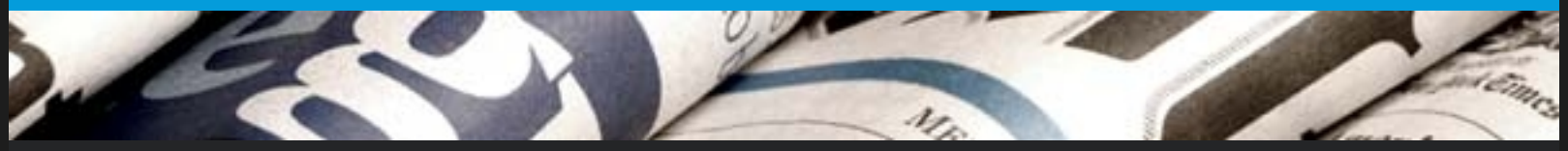
News, Resources and Useful Information for the Online Investigative and OSINT Professional from Toddington International Inc.



Toddington International Inc.

Online Research and Intelligence Newsletter

OCTOBER 2017 EDITION

In This Edition

Welcome to the Newsletter

Welcome to the October 2017 edition of TII's Online Intelligence Newsletter. August and September were incredibly busy months for us, with our team delivering a host of fresh, new, and updated training programs throughout Europe, Asia, Australia, and of course, North America. Earlier in September, we formally launched our much-anticipated, brand new online course, "Open Source Intelligence for Financial Investigators", in partnership with finINTEL's Robert Maxwell.

To start off this month, we want to take the opportunity to formally welcome our newest team members, Kathy Macdonald, Dr. Cynthia Baxter, and Colin Crowden. We are also proud to announce our newly appointed Vice President, Jasmeen Sandhar-Gill, who has served as TII's International Training Manager and GM for 5 years.

To keep things exciting, soon we are rolling out a completely overhauled version of our online course, "Using the Internet as an Investigative Research Tool", and will be announcing the launch date in our upcoming newsletter.

TII is pleased to offer a number of specialized and customizable in-house training programs for both the public and private sector in a variety of formats. To learn more about what we can do to empower your workforce, contact us.

E-Learning Graduates

Congratulations to the following students who are among those who successfully completed the 40-hour ***Using the Internet as an Investigative Research Tool™*** e-learning program with TII recently:

- Swetha Balla – Credit Suisse
- Claire Worsley – National Trading Standards
- Junior Williams
- Danielle Orr
- Simon Moy – Chevron
- Garry McBride
- Caitlin Robinson
- K. Morren – Trinidad and Tobago
- S. Springer – Trinidad and Tobago
- N. Baldeosingh – Trinidad and Tobago
- C. Ramlogan – Trinidad and Tobago
- Paul Mazziotta – Nemesis Intelligence
- Shamim Rafique
- Loretta Schroh

Upcoming Select Worldwide Training Dates

"Advanced Internet Intelligence & Online Investigations" – Abu Dhabi, UAE

5-Day Course

November 5–9, 2017, Abu Dhabi, UAE

Webpage coming soon. To register or to learn more, please contact us.

"Advanced Internet Intelligence & Online Investigations" – Dubai, UAE

3-Day Course

November 14–16, 2017, Dubai, UAE

Webpage coming soon. To register or to learn more, please contact us.

"Advanced Internet Intelligence & Online Investigations" – Toronto, ON

3-Day Course

November 20–22, 2017, Toronto, ON

"Advanced Internet Intelligence & Online Investigations" - Calgary, AB

3-Day Course

(Early-bird pricing available for a limited time only)

December 11-13, 2017, Calgary, AB

"Cyberpsychology & OSINT Training" - Vancouver, BC

2-Day Course

With Dr. Cynthia Baxter

January 29-30, 2018, Vancouver, BC

Webpage coming soon. To register or to learn more, please contact us.

"Cyberpsychology & OSINT Training" - Toronto, ON

2-Day Course

With Dr. Cynthia Baxter

February 26-27, 2018, Toronto, ON

Webpage coming soon. To register or to learn more, please contact us.

Please contact us directly for your in-house training requirements.

"Sexting" - So what's the big deal?

Having conducted countless online safety presentations over the years, few subjects trigger greater angst for parents than the topic of sexting. Picturing their child sharing nude or nearly nude images on the Internet sends most parents into a state of sheer panic or complete denial.

In Canada, research shows that sexting amongst young people is a frequent occurrence. According to a MediaSmarts study from 2014, eight per cent of students in grades 7-11 with cell phone access send sexts. This same study noted that by grade 11, that number increased to fifteen per cent and that twenty-four per cent of students in grades 7-11 with cell phone access had received a sext sent directly to them.

In Australia, the term 'image-based abuse' is used to describe the sharing of humiliating and sexually explicit material. Research findings recently released reveal that one in five Australians have experienced image-based abuse, which is up from one in ten only two years ago.

A Dutch campaign reported that only six per cent of Dutch boys and fourteen per cent of Dutch girls have had negative experiences with sexting. This campaign titled, ‘Hou het lekker voor jezelf’ (‘Keep it to yourself’), not only informs Dutch youngsters about the risks of sexting, but also gives them safer sexting tips. These tips include comments like: “don’t include your face, any recognizable tattoos, or birthmarks; only send nudes to people you already know and trust for a while off-line; and agree to delete nudes after seeing them.” This study went on to say, "aside from being part of a cluster of risky behaviours, however, there is little evidence that sending sexts is by itself a risky act."

So is the practice of sexting not that big of a deal anymore? Is sexting now being

accepted by the community as just a normal part of a child growing up in this new technological era?

As parents grapple with their kids sharing intimate images online and the police struggling to keep up with the rapidly growing increase in online child sexual exploitation, I believe we need to come together and strongly declare that the practice of sexting, no matter how it is done, is totally unsafe and completely dangerous. Once these images are shared over the Internet, whether the victim consents to it or not, there is going to be non-contact sexual abuse. Further, would it not make sense that if significant efforts were made to halt this insidious abusive activity, then at the very least the purveyors of child pornography would find less sexual content to trade, share, and view?

Most parents cannot believe their child would willingly take an intimate picture of themselves and then simply share it with someone on the Internet. However, this practice seems to be more palatable to parents if they believe that predators on the Internet apply expert grooming techniques to pressure and manipulate children into sharing nude or nearly nude images.

Online exploitation by child predators occurs frequently today and is extremely dangerous for all involved. Unfortunately, young people are unknowingly contributing a plethora of intimate images to these image banks when they believe they are in a relationship, or they are flirting or trying to get attention from someone they know, or have recently met online, by sharing nude or semi-nude pictures. We know these pictures are widely shared by recipients; is it now becoming acceptable for organizations to give the green light for young people to share intimate images? Have we thought about the long-term risks of taking intimate images and sharing them online?

In reality, when a child shares intimate images on the Internet, their entire family becomes victims of non-contact sexual abuse. Both the child and their family can experience long-term anxiety and stress from the knowledge, whether they believe it or not, that these nude or nearly nude images are being spread like wildfire, as they are viewed, shared, and otherwise circulated in a technological environment. The loss of control and the fact that intimate images could resurface at any time leads to ongoing anxiety. And, the reality is, sophisticated communications technology will increase the potential for increased production, better quality, and faster sharing of compromising images by young people simply carrying smart devices.

So what can we do? Education is critical and so is sharing stories with others about how child exploitation and human trafficking rings operate on the Internet. For example, there was a recent arrest in the U.S. involving six men operating a sophisticated web ring, frequenting Internet forums like Kik, Instagram, and Skype to target young underage girls, primarily of the ages 10 to 14. This group lured children into private group chat sessions, where they took on the role of

either hunters, talkers, loopers, or watchers. These predators would encourage a game of dare, that escalated into sexual activity where the looper would play a video of a teenage boy engaging in sexual acts to encourage the victim to also strip off and perform for the group. Over the course of three years, these six offenders accumulated hundreds of images and videos. The criminal sentence for these offenders totals 171 years for offences including producing and viewing child abuse images, engaging in a child exploitation enterprise, committing conspiracy to access with intent to view child pornography, and enticement of a minor to engage in illegal sexual activity. In this incident alone, the non-contact images of child sexual abuse will likely be distributed and broadcast over the Internet for years to come.

Education and focusing on raising awareness is critical for everyone. Children and youth need to be told in no uncertain terms that creating or sending sexually explicit images can be extremely damaging to their emotional well-being because of the long-term potential for harassment, embarrassment, blackmail, and exploitation. They need to know that online sexual predators frequently disseminate playful or sexually explicit messages in locations that young people frequent. They must understand that online relationships can happen very quickly or develop over a prolonged period of time. And, when it comes to online child sexual exploitation, they need to understand how a groomer uses techniques to build an emotional relationship with them to normalize sexual activity. Moreover, it is important to make sure young people understand they have choices when they are online and they do not have to believe everything their online contacts are telling them.

Finally, the police should always be involved when young people are blackmailed or pressured into sharing a nude or nearly nude image.

Below are some tips for parents dealing with the issue of sexting:

1. If the image is posted to a website or is on an app, take a screen shot of the picture and save it or print the page. Document times, dates, links, emails, IM's, anything you have related to the image(s).
2. Request removal. The Canadian website www.NeedHelpNow.ca provides information, resources, and tools to help you remove sexual pictures and videos from popular providers where the picture/video may be displayed on the Internet.
3. Request that image(s) be immediately removed from the website as it violates their terms of use and is causing personal/professional harm. The website may not remove a picture just because it is unflattering.
4. Consider reporting the incident to your local police department. If this is an emergency, call 9-1-1. Show the police the screen shot or any other evidence you may have collected, complete a witness statement if requested, and explain all of your actions to date. Record the police case

number and forward it to the website or any other organizations you have already reported the incident to. The police may follow-up on their own time and with their own investigative procedure.

5. Speak to someone at your child's school to request an educational session be held for the grades involved. These incidents are never just between two people, there are often hundreds of people viewing and forwarding these pictures, and schools are often the collection point.

Key messages for young people about sexting:

1. Never share sexually explicit images of yourself online with anyone. This is extremely dangerous and it may have long-term adverse effects on you personally and professionally.
2. Speak up if you receive a photo that is humiliating, rude, obscene, harmful, and/or sexually explicit. Immediately tell someone that can help such as a parent, teacher, coach, lawyer, website, or possibly the police.
3. Do not share or forward an image of anyone that is inappropriate as this could be against the law. It is illegal to share intimate images of a person, regardless of their age, without the consent of the person in the image. An "intimate image" is defined under the Canadian Criminal Code as an image depicting a person engaged in explicit sexual activity or that depicts a sexual organ anal region or breast. The image would have to be one where the person depicted had a reasonable expectation of privacy.
4. If it is appropriate, speak to the subject of the image yourself. They may not be aware their picture is being distributed and they may need to immediately take action to control the damage.
5. If you (a person under 18 years of age) receive a sexually explicit picture from an adult, report this immediately to the police, a parent or guardian, or to www.Cybertip.ca
6. Everything you do online leaves a digital footprint. Even when using websites or apps that appear anonymous, there are always opportunities to capture screen shots. Disable or obscure your computer's webcam. Don't do anything in front of a camera that would not want the world to see.
7. If you are considering suicide, self-harm or are feeling depressed, seek professional support or counselling at locations like www.KidsHelpPhone.ca or www.NeedHelpNow.ca.
8. Depending on the situation, seek the support of others, including your school principal, counsellor, teacher, school board, superintendent, coach, school resource officer, the website involved, Internet Service Provider, a civil lawyer, or to websites like Cybertip. Depending upon the situation, all of these can be done simultaneously.
9. Be proactive. Set up an alert on your name, email, or cellphone number to help monitor your online identity.
10. Change your passwords on all websites involved. Make sure you have a

strong passcode established on your mobile devices.

Kathy Macdonald, M.O.M., MSc., CPP

A police officer, now retired after 25 years with the Calgary Police Service, Kathy brings almost three decades of investigative experience and security awareness to her position as Instructor with Toddington International. In 2009, the Governor General of Canada invested Kathy with the Order of Merit of the Police Forces (M.O.M.), in recognition for her outstanding work in the area of cyber safety and cyber security.

Kathy has extensive experience developing and delivering cyber awareness and crime prevention programs to both public and private sector organizations worldwide. Her areas of expertise include online fraud, the application of social engineering techniques, child online risk, social media, targeted intrusion, and privacy.

Learn more about Kathy Macdonald and her work here.

Resources for the OSINT Professional

worldc.am – Instagram location search

dragdis.com – Visual bookmarking tool

social-searcher.com – Real-time social media search engine that allows users to set up alerts and save searches

orbisdirectory.bvdinfo.com – International company search tool

moreofit.com – Search for similar sites

bellingcat.com – Resources for the online investigator

pdevesian.eu/tet – Test to see if an email address is connected to a Twitter account

zamzar.com - Online file converter

abalegalfactcheck.com/indexa.html - The American Bar Association's site for fact-checking recent "legal" news

crime-data-explorer.fr.cloud.gov - FBI's 'Crime Data Explorer'

facebook.com/livemap - View a map of Facebook Live streams in your area

keitharm.me/projects/tweet - View a Twitter user's tweet locations on a map

sudoapp.com - A platform that allows your to create an "identity proxy" to safeguard your personal data both online and offline

deseat.me - App that allows you to manage/delete all your online subscriptions

picodash.com - Instagram search engine for exploring posts, users, and locations

unfollowgram.com - Find out who "unfollowed" you

mulpix.com - Instagram search engine: search captions, mentions and tags

socialmention.com - Real-time social media search and analysis

---

Want more? Visit our continually updated, FREE online research resources page featuring hundreds of links, cheat sheets, investigative guidelines, and more!

E-Learning: *"Using the Internet as an Investigative Research Tool™"*

Take your Online Research and Intelligence Skills to New Levels

The most comprehensive and up-to-date Internet research and investigation e-learning program available anywhere, *"Using the Internet as an Investigative Research Tool™"* is designed to enable investigators, researchers, and intelligence personnel to *find better online information, in less time, at less cost, with less risk™*.

For a fraction of the cost of classroom-based training, our flexible and interactive virtual classroom environment allows candidates to progress at their own pace and competency level, with a qualified personal instructor on hand at all times to ensure success. Initially launched in 1998, this highly-acclaimed and continually updated online course has been successfully completed by well over six thousand investigators and knowledge workers around the world.

Enrollment takes only a few moments; online credit card payments are accepted, group discounts and licensing options are available for five or more registrants. Visit the course page to find out more and instantly register, or contact us directly with any questions.

Bonus: Tuition fee includes a one-year subscription to the newly revised and updated TII Premium Resource Knowledge Base, a premium resource of some 4,000 deep web resources and sites (**an additional $299 value**)!

As a HRSDC certified educational institution, TII provides Canadian students with a T2202A Tuition Tax Receipt.

More Online Training

Open Source Intelligence for Financial Investigators
40-Hour E-Learning Program

Essential for all financial institutions and corporations required to comply with the *European Union Fourth Anti-Money Laundering (AML) Directive* and similar legislation, or otherwise engaging in enhanced due diligence activities, this comprehensive training provides financial and business professionals with the latest tools and techniques required to effectively gather online OSINT, with the aim of enhancing compliance activities and minimizing potentially detrimental risks to an organization — both quickly and accurately. **Sign up or learn more** here.

Introduction to Intelligence Analysis
40-Hour E-Learning Program

This program provides a rich and interesting opportunity to explore the key concepts and intellectual foundations which inform intelligence analysis activity. Students will develop awareness of, and experience in, using common tools and methodologies to conduct analysis assignments, as well as learn how to fashion one's insights and ideas in a way that communicates effectively to clients and other intelligence consumers. **Sign up or learn more** here.

Criminal Intelligence Analysis
40-Hour E-Learning Program

This program is designed to equip aspiring and inexperienced analysts, as well as other interested law enforcement and investigative professionals, with the knowledge and skills required to undertake criminal intelligence analysis work, and to understand criminal intelligence analysis products when encountered. **Sign up or learn more** here.

Strategic Intelligence Analysis
40-Hour E-Learning Program

This program is intended for professionals working in public sector enforcement, intelligence, national security, and regulatory compliance roles, or those aspiring to do so. Students will be equipped with the skills and knowledge required to

effectively conceive, plan, and implement strategic analysis projects, and deliver impactful strategic advice to clients and other end users. **Sign up or learn more here.**

Also of Interest to the OSINT Professional

"Here's what your identity sells for on the dark web"

"Most-wanted criminal arrested after posting Instagram video of himself"

"What is phishing? How to protect yourself from scam emails and more"

"Identity theft at 'epidemic' levels, warn experts"

"These are the 10 most used smartphone apps"

"Cyberwar: A guide to the frightening future of online conflict"

"Spambot leaks more than 700m email addresses in massive data breach"

Favoured by drug dealers, Monero aims to be more anonymous than Bitcoin with trades not viewable on a public ledger

The importance of profiling during the course of difficult investigations

"Search Flickr Better With Google Images"

"How to Hide a File in your Google Drive in Plain Sight"

"Turning To VPNs For Online Privacy? You Might Be Putting Your Data At Risk"

"Court rejects LinkedIn claim that unauthorized scraping is hacking"

"How Much Data is Generated Every Minute?" [Infographic]

"Dust isn't the only thing your Roomba is sucking up. It's also gathering maps of your house."

"When, Where & How to Listen to Google"

"'Social media triangulation' provides new approach for emergency responders"

"How to Tell if a Photo Has Been Doctored"

“Who Unfollowed Me on Instagram? The Only Way to Find Out”

follow on Twitter | friend on Facebook | forward to a friend