

FOR IMMEDIATE RELEASE

## Internet banking virus threatens bank accounts – consumers need to fortify home computer security

*Burnaby, February 14, 2008* The British Columbia Crime Prevention Association is issuing an urgent warning to those who do online banking to make sure that they have implemented security measures to protect them from the SilentBanker Trojan virus.

Following on the heels of warnings from computer security experts that 2008 would see the emergence of more sophisticated computer viruses, along comes a Trojan virus labeled *SilentBanker*.

SilentBanker is aptly named because this virus embeds itself on home computers after users have visited random websites and it has the ability to redirect money from customer's accounts during a normal Internet banking session – all without any outward signs that a virus is at work. And most worrisome of all is that the usual indicators of a secure website; the locked padlock symbol and the letter "s" in a website address (https :), no longer guarantee that a website is secure.

Those who are at most risk are customers who have no anti-virus and anti-spyware software installed or who have allowed their subscription to lapse.

Jeff Burton, Manager of Programs and Projects for the BC Crime Prevention Association, points out that this is not a bank software issue but the responsibility of individual users. "Conducting internet banking sessions without anti-virus protection is analogous to leaving your back door unlocked when you have an alarm system installed."

The BC Crime Prevention Association recommends the following preventive measures to enable safe online banking:

- Ensure anti-virus and anti-spyware software programs are installed and able to detect and isolate threats
- Configure Windows updates to be installed automatically
- Check for the latest patches and service packs
- Make sure your firewall is on
- Read the advice on bank websites for recommendations re minimum computer security standards
- Don't do online banking from a public computer (Internet café, library, etc), worksite or your friend's computer

- Check your bank accounts and statements regularly online

Internet banking issues apart, the BC Crime Prevention Association encourages computer users to develop a Fort Knox approach to computer interaction – create an electronic “moat” around your computer to keep intruders at bay.

To learn more crime prevention tips, visit [www.bccpa.org](http://www.bccpa.org).

-30 –

*This news release is one of a series in which the BCCPA offers advice under its Crime Shield banner to give the public the tools they need through education and awareness to protect themselves against crime.*

*Our new Ask an Expert column is an additional resource for crime prevention information pertinent to British Columbia. The column can be viewed at [www.bccpa.org](http://www.bccpa.org). Topics will be frequently updated and refreshed depending upon response.*

Media Contacts:

Valerie MacLean  
Executive Director  
BC Crime Prevention Association  
604-291-9959, Ext.226  
[v.maclean@bccpa.org](mailto:v.maclean@bccpa.org)

Jeff Burton  
Manager Programs &Projects  
BC Crime Prevention Association  
604-291-9959, Ext.234  
[j.burton@bccpa.org](mailto:j.burton@bccpa.org)