

Computer scam goes viral in Canada

September 29, 2011 - OTTAWA - The Royal Canadian Mounted Police (RCMP) and their partners at the Canadian Anti Fraud Center (CAFC) are warning that if someone calls you claiming to be able to protect your computer from viruses, your best bet is to just hang up the phone. Don't give the caller your computer access codes and don't provide your credit card information.

The virus scam has grown to epidemic proportions in Canada, now accounting for between 70 and 80 per cent of frauds reported daily to the CAFC. "We began noticing virus scam calls in March 2010. Since then, they've become an increasing proportion of our calls. Now, they're the scam we deal with most often," said RCMP Staff Sgt. Paul Proulx of the CAFC.

This dramatic increase means the scam is working – more and more Canadians are being targeted by the virus scam. Staff Sgt. Proulx warns, "If a scammer is able to log on to your computer then he has access to all the personal information you have stored there, including your banking information."

Here's a typical scenario: a caller, often claiming to work for Microsoft or another reputable software company, will cold-call you and ask if your computer is running slowly or not working as it should. He will then offer to repair your computer via internet access, which can involve either software installation or the caller gaining remote control of your computer after you've granted him access. Payment for the software or the repair service is handled via your credit card with charges typically ranging from \$35 to \$470 per call.

Allowing a third party to download software or remotely access your computer carries a number of serious risks. Malicious software can be installed to capture sensitive data such as your online banking user names and passwords, bank account information and your personal identity information. All of this information can be used in subsequent frauds that empty your bank accounts and charge your credit cards. Your computer can also be converted to a bot-net, which means criminals can use it without your knowledge or participation. It can then be used to spam other people, spread viruses to your friends or overload computer networks. Getting your credit card information is the second important part of the virus scam. Once a criminal has that information it can be used to make purchases without your consent.

Canadians should be aware that not all virus scams are conducted over the phone. Many CAFC callers report being scammed after responding to internet pop-up ads for anti-virus software.

Staff Sgt. Proulx offers this simple advice: "If you're really worried about viruses on your computer, be pro-active and use anti-virus software that you've acquired from reputable sources and keep it up to date. If someone calls you out of the blue offering to provide this kind of help, it's probably a scam. Remember, it's not rude to hang up on someone who's trying to steal your money and information."

"When it comes to cyber security, we all have a role to play," said Public Safety Minister Vic Toews. "Canada's Cyber Security Strategy is the Government's plan to help secure Canada's vital

cyber systems and help Canadians protect themselves, their families and their personal information online."

Please visit the Canadian Anti Fraud Centre's new website for the latest on emerging fraud trends, advice on protecting yourself and victim's guides that will help you recover from fraud loss: www.antifraudcentre.ca. For more information on the Government of Canada's Cyber Security Strategy: www.publicsafety.gc.ca/cyber

Fraud: Recognize It, Report It, Stop It.

- 30 -

For more information:

Canadian Anti Fraud Centre
1-888-495-8501

Royal Canadian Mounted Police
Media Relations
(613) 843-5999