



GCSC

Issue 9, November 13, 2008

# E-Telligence

HEADLINE NEWS — November 13, 2008

## What's New on the Frontline!



### Justin's Story Captivates Calgary Students

*By Kathy Macdonald, VP, Communications, GCSC*

Recently, 1600 Calgary junior high school students sat captivated, quietly listening to an unbelievable story read aloud by Justin Berry, a 22-year-old man who has experienced unimaginable highs and lows in his short life. Justin's story has been well documented on the Internet. In fact, like the *Truman Show*, he has literally grown up in front of the camera. Justin has appeared on the *Oprah Winfrey* show and *Larry King Live*. Even today, blogs on the Internet express controversial opinions about his life. Countless images of Justin, in various stages of undress, are also archived on the Internet. On this day, 1600 young kids heard firsthand how it all began.

As Justin explains it, at the age of 13, he was an honour student who loved to play soccer. His life drastically changed when he received a free web camera in the mail. Justin's entrepreneurial spirit, combined with an immature, impressionable mind and grooming techniques used by pedophiles and predators, resulted in a sordid story of a million dollar business, a cocaine habit and the sexual exploitation and molestation of Justin between the ages of 13 to 18.

Justin said he felt like he was the one in control as he calculated the prices of his photos and managed the expanding list of 1500 subscribers who were accessing the online child pornography business he was operating. Raking in heaps of money and gifts including computers, high resolution digital cameras and airline tickets to luxury destinations, Justin felt like he was on top of the world.

The student audience heard about the grooming techniques used by an ever-growing number of predators subscribing to Justin's for-pay pornography website service. Techniques included monetary and status grooming, psychological manipulation, aggressiveness, romance and every other conniving tactic employed by online predators. They enticed Justin to expose himself in front of the camera and eventually meet them in the real world.

In 2005, Justin's life radically changed after he told his story to Kurt Eichenwald, a reporter from the New York Times. Eichenwald inspired Justin to speak to law enforcement which resulted in criminal charges being substantiated against a number of individuals. Justin now stands in front of huge audiences, like the one in Calgary, to quietly read about his life and tell about the sad loss of his childhood and his current efforts to help support tougher legislation against child pornography.

As a result of the presentation, about 40 students asked Justin some very tough, personal questions — questions that parents and security professionals might think kids would never dare ask adults about or even talk to their friends about. But, despite being part of such a large audience, after listening to Justin, these kids appeared encouraged to speak from behind the wall of secrecy and anonymity they often feel when at the keyboard.

Justin is now posing in front of a camera for other reasons. He operates [www.justinberry.tv](http://www.justinberry.tv) and offers Internet safety advice to kids, teens and parents. His slogan reads "education is crucial to protecting your kids from online predators."

### 2008/09 Calendar

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, 2008  
**Kestenberg Siegal Lipkus 13th Anti-Counterfeiting Training Conference**  
Toronto, ON, Canada  
[Click here](#)

January 6-8, 2009  
**International Conference on Cyber Security**  
New York, NY, USA  
[Click here](#)

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

March 30-April 2, 2009  
**USAIEEE Computational Intelligence Society Conference**  
Nashville, Tennessee, USA  
[Click here](#)

April 13-16, 2009  
**Cyber Physical Systems Week**  
San Francisco, CA, USA  
[Click here](#)

April 20-24, 2009  
**18th Annual International World Wide Web Conference**  
Madrid, Spain  
[Click here](#)

May 12-14, 2009  
**APWG Spring Counter-Crime Operations Summit**  
Barcelona, Spain  
[Click here](#)



## Welcome to E-Telligence

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

### CIOs Versus Cyber Crooks: How to Combat the New Generation of 'Most Wanted'

*By Ross Allen, Canadian General Manager, McAfee, Inc.*

As an effective CIO, you've developed a balanced IT skill set; strategic vision, devotion to best practices, people skills, technical knowledge, an ability to further your enterprise's objectives and the ability to create a learning organization that adapts proactively rather than reactively.

In addition to the day-to-day demands of the job, CIOs also live a uniquely precarious existence — just Google 'CIO survival guide' if you need further evidence of that. If anything even remotely connected to the IT department and employee use of enterprise networks goes wrong, the blame will end up at your desk.

CIOs also carry the responsibility of managing the enterprise's internal IT strategy and operations but, also, of anticipating and preparing for a wide range of external disruptive changes. In order to survive and thrive, CIOs need to stay several steps ahead of the curve.

One of the most challenging IT trends in the early 21<sup>st</sup> century is the rise of cyber crime as a rapidly proliferating, highly profitable global business sector targeting the legitimate enterprise. In some ways, cyber criminals try to function as a malevolent mirror to your IT department.

- They are learning organizations, always refining cyber crime best practices to achieve the fraud and theft business model which provides maximum ROI, at minimum risk.
- They constantly re-invent and improve their methods for establishing predatory relationships of trust with your enterprise's unwary employees, suppliers, partners and customers.

- They are always attempting to put themselves in your shoes, to better understand and exploit the weaknesses in your overall enterprise security strategy.
- Like any would-be world class IT department, cyber crime groups constantly acquire expert computer science talent. But, just as critically, they concentrate on developing 'social engineering' capabilities: understanding how the people in your enterprise (starting with you) think and work, so that they can 'turn' one or more people inside the enterprise into unwitting assistants to fraud and theft.

#### The Weakest Link

Using a range of automated tools and customized email and telephone contacts, cyber criminals scope out the architecture of your network, your security processes and components and the level of security awareness and training of your network users.

Once they have a clear picture of your firewalls, network architecture, installed software and email and voice phone procedures, they start looking for weak spots.

The main target, aside from gaping holes in your network security system, is careless, trusting, poorly trained or motivated *authorized users* of your enterprise network.

One increasingly popular tactic, once a human weak point is identified, is 'spear phishing' which involves the criminal following up an unwary employee's response to an automated email or a phone call with a customized email or phone call, purporting to come from a trusted source.

When the employee responds, the cyber criminal may direct the employee to a fake website or email address which looks like a genuine one, and dupe the employee into giving confidential information (such as passwords, account information, email addresses and personal information) that enables a fraud to be committed.

Expanding CIO Stewardship, Horizontally and Vertically

The effective response to the 'bad business model' of the cyber criminal is to incorporate an understanding of cyber crime IT strategy and social engineering tactics into the enterprise's overall best practices, risk management, security strategy and IT strategy.

If CIOs exercise their imaginations and empathy, to put themselves into the shoes of both the hapless employee at his or her desk, and the cyber crook trying to social-engineer a penetration through the corporate security system, then the necessary strategy becomes apparent.

As CIO, to manage cyber criminal attempts to socially engineer relationships with your enterprise, you need to construct a proactive security strategy.

- Integrate anti-cyber crime best practices with the overall enterprise security plan as well as within the IT strategy.
- Develop and communicate manager and employee responsibility for best security practices.
- Include anti-cyber crime education as a part of the HR department's interviewing, hiring and ongoing education programs.
- Include regular participation in cyber crime conferences and updating as part of your own professional development and that of key IT managers and technicians.
- Develop procedures for recording forensic evidence of cyber crime activities, both for IT system improvement and for investigation and prosecution of perpetrators.
- Ensure that the entire enterprise management team, not just the executive that the CIO directly reports to, is kept updated on known cyber crime activities against the enterprise, outcomes of those activities as well as current and anticipated threats and trends in cyber crime.

The well-tempered CIO can, with professional care and education, reduce the threat of cyber crime from an unpredictable potential catastrophe to a chronic but manageable responsibility that is part of doing business in the global economy.

#### Websites you should visit...

- **Password Management** <http://www.boonbox.net/>
- **TruthOrFiction.com** <http://www.truthorfiction.com/>
- **Symantec Security Response Hoaxes** <http://www.symantec.com/avcenter/hoax.html>
- **McAfee Security Virus Hoaxes** <http://vil.mcafee.com/hoax.asp>
- **Urban Legends and Folklore** <http://urbanlegends.about.com/>
- **Urban Legends Reference Pages** <http://www.snopes.com/>

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

##### Obama Urged to Take Immediate Cyber Security Steps

**eWeek (11/06/08); Mark, Roy**

The Defense Science Board, a federal advisory committee that provides independent advice to the Secretary of Defense, is urging president-elect Barack Obama to take steps to improve cyber security after he is inaugurated in January. In a report entitled 'Defense Imperatives for the New Administration,' the board outlines several ways that the incoming administration could accomplish this goal. For instance, the board recommends that the Obama administration accelerate efforts to use automated tools and algorithms to detect suspicious activity, increase the frequency of upgrades to hardware and software elements of critical systems, and create a way to reconstitute the network using an independent communication path that is not associated with the compromised network.

In addition, the report calls on Obama to make immediate improvements to space situational awareness. The report notes that this is important because understanding what the threats to the nation's space assets are, where they are, and what they may or may not do underlies all other defensive actions that can be taken. For his part, Obama has promised to make cyber security a top priority by declaring the nation's cyber infrastructure a strategic asset and appointing a national cyber-adviser who will report directly to him.

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

##### ITU Launches Child Online Protection Initiative

**IDG News Service (11/13/2008)****Olusegun Abolaji Ogundeji**

The International Telecommunication Union (ITU), in collaboration with several U.N. agencies, launched an initiative to safeguard children, the Internet's most vulnerable users. Called Child Online Protection (COP), the initiative will bring together partners from all sectors of the international community with the aim of creating a safe and secure online experience for children everywhere.

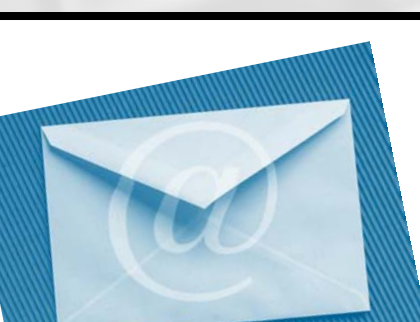
"We have to protect against cyber threats, especially when they target children," U.N. Secretary-General Ban Ki-moon said in his video address to the 2008 ITU Council High-Level Segment on Wednesday. "I welcome the ITU's Child Online Protection initiative and urge all states to support it." [\(go to web site\)](#)

##### Cyber Thieves Mine for Corporate Data Nuggets

**USA Today (11/12/08); Acohido, Byron**

The past year has seen an increase in cyber theft, with more and more criminals targeting corporations whose employees use free web tools, such as AOL instant messaging, Gmail and MySpace. Some of the desired information includes e-mail address books, PowerPoint presentations, engineering drawings and bid proposals. Most companies do not recognize the need to limit the use of free online programs or to address the security issues they present.

Security firm Finjan said that data thieves in the past nine months now harvest large amounts of data without a specific buyer in mind, searching through it later to find information valuable enough to sell. According to Gunter Ollmann, chief security strategist at IBM ISS, stolen data is sometimes used to access deeper levels of information, such as company databases. In 2000, stolen information from Super Vision Lighting was purchased by Chinese entrepreneur, Manson Wu, and used to imitate the company's manufacturing facility. Last month, data thieves found a security flaw in Windows XP and Windows Server PCs that allowed them to copy all personal data stored on the PC's web browser and registry.

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

## Cyber Tips

### Chain Letters

The National Cyber Alert System offers the following information regarding chain letters. For more information, please visit [www.http://www.us-cert.gov](http://www.us-cert.gov)

#### Why are chain letters a problem?

The most serious problem is that chain letters mask viruses or other malicious activity. Even the ones that seem harmless may have negative repercussions if you forward them. These consequences include:

- they consume bandwidth or space within the recipient's inbox
- you force people you know to waste time sifting through the messages and possibly taking time to verify the information
- you spread hype and, often, unnecessary fear and paranoia

#### What are some types of chain letters?

There are two main types of chain letters:

- **Hoaxes** — Hoaxes attempt to trick or defraud users. A hoax could be malicious, instructing users to delete a file necessary to the operating system by claiming it is a virus. It could also be a scam that convinces users to send money or personal information. Phishing attacks could fall into this category.
- **Urban Legends** — Urban legends are designed to be redistributed and usually warn users of a threat or claim to be notifying them of important or urgent information. Another common form are emails that promise users monetary rewards for forwarding the message or suggest that they are signing something that will be submitted to a particular group. Urban legends usually have no negative effect aside from wasted bandwidth and time.

#### How can you tell if the email is a hoax or urban legend?

Some messages are more suspicious than others but be especially cautious if the message has any of the characteristics listed below. These characteristics are just guidelines — not every hoax or urban legend has these attributes and some legitimate messages may have some of these characteristics:

- it suggests tragic consequences for not performing some action
- it promises money or gift certificates for performing some action
- it offers instructions or attachments claiming to protect you from a virus that is undetected by anti-virus software
- it claims it's not a hoax
- there are multiple spelling or grammatical errors or the logic is contradictory
- there is a statement urging you to forward the message

it has already been forwarded multiple times (evident from the trail of email headers in the body of the message)

- it suggests tragic consequences for not performing some action
- it promises money or gift certificates for performing some action
- it offers instructions or attachments claiming to protect you from a virus that is undetected by anti-virus software
- it claims it's not a hoax
- there are multiple spelling or grammatical errors or the logic is contradictory
- there is a statement urging you to forward the message

it has already been forwarded multiple times (evident from the trail of email headers in the body of the message)

- it suggests tragic consequences for not performing some action
- it promises money or gift certificates for performing some action
- it offers instructions or attachments claiming to protect you from a virus that is undetected by anti-virus software
- it claims it's not a hoax
- there are multiple spelling or grammatical errors or the logic is contradictory
- there is a statement urging you to forward the message

it has already been forwarded multiple times (evident from the trail of email headers in the body of the message)

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

Please email us if you have questions, special events, story ideas or experiences you would like to share. We hope you've 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)