most legitimate firewall software is updated on a continuing basis" when you buy a one- or two-year subscription, Popovic says.
- Download patches. Whether you use Microsoft Windows XP or another operating system, the manufacturer sometimes finds trouble spots that are vulnerable to hackers. The company will release patches so clients can protect the weak spots, Sahni says.

If you don't keep the patches up-to-date, it might just be a matter of time before a hacker gains access to your computer.

- Install anti-virus and anti-spyware software, and keep it up-to-date. Most attacks used to be launched by viruses. In the past two years, however, spyware has become much more common, Sahni says.

Either way, you need protection from keystroke software. This software can arrive in either a virus or spyware format. The program records every keystroke you type on your computer and sends that information back to the hacker.

"We know of one situation where an online account was broken into" because of a keystroke virus, Popovic says. The investor's anti-virus software wasn't up-to-date. The hacker broke into the investor's online accounts at two brokerage firms and caused the investor to lose tens of thousands of dollars.

- Avoid opening emails or downloading files from unknown sources.

"A lot of the malware, the dangerous software, will sometimes be contained in an email. ... It's hidden away inside of whatever it is that's being emailed to your computer, and then it installs itself once you open the link or receive the email," Popovic says.

- Be very suspicious of emails asking for personal information. One Canadian investor received an email from what appeared to be the person's discount brokerage firm. The email asked the investor to click on a link, which brought the investor to what seemed to be the discount brokerage firm's website. The investor was asked to log on.

The website was a fake, Popovic says. By logging on, the investor gave away personal information. Most banks and online investing agencies say they would never request confidential information via an email, Sahni says. If you get an email like that, chances are it's a scam.

- Set up different user accounts. If you are using the family computer for online investing, consider whether everyone using that computer will take the necessary security precautions. If not, set up various user accounts with different levels of access to the computer. For example, a child's user account might limit the websites the child can visit.

Security doesn't end at the computer. You still have work to do after you've installed anti-virus software, anti-spyware software, patches and different user accounts.

- Confirm, confirm, confirm.

Check the trade confirmation tickets you receive after each trade to verify you were the one who placed the order. Also, check your online trading account weekly to ensure you authorized all the trades, Popovic says.

Read the fine print.

Some of the Canadian investors whose accounts were hacked this year were compensated for the money they lost. But that depended on the contract between the investor and their discount brokerage firm, Popovic says.

Check to see if your contract specifies that the firm will compensate you in the event of fraud by a third party.

TheStar.com [Corrections](#) | [Contact Webmaster](#) | [RSS](#) | [Star P.M.](#) | [FAQ](#)

Toronto Star [About Us](#) | [Classroom Connection](#) | [Brand New Planet](#) | [Subscriber Services](#) | [Contact Us](#) | [News Releases](#) | [Star Internships](#)

Advertise With Us [Media Kit](#) | [Online Advertising](#) | [Print Advertising](#) | [Special Sections](#)