

2008/09 Calendar

November 15-21, 2008
2008 CSI Conference
 National Harbor, MD, USA
[Click here](#)

November 24-25, 2008
Privacy and Identity Theft Conference
 Vancouver, BC, Canada
[Click here](#)

December 1-2, 2008
11th International West Coast Security Forum
 Vancouver, BC, Canada
[Click here](#)

December 2-5
Kestenberg Siegal Lipkus 13th Anti-Counterfeiting Training Conference
 Toronto, ON, Canada
[Click here](#)

January 19-21, 2009
e-Forensics 2009
 Adelaide, Australia
[Click here](#)



HEADLINE NEWS — October 28, 2008

What's New on the Frontline!



Identity Theft Twice as Likely in Canada, the U.K. and the U.S.

According to a 2008 Ipsos survey, online consumers in Canada, the U.K. and the U.S. are the most frequent victims of identity theft — twice the rate of France, Germany and Spain, according to a new study released by PayPal.

Understandably, with the holiday season fast approaching, three quarters of online shoppers worldwide are concerned about online scams or identity theft.

The survey found that 10% of online shoppers in Canada, the U.S., and the U.K. had experienced identity theft, compared to about 5% in France, Germany and Spain.

Approximately 25% of online shoppers in the three English-speaking countries knew friends or family who had their identities stolen. In Canada, Ontario was hardest hit with 12% saying they have been victims of identity theft, followed by Alberta (9%), and Quebec and BC (8%). Less than 6% of Atlantic Canadians said they have been victims of identity theft.

“Concerns about identity theft form a universal language,” said Michael Barrett, chief information security officer at PayPal.

“The PayPal study sheds light on a few simple things that consumers can do to feel more confident in shopping online.” (See tips at bottom of newsletter.)

While there is a national discrepancy between those who have been victims of identity theft, or know someone who has, (49% of Americans have been victim or know someone who has, versus 13% of Germans), the level of concern for identity theft is high everywhere.

More than 85% of Canadian, American and British consumers are either slightly or very concerned. Even in Germany, where the percentage of victims is relatively small, 72% are slightly or very concerned.

“Canadians are aware of the issue of identity theft and are proactively doing things to reduce the odds of falling victim to it,” said Darrell MacMullin, country manager, PayPal Canada.

“One interesting bit of information that came out of this survey is that we are a nation of shredders! Sixty-seven per cent of us shred all financial statements, which is a simple, yet effective, way to help protect yourself.”

Welcome to E-Telligence

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

Child Pornography in the Workplace

By Jennifer Rees, Alberta Crown Prosecutor

Alberta is fortunate to have a dedicated ICE (Integrated Child Exploitation) unit that deals with the exploitation of children over the Internet.

On the police side, the unit has a north and south team and deals with all the cases in Alberta. They are available for consultation and will assist police detachments and the public if they have any questions about suspected child pornography or child exploitation over the Internet.

Alberta is doubly fortunate in that they have a group of dedicated prosecutors (five – soon to be six) that deal with Internet crime and have gained expertise in this area. The majority of the cases that we deal with are those that involve child exploitation and the majority of these cases deal with child pornography.

Child pornography can be photographs of teenagers where “the dominant characteristic is the depiction, for a sexual purpose, of a sexual organ or the anal region.” Unfortunately, in the vast majority of cases, the child pornography images are extremely graphic and involve babies and children being raped. Viewing these images, even momentarily, can have horrific affect on people. Now, technology makes it easier to get and store images and videos and build collections.

If child pornography is discovered in the workplace, it is best to contact the police, preferably someone from the ICE unit. Police departments can seize computers under 489 (2) of the *Criminal Code* without a warrant if they have evidence that it has been used in the commission of an offence. Usually, the officer will ask the complainant what they saw and why they believed it to be child pornography – so be prepared to describe what you saw.

It is also important to remember that, even if the child pornography is not downloaded and stored, people can be charged with accessing child pornography.

Whether or not police need a general warrant after seizing a computer depends largely on the workplace policy and on the reasonable expectation of privacy of the suspect. Different procedures and warranties can be used to obtain evidence from computer network systems in cases where a computer cannot simply be seized.

It is important to have a clear unambiguous acceptable computer use policy in the workplace. The policy should be comprehensive and banner warnings are usually the most effective.

Banner notices are written notices that greet users before they can access the computer system and set out privacy rights that they do or do not retain.

In some cases, the absence of banner notices has been held to support a claim of privacy rights. There is a need for consistency between departments in an organization or corporation and the use of banners in one area but not in another is significant.

An effective banner must warn authorized and unauthorized users about what is considered the proper use of the system and indicate that the system is being monitored to detect improper use and other illicit activity.



To be very clear, there should be an indication that there is no expectation of privacy while using this system.

With the onset of new technology, it is important that the banner should display regardless of access point. To be effective, the user should have to acknowledge compliance before gaining access.

If pre-login is not possible, then the warning should display immediately thereafter. If the system does not support banners and warnings, use printed ones. The printed notices should be clearly visible and new employees should be specifically made aware of the policies.

It is important to try to make the policy comprehensible, especially where criminal liability is implicated. Consult your legal department when creating these policies. Some considerations should be given to a general prohibition against hacking, use of another person's account, interception or collection of passwords, sending e-mail or posting a webpage with intent to harm a particular individual or promoting hatred towards a group, forging someone else's name to any communication or misusing trademarks, or forging an e-mail address including in the header.

It is also useful to prohibit the use of a corporate/government network for personal financial gain or partisan political purposes, sending bulk e-mail, installation/use of unlicensed software and counseling any offence using the computer system including virus writing. Practically, there should be a prohibition against use of computer resources for personal recreation.

We have had a number of recent cases where computer repair shops, pawn shops and businesses have contacted us in regard to finding child pornography on their computers. Recently, we had a case in Red Deer, Alberta, where a computer repair shop reported finding child pornography on a computer.

These cases usually lead to charges of possession of child pornography but, in this case, the police forensic examiner discovered that child pornography was being made and two different children were being sexually assaulted. An adult male and an adult female were charged and both plead guilty and were each sentenced to seven and a half years. If the repair shop had not reported their discovery and contacted the police, this crime would probably never have been discovered as the victims were too young to reveal abuse.

Jennifer Rees was involved in a precedence setting case in which an Alberta man was charged after amassing Alberta's biggest known child pornography collection of more than one million images and 7,000 videos. The accused explained he had a male modeling hobby.



Fifty Speakers at Privacy and Identity Theft Conference

The Freedom of Information and Privacy Association (FIPA) is presenting its 10th conference on privacy and related issues on November 24-25, 2008 at the Fairmont Hotel, Vancouver, BC.

This year's conference is focused on the relationship between privacy, trust and identity theft. The conference will feature leading experts from government, industry, academia and the non-profit sector who will address these topics.

With more than 50 leading experts in the areas of privacy and ID fraud, including the Privacy Commissioner of Canada, this *Privacy and Identity Theft* conference will be the most comprehensive ID conference ever held in Canada. For more information, please visit www.idconference2008.com

Websites you should visit...

<https://www.paypal.com/security>

<http://www.unspam.com>

DidYouKnow?

Internet users trust information posted online less now than eight years ago.

Source: USC Annenberg School Center for the Digital Future

PayPal Survey Methodology

The 2008 PayPal Trust and Safety Study was conducted by Ipsos Research from May 28 - June 3 in the United States, August 19 - 26, in Canada and August 15 - 25 in Europe. The e-mail survey reached 1,000 panelists in each of the six countries: the United States, Canada, France, Germany, Spain and the United Kingdom. All respondents had shopped online in the past 90 days. Quotas for age, gender and PayPal usage were set during the survey to ensure representative populations in each of the six countries.

Other Global Findings (see article at top of newsletter)

- The majority of French consumers surveyed never change their passwords or do so only when required.
- German consumers keep their passwords to themselves. Only about one in four (28%) has ever shared an account password with a family member or significant others. This compares with 60% of Americans, 56% of French and 48% of Canadian consumers who've shared passwords.
- Germans also experienced the fewest problems with identity theft — only 3% of German consumers have experienced identity theft, and fewer than one in 10 knows someone who has.
- Almost half of online consumers in all countries surveyed use important dates, family member names, nicknames or pet names as their online passwords. Nicknames (22%), pet names (21%) and birth or anniversary date (15%) are the top password choices in Canada
- Spanish consumers are relatively new to e-commerce and more than 80% of Spanish respondents said they are concerned that the purchased product will not be as pictured or expected, will be of poor quality or will not arrive at all.
- Privacy is the number one concern among Canadians, with more than half (53%) indicating that they are “very concerned” about protecting it.
- Consumers in Germany, the UK and Canada are least likely to store their passwords on their browsers (70%, 61% and 58%, respectively, never do so). About half of the consumers in the U.S., France and Spain store passwords on their browsers.
- More than half of all consumers receive financial statements in the mail. Only 17% of consumers in France and 23% of consumers in Spain own shredders, compared to a large majority in all other countries.

PayPal Online Safety Tips

1. **Use safer passwords:** Use a combination of upper and lowercase letters and numbers and change passwords every 30 days.
2. **Protect your computer:** Use anti-virus software as well as an updated Internet browser that blocks fraudulent web sites.
3. **Never click on links in emails:** Even if the email appears to be from your bank, the IRS, or popular links like PayPal, do not click on links to pages that ask you to share sensitive personal or financial information.
4. **Use safer payment methods:** Systems such as PayPal or a credit card have policies that provide recourse if something goes wrong.
5. **Use common sense:** If something seems too good to be true, it probably is.

Portions reprinted courtesy of Canadian e-commerce Safety Guide and PayPal.

You'll be interested in this...

Keyboard Sniffers to Steal Data BBC News (10/21/08)

Doctoral students Martin Vuagnoux and Cryptography Laboratory at the Swiss Ecole Polytechnique Federale de Lausanne (EPFL) were able to monitor what people type by analyzing the electromagnetic signals produced by every keystroke.

The EPFL students developed four attacks that will work on a variety of computer keyboards, leading them to declare that keyboards are not safe to transmit sensitive information.

Vuagnoux and Pasini tested 11 keyboards that connected to a computer through either a USB or PS/2 socket, though the attacks also work on keyboards embedded in laptops.

Each keyboard tested was vulnerable to at least one of the four attacks they developed, with one of the attacks being effective at a distance of 20 meters.

The students used a radio antenna to fully or partially recover keystrokes by detecting the electromagnetic radiation emitted when keys are pressed. ([go to web site](#))

Is Online Banking Completely Safe? WBZ TV (Boston) (10/13/08); Ebben, Paula

Around 63 million U.S. households currently conduct their banking over the Internet — even though it is not totally safe.

University of Michigan computer science professor Atul Prakash recently examined weaknesses in the web sites of over 200 banks and one designed that 75 percent of them had a minimum of one security flaw.

Prakash explains that for a web page to be totally secure, the letters https must be in the address bar.

The letter S is at the heart of security, and if a user can just see http without the S, there is no certainty that it is really coming from the user's bank.

Security expert Robert Siciliano notes that when a bank constructs a web site, it should make sure that all pages have email addresses and phone numbers that are also safe. ([go to web site](#))