

## 2008/09 Calendar

October 15-16, 2008  
**APWG Researchers Summit**  
 Atlanta, GA, USA  
[Click here](#)

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 10, 2008

### What's New on the Frontline!



### Most Teens Have Been Victimized By On-Line Bullies

Research indicates that as many as 75 per cent of teens have been bullied online but only one in 10 have reported the problem to parents or other adults, a new study shows. The study, published in the September issue of [The Journal of School Health](#), is the latest to sound the alarm about so-called cyber-bullying, which can occur on social networking sites and in e-mail and text messages. Sometimes cyber-bullying involves taunting or threatening e-mail or text messages, posting embarrassing pictures or personal attacks on teen networking sites like MySpace or Facebook.

"The Internet is not functioning as a separate environment but is connected with the social lives of kids in school," said lead study author Jaana Juvonen, a professor of psychology and chair of the developmental psychology program at the University of California, Los Angeles. "Bullying on the Internet looks similar to what kids do face-to-face in school."

The U.C.L.A. study surveyed 1,454 teens between the ages of 12 and 17, who were recruited through an unidentified teen web site from August through October 2005. Forty-one percent of the teenagers surveyed reported between one and three online bullying incidents over the course of a year, 13 percent reported four to six incidents and 19 percent reported seven or more incidents. Despite the prevalence of cyber-bullying, many teens don't realize how common it is and often believe it is only happening to them, Dr. Juvonen said.

"When kids start thinking, 'It's just happening to me,' they likely blame themselves, and once they do that, it increases their risk of depression," Dr. Juvonen said. "Kids don't know how common cyber-bullying is, even among their best friends. Cyber-bullying is not a plight of a few problematic children but a shared experience."

Teens in the survey said they didn't tell their parents about the problems for a variety of reasons. Half of the teens who were cyber-bullied said they just "need to learn to deal with it." Nearly one-third said they worried parents might restrict Internet access, a fear more commonly expressed among girls than boys. One-third of 12- to 14-year-olds said they didn't tell an adult about the bullying out of fear that they could get into trouble with their parents.

"Many parents do not understand how vital the Internet is to their social lives," Dr. Juvonen said. "Parents can take detrimental action with good intentions, such as trying to protect their children by not letting them use the Internet at all. That is not likely to help parent-teen relationships or the social lives of their children."

Although most people view cyber-bullying as anonymous, nearly three out of four of the bullied teens in the survey said they knew or were "pretty sure" they knew who was doing the bullying.

## Welcome to E-Telligence

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

### DIRTY WORK: Finding Pornography in the Workplace

By Richard DeBruyne, ISP, CISA, CISM and senior manager at Grant Thornton LLP, leading the Alberta IT Security and Computer Forensics Practice

Whether you are a computer technician, a computer investigator, a police officer, a computer forensics specialist, a security manager or a computer auditor, many of you have probably had the unpleasant duty to root through someone else's computer files. It is kind of like rooting through their laundry basket; sometimes you come across incredible designer fashions and, other times, you come across things that are better left untouched.

This article will provide some valuable tips on what you should know before you get started. It will also provide some good advice on what you should consider before you have the unfortunate experience of discovering illegal material — specifically child pornography.

Despite tough laws and the complete distain by organisations, it is surprising how many individuals still download and view pornography using their work computers. Despite strict policies and automated web blocking technologies, many individuals are continuously caught with inappropriate material on their systems. These individuals not only risk their livelihood and their reputation but, in some cases, face serious criminal charges depending on what they are viewing.

So what is inappropriate material? From a corporate perspective inappropriate sexual material is just about any text or image that is sexual in nature and might be considered offensive to another person. Cartoons, stories, jokes, and photographs of men or women, unclothed or involved in sexual activities, all have the potential to be labelled as pornography. Whether collected and stored on one's computer system or simply viewed on the screen, access to this pornography is most often a serious breach of corporate policy and can be cause for immediate dismissal.

Child pornography, on the other hand, is the darkest form of pornography and is the least tolerated by society, corporations, and the legal system. It also crosses the line from inappropriate to illegal. Often its existence is obvious but, sometimes, it is difficult to distinguish child pornography from other forms of inappropriate material. The Criminal Code of Canada provides the following definition:

PART V: SEXUAL OFFENCES, PUBLIC MORALS AND DISORDERLY CONDUCT Offences Tending to Corrupt Morals

Definition of "child pornography" 163.1

(1) In this section, "child pornography" means:  
 (a) a photographic, film, video or other visual representation, whether or not it was made by electronic or mechanical means,  
 (i) that shows a person who is or is depicted as being under the age of eighteen years and is engaged in or is depicted as engaged in explicit sexual activity, or  
 (ii) the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ or the anal region of a person under the age of eighteen years;

(b) any written material, visual representation or audio recording that advocates or counsels sexual activity with a person under the age of eighteen years that would be an offence under this Act;

(c) any written material whose dominant characteristic is the description, for a sexual purpose, of sexual activity with a person under the age of eighteen years that would be an offence under this Act; or

(d) any audio recording that has as its dominant characteristic the description, presentation or representation, for a sexual purpose, of sexual activity with a person under the age of eighteen years that would be an offence under this Act.

The possession and/or distribution of child pornography is illegal and carry very stiff penalties.

The first and most important thing to understand is that you, as a technician, an investigator, security manager, auditor or even a police officer, are not exempt from the laws governing the possession and distribution of child pornography.

If you pass it to anyone else in the course of your responsibilities, you could be charged with distribution. Sloppy handling or actions that might seem innocent enough could come back to haunt you and your company in a very serious way.

Draft a policy in advance on the actions you will take in the event you discover inappropriate material or child pornography. Inappropriate material should be reported internally for legal guidance and handling. In the event that you discover something that you think might be child pornography, stop what you are doing and report the discovery to the police immediately.

In the next edition of E-Telligence, Alberta Special Prosecutor Jennifer Rees will write about Alberta's Internet Child Exploitation (ICE) team, offering recent criminal cases and additional ideas for establishing a corporate policy.

Tips to create a corporate office policy for investigating computer incidents.

- Involve your legal department in the drafting of your corporate policy.
- Make sure everyone handling computers, where this material might be discovered, is trained on the policy and confirms their understanding of it.
- Do not pass the material to anyone else if you discover something suspicious. Do not print or make any copies of the suspected child pornography. Your policy should outline the exact steps to be taken in the event that inappropriate material or suspected child pornography is discovered. These steps should be confirmed by your legal counsel and carried out every single time.
- If you suspect that child pornography might be present on a computer, contact the police to allow them to intervene before you do anything. Do not under any circumstances start an investigation on your own if you suspect child pornography is present.
- If you discover suspected child pornography accidentally, as in the case of a computer technician doing repairs, unplug the computer from the electrical outlet to immediately cut power to the machine and report it as outlined above.
- If child pornography is discovered on a network server, hard shut down the server and call the police immediately according to your policy. Production services should be considered secondary in the event that child pornography is found. Let law enforcement take lead over any subsequent investigation and network activities.
- If you are working for a third party or an external customer, make sure they understand your policy before you accept their equipment. Under no circumstances can you give the equipment back to them, once you have discovered it contains child pornography.
- Wherever possible, make a forensically sound image of the computer system before you begin to look at it. Examining the original machine and its storage, from a running machine, can corrupt evidence. If you don't have this capability in-house, consider hiring a professional external firm to handle the forensic activities for your company.
- Always act. Never tamper with the evidence by deleting files or otherwise try to remove them from the system.
- Always record your activities in writing along the way. A detailed record of what you have done to the system and who you have talked to, at each step, could be invaluable once law enforcement gets involved. Be sure to involve your legal council in every step. The laws concerning child pornography are tricky and professional legal guidance is a must to protect you and your corporation.

### Websites you should visit...

[www.getsafeonline.org](http://www.getsafeonline.org)

[www.sans.org/resources](http://www.sans.org/resources)

[www.parentcentre.gov.uk/usingcomputersandtheinternet/](http://www.parentcentre.gov.uk/usingcomputersandtheinternet/)



### Take Care When You Meet Strangers Online

GetSafeOnline is a popular website sponsored by the British government, the Serious Organized Crime Agency (SOCA) and leading businesses. This site offers interesting and informative advice to help stay safe when on the Internet.

You shop online and bank online, so why not find love online? Online dating sites have soared in popularity, but are they safe to use? GetSafeOnline offers that interesting advice for those visiting matchmaking sites — a popular but sometimes risky online activity.

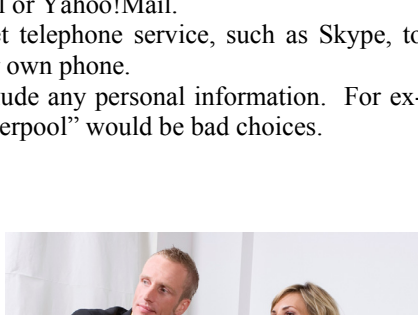
#### Protect Your Privacy

You are in control of what happens. Don't let anyone pressure you into giving away more information than you want to.

- You wouldn't give your phone number to every stranger on the street. Similarly, don't post personal information, such as phone numbers, in public places on the Internet.
- Wait until you feel comfortable with an individual, before telling them things like your phone number, place of work or address.
- A well-run dating site will offer the ability to email prospective dates using a service that conceals both parties' true email addresses. Use it.
- As a second line of defense for your privacy, set up a separate email account that doesn't use your real name. This is very simple and quick to do using such providers as Hotmail or Yahoo!Mail.
- Similarly, you can use an Internet telephone service, such as Skype, to call someone instead of using your own phone.
- Pick a user name that doesn't include any personal information. For example, "joe\_glasgow" or "jane\_liverpool" would be bad choices.

#### Meeting Someone

If someone you meet online is sincerely interested in you, they will want you to feel safe and they will be happy to let you apply a few common sense rules when you meet.



- Always meet in a populated public place. Stay in popular public places.
- Travel there on your own — don't accept a lift from your date.
- Do tell a friend or family member who you are meeting, where you are going and when you will be back.
- Stay sober.
- Take your mobile phone.
- Your personal belongings can be stolen. Your drink can be drugged. Don't leave them unattended.

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

**The Snake Within**  
**Governing (10/08) Vol. 22, No. 1, P. 60 ;**  
**Perlman, Ellen**

After studying 49 insider cyberattacks, Carnegie Mellon's Software Engineering Institute Computer Emergency Response Team (CERT) developed a model that could help IT managers in state and local governments to understand and mitigate the risk of such threats. CERT's study found that people who perpetrated cyberattacks on their own organization were database or system administrators who often did not get along well with others or were unable to take criticism.

The study found that these people were often provoked into launching an attack against their organization when they did not get a raise they felt they deserved or when they were punished in some other way. Once the employees have been provoked, they create "back door" accounts that only they can access. The employee can then use that account to plant a logic bomb or a time bomb that will wreak havoc on the organization's IT systems, days, weeks, or even months after they quit or have been fired.

CERT's Dawn Cappelli says employers can diminish the threat of such attacks by demoting or firing such employees when they begin to notice bad behavior. Unfortunately, many organizations leave themselves vulnerable to insider attacks by choosing to ignore such behavior, she says.

[\(go to web site\)](#)

**Majority of Employees Fear Identity Fraud**  
**Western Mail (Wales) (10/08/08)**

In Britain, 75 percent of workers think their business is not doing enough to combat identification fraud, according to new research. More than 50 percent believe classified documents could be taken from desks, while 72 percent think dishonest coworkers might share data with fraudsters. According to official statistics, ID theft costs the U.K. economy over 1 billion pounds annually. Consumers also have their doubts, with 97 percent saying they do not think the organizations they deal with take proper action to safeguard information.

"Businesses should be aware of the myriad of different ways in which their corporate identity can be used and abused, from theft of internet domain names to phishing or spam emails that pose as a legitimate business and damage their reputation," said Mike Cherry, home affairs chairman at the Federation of Small Businesses.

"We urge businesses to think foremost about prevention, and training for staff who handle sensitive business information and that of their customers and clients." [\(go to web site\)](#)