



# E-Telligence

Issue 1, June 27, 2008

## 2008 Events

**Sept. 8-9, 2008**  
**1st Annual Cyber Security Conference**  
 Calgary, Alberta, Canada  
[Click here](#)

**Sept. 15-18, 2008**  
**ASIS International 54th Annual Seminar and Exhibits**  
 Atlanta, Georgia, USA  
[Click here](#)

**Sept. 29-30, 2008**  
**Cybera's Annual Cyberinfrastructure Summit**  
 Banff, Alberta, Canada  
[Click here](#)



## HEADLINE NEWS

### GCSC Launches Official Website



This week the Global Centre for Securing Cyberspace launched a completely re-designed official website filled with interesting reports, cyber crime tips, event listings and numerous resources to help raise awareness.

Tell your colleagues and please visit the site today! [www.gcsc.ca](http://www.gcsc.ca)

# Welcome to E-Telligence

Twice a month, to keep you informed, we'll be profiling cyber crime news and events.

## High Tech Crime Becoming #1 Crime in North America

by Nancy Argyle



Calgary — Cyber crime is now the most significant challenge facing law enforcement organizations in Canada. The results of a nationwide Deloitte survey, commissioned by the Canadian Association of Police Boards (CAPB) to determine the magnitude and impact of cyber crime on Canadians, has indicated that cyber crime is a much more serious threat than previously believed. CAPB considers the results of this survey to represent a “call to action.”

“We knew that many law enforcement agencies were seeing impacts but, without good numbers, it was hard to get a true sense of how significant the threat was,” says Ian Wilms, chair of the Canadian Association of Police Boards. “We now know, thanks to our survey and the efforts of other organizations, that cyber crime is surpassing drug trafficking and is very close to becoming the #1 crime in the nation.”

“As a result, the average citizen is now more likely to be a victim of crime through the Internet than on the street or in their home,” says Wilms. “Even if they don’t own a computer, their information may be on someone else’s computer or with a business that uses the Internet which can put them at risk.”

“And, just like drug trafficking, cyber crime has a very real impact on victims...unfortunately, it is an invisible threat to many Canadians,” he adds.

Combining the results of the CAPB Cyber Crime in Canada survey with other studies, Wilms says agencies are now realizing that the crime forecast looks grim. With a huge upswing in malicious cyber attacks reported, Wilms says the “landscape of law enforcement has changed dramatically.”

“Right now, the criminals have all the advantages and we are struggling to keep up and every day we fall further behind,” he says. “The pool of victims grows larger every day while the pool of perpetrators also gets larger, younger and more sophisticated...this is a new era for police, fighting a new type of criminal.”

With little funding and already-overworked officers, the fight against cyber crime “has to be shared,” says Wilms. “This is now a global, societal problem that will require a coordinated, intelligent and powerful response.”

“Technology crime units can no longer be viewed as ‘nice to have’ within our police services,” he says. Instead, Wilms says these units must become an integral, key component of any police service strategy including supplying the appropriate resources for computer forensics, cyber crime investigations and cyber crime prevention.”

One of the key recommendations from the CAPB survey is the establishment of a dedicated Canadian centre where law enforcement and various agencies can work together to combat cyber crime.

“Canada has many leading experts...ultimately, this is an opportunity for our country to assume a leadership role by helping to become peacekeepers of the Internet,” Wilms says.

Funded by Public Safety Canada, the Government of Alberta Solicitor General and Public Security and the City of Calgary, the survey consisted of three components; an Ipsos Reid market research survey of 587 Canadians, an extensive interview process with 63 key contacts from law enforcement, prosecutions, government, academia and industry and an analysis of open source survey data.

### Key findings of the report:

- 49% of respondents have been a victim of cyber crime (cyber crimes include computer viruses, banking and personal information being lost or stolen through the Internet, children being bullied or sexually abused through online contact, businesses being hacked and held for ransom, identity theft and interference with critical infrastructure such as power grids, water systems or telephone services).
- 70% of victims of cyber crime have not reported the crime as they were unsure who to report to or did not think any justice would occur.
- 86% of respondents indicate that cyber crime has become a concern.
- 95% of respondents believe they are being targeted for cyber crime (most respondents believe the greatest threats are identity theft, financial fraud and computer viruses).
- 89% of respondents believe that preventing cyber crime should be a priority of government and law enforcement agencies.

### Additional supporting statistics:

- According to a 2007 Symantec study, Canada ranks ninth as a country targeted for malicious cyber activities while the U.S. holds the #1 position. This same study discovered more than 700,000 new malicious code threats for 2007, up from only 125,000 in 2006.
- A 2006 estimate by the Canadian Council of Better Business Bureaus indicates that identity theft is costing consumers, banks, credit card firms and stores \$2 billion annually.
- According to the U.S. Dept. of Justice statistics, identity theft is passing drug trafficking as the number one crime in the nation — approx. one new victim every two seconds.
- Internet child pornography has become a \$2.6 billion industry (NCMEC). The latest RCMP estimates indicate there are 60,000 identified IP addresses in Canada accessing child pornography.
- In a recent IBM survey of healthcare, financial, retail and manufacturing industries, nearly 60% of businesses believe that cyber crime is more costly to them than physical crime.
- In 2006, FBI statistics showed a loss of \$70 million in bank robberies compared to \$220 million lost in due to Rock phishing. Currently the most popular phishing kit, Rock phish allows non-technical individuals to create and carry out phishing attacks.
- 2007 research from the U.S. Cyber Consequences Unit shows that the destruction from a single wave of cyber attacks on critical infrastructures could exceed \$700 billion – the equivalent of 50 major hurricanes hitting U.S. soil at once.

## Websites you should visit...

- [www.calgarypolice.ca](http://www.calgarypolice.ca)
- [www.kinsa.net](http://www.kinsa.net)
- [www.phonebusters.com](http://www.phonebusters.com)
- [www.cmch.tv](http://www.cmch.tv)
- [www.cba.ca](http://www.cba.ca)
- [www.antiphishing.org](http://www.antiphishing.org)
- [www.cscic.state.ny.us](http://www.cscic.state.ny.us)



## You'll be interested in this...

**How to Safely Use Facebook and LinkedIn at Work, IT Business Cran** (06/23/08); Jackson, Brian

Some companies are using social networking sites Facebook and LinkedIn as a communications tool. However, information posted by employees could pose a security risk for companies. Some organizations ban the use of social networks in the workplace, but many use Facebook to organize group social events and attract interest in the company. A marketing expert advises companies concerned about their information to hire an outside service to search the Internet for confidential data. Users should also be selective about who they add to their LinkedIn network and who is able to see their Facebook profile. Spammers are using social networking sites, so employees should only add people they actually know. [\(go to web site\)](#)

**Digital Image Forensics Scientific American (06/08) Vol. 298, No. 6, P. 66; Farid, Hany**

The field of digital image forensics has grown around commercial software that allows photographs to be convincingly doctored, writes Dartmouth College professor Hany Farid, who, with his team, has developed a number of tools designed to identify signs of digital image manipulation by understanding what statistical or geometric characteristics of an image are disturbed by tampering. One common image manipulation strategy is the copying and pasting of a region of an image, a technique known as cloning. To spot cloning, Farid's team has developed a method that works with small blocks of pixels, using an algorithm to compute a quantity that represents the colors of the pixels in the block, which it then applies to order all the blocks in a sequence that has identical and very similar blocks in close proximity. The program then searches for identical blocks and tries to "grow" larger identical regions from them block by block. [\(go to web site\)](#)

**Beware, Your Computer May Betray You New Scientist (06/07/08) Vol. 198, No. 2659, P. 26 ; Barras, Colin**

Non-repudiation is a system whereby sensitive data sent over the Internet is digitally signed at the source with a signature that can be traced to the user's computer as a safeguard against fraud, but Len Sassaman of the Catholic University of Leuven warns that making this system the default setting for all traffic on a network would enable authorities to trace the source of any online activity and take away users' anonymity. Worse still, Sassaman and University of Ireland colleague Meredith Patterson say that the One Laptop per Child (OLPC) foundation is unintentionally engaged in establishing such a system throughout the Third World by supplying inexperienced users Internet-ready laptops. [\(go to web site\)](#)

## Tip of the Week

### Cell Phone Security

Cell phones are more vulnerable than regular phones due to two dangers: eavesdroppers can listen in on your calls and thieves can bill their own calls to your account.

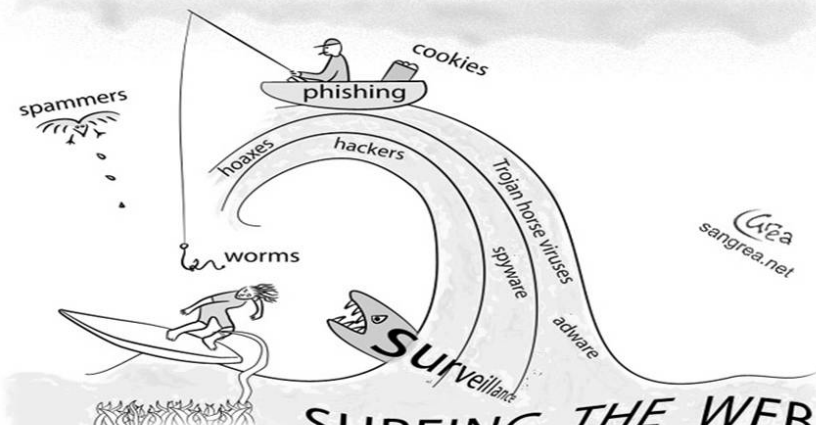
**Eavesdropping:** Anything you say on a cell phone can be easily overheard by someone using a scanner. The best protection? Be aware of what you discuss on your cell phone. Remember that it acts as a handheld broadcast station. Don't give out your credit card number or other sensitive or confidential information; don't say anything you wouldn't say on broadcast radio or TV.



**Fraudulent billing:** It is possible for thieves to intercept a cell phone signal and clone the phone's ID numbers (its electronic serial number and mobile identification number or ESN/MIN). The result is the equivalent of a stolen calling card. Some simple countermeasures include:

- **Limit roaming.** Cloners target airport parking lots, airport access roads and rural highways.
- **Turn the phone off when not in use.** Cell phones poll the cellular base station with the strongest signal every few seconds. However, this polling exposes the phone to interception and cloning.
- **Review all bills.** Report every erroneous call to the service provider. There are two types of cloning. Outright theft of the phone's ESN/MIN is most common. A bill will reflect hundreds, even thousands of bogus calls. The other type of cloning is called tumbling, where a cloned phone uses a different ESN/MIN for each call. A bill might have only one bogus call this month, none next month, but three calls the month after that. The phone has still been cloned and fraud is occurring.
- **Prefer hands-off vehicle-mounted phones to handhelds.** The boxes used to capture ESN/MIN have a limited range; cloners will follow an individual they know is using a phone.

— Cornell University advice to students and staff



The Global Centre for Securing Cyberspace will provide a collaborative environment which will directly impact present and future criminality on the Internet. It's a collaborative centre concept dedicated to preventing, reducing and eliminating the criminality advantage of cyberspace. Bookmark [www.gcsc.ca](http://www.gcsc.ca) today!

Please email us if you have questions, special events, story ideas or experiences you would like to share. We hope you enjoyed reading this webletter and we look forward to bringing you E-Telligence again soon. If you wish to unsubscribe, please contact: [kathy.macdonald@gcsc.ca](mailto:kathy.macdonald@gcsc.ca)