Subscribe | Past Issues | Translate ▾

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 2020 EDITION

In This Edition

Welcome to the Newsletter

Subscribe Past Issues Translate ▼

This year of 2020 has been anything but normal, and just as with everyone, our business has changed in significant ways.

Gone are the classroom-based, in-person training programs. Here are live remote training programs via Zoom and enhanced self-paced study programs via Moodle.

In pivoting to new delivery mechanisms to serve our clients in isolated work environments, we've noticed something remarkable: **By fully embracing remote delivery technologies, there are many significant and quantifiable advantages to remote learning that are not available through the "old school" (classroom) delivery mechanisms we have all relied on for so many years.**

The advantages of remote training we've been able to realize have not happened by accident; rather, they have come as a result of significant investment in hardware, software, and the skill building necessary to deliver a quality product. We have put deliberate effort into re-thinking adult-learning models in this new paradigm, and we have consulted with psychologists and other behavioural scientists to not just understand, but to innovate in this new environment.

Taking advantage of the elimination of training venue and travel costs, we have been able to introduce multiple specialized instructors into many of our learning programs to create even more comprehensive training offerings that appeal to a wider range of students, all the while providing better value for money.

And this shift is paying off. Customer feedback is excellent, clients are receiving more "bang for their buck," and student satisfaction is at an all-time high.

employees are now working in, training is seen as “highly important,” not just for personal development, but also for essential team building in these difficult times.

What can we do for you? Contact us to find out, we are happy to share our experience.

e-Learning Graduates

Congratulations to the following students who are among those who successfully completed an e-learning program with TII this month:

- Ronald Mathews
- Colleen Maynes
- Josh B
- Isabelle Carter
- David Willey
- Arjun Patel
- Holly Rivard
- Roger Jing Severo
- Meriam Larbes
- Fernanda Rodriguez
- Sarah Chan
- Stephen Vaucher
- Kassandra O'Brien
- Barbara Coleman
- Andrew Bain
- Jason Muise
- Alex Cheyne
- Charlotte Foster
- Sharon Roddis
- Vincent Murray
- Shaminder Singh
- Annie Law
- Sima Fazel
- Brad Connor
- Liana Velásquez
- Mattias Nilsson
- Patrick Hogan
- Casey McRae
- Amelia Robinson
- Denise Winston
- Jamie Herbert

- Phillip Lang
- Anouk Van de Berg
- Maria Ruiz Guzmán
- Rita Bauer
- Kyle Cunningham
- Emiliano Amici
- Michael Peters
- Anthony Hiebert
- Gurinder Bassi
- Adam Webb
- Neil Stefanyk

Important Note: As we respect the privacy of our students, we only publish the names of students who have provided express permission to do so. Many of our students are unable to share their completion due to the nature of their employment, or due to online privacy concerns. If your name did not appear in the above list and you wish to announce your completion of the course with TII, please contact us.

"Using the Internet as an Investigative Research Tool™" Self-Paced e-Learning

Take Your Online Research and Intelligence Skills to New Levels with TII's Comprehensive, Self-Paced e-Learning Program, "Using the Internet as an Investigative Research Tool™"

The most comprehensive and up-to-date internet research and investigation e-learning program available, "Using the Internet as an Investigative Research Tool™" is designed to enable investigators, researchers, and intelligence professionals to find

Initially launched in 1998, this highly-acclaimed and *continually updated* online course has been successfully completed by tens of thousands of investigators and knowledge workers around the world.

Our proven, 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.

Enrollment takes only a few moments; online credit card payments are accepted, and 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 complimentary accounts for EchoSec, PIPL Pro, and more.

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

More Self-Paced e-Learning Programs

Social Media Intelligence & Investigations

30-Hour e-Learning Program

COMING SOON - This highly-anticipated program will introduce research and investigative professionals to a variety of essential tools and techniques necessary to safely and appropriately. **Learn more and sign up for the wait list** 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 of intelligence analysis.** Students will develop awareness of, and gain 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. **Learn more and sign up** here**.**

Criminal Intelligence Analysis

40-Hour e-Learning Program

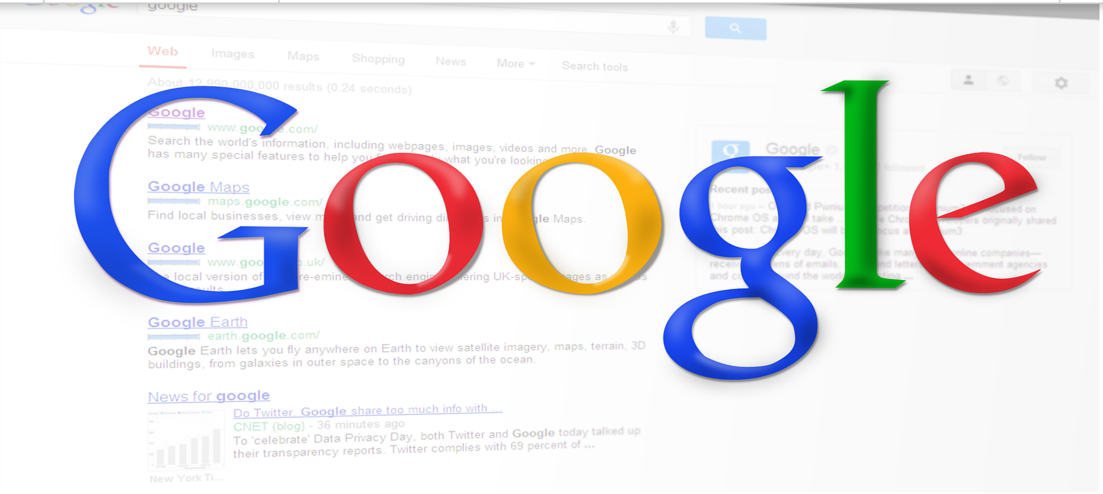
This program is **designed to equip aspiring and new analysts**, as well as other interested law enforcement and investigative professionals, with the knowledge and skills required to undertake criminal intelligence analysis work, and to understand criminal intelligence analysis products when encountered.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

Google Ratchets Up AI to Increase Search Result Relevance



Google is always tweaking its algorithms to improve search results and at its recent Search On event, the company revealed some significant AI driven improvements that it will be making in the coming months, to assist the average user finding what they are looking for.

According to Head of Search, Prabhakar Raghavan, over a billion people each day now use Google, and of all of the queries they enter, a whopping 15% have never been seen by that search engine before. Add to the mix that 1 in 10 queries are misspelled, and it's easy to understand why Google is sometimes left lacking in relevant results.

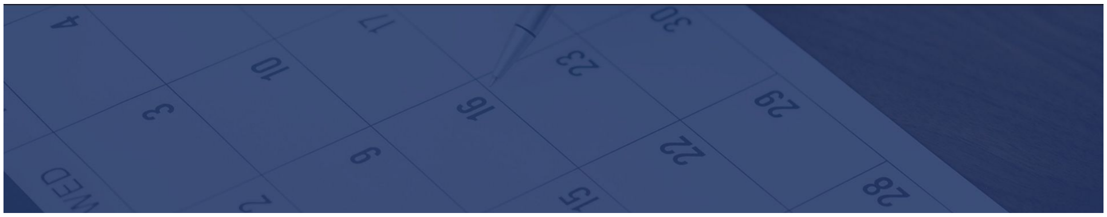
Within the next month Google will be attempting to overcome some of these issues with upgraded AI capability. What the company promises will be an improvement over its "Did You Mean" function, a new spelling algorithm powered by a 680 million parameter neural network. Improvements to indexing algorithms are also promised with Google's search 'bot now indexing individual passages of web pages, instead of the whole web document. Google also announced they will be improving capability around dividing broader searches into subtopics, and important to OSINT practitioners, using computer vision and speech recognition to tag and divide video content into distinct parts (an automated version of the existing chapter tools it currently provides).

Statistical research will also see some significant improvements. Since 2018, Google has been working with the Data Commons Project, an open knowledge database of statistical data started in collaboration with the World Bank, US Bureau of Labor Statistics, US Census, and many others. With a question that could be answered best with a statistic (example: "how many people work in Portland?") Google will start using natural language processing to map that query to one specific set of the billions of data points in Data Commons to provide the right statistic in a "visual, easy to understand format"; it may also provide other relevant data points and context (like stats for other cities) to help a user explore that topic in more depth.

If it performs as advertised, these will certainly be great strides in Google's ability to

While these new capabilities will be potentially very beneficial for average internet users, we strongly suggest that semantic search is still very much in its infancy, and that OSINT and investigative professionals will need to continue to tactically and strategically apply Google's advanced search operators to get the most of the world's most popular search engine for maximum effect.

Upcoming Select Public Courses



Dates	Location & Time	Courses
November 5-6, 2020	Remote Delivery 1000-1800 EDT (1400-2200 UTC)	Social Media Intelligence & Investigation
November 16-17, 2020	Remote Delivery 1000-1800 EDT (1400-2200 UTC)	Advanced Internet Intelligence & Online Investigations

Group discounts are available. Contact us to find out more.

Don't see the course you're looking for? TII is pleased to offer a number of specialized and customizable in-house training programs for both the public and private sectors internationally. To learn more about what we can do to empower your workforce, contact us**.**

"How to Survive the Internet - Protect your family from hackers and cyber stalkers"

It seems that any book published these days about cyber security will be of two types: the highly technical manual that leaves the average technology user befuddled, or the dark and ominous read (think dark images of hoodie-wearing hackers behind a keyboard) that can leave those same average

Is it possible for a book to provide a positive, non-technical account that will leave the average technology user not just feeling better informed, but actually empowered?

Enter “How to Survive the Internet - Protect your family from hackers and cyber stalkers” by Paul Vlissidis.

A long-time security guru, Paul has an impressive resume advising on cyber risks at the board level on a variety of high-level areas, including risk assessment, threat modelling, network security testing, and the high-level auditing of architectures and designs. He’s the person who has “been there and done that” on a huge number of cyber-security issues over the past few decades.

And so why would he write a book for the average user? And why something so different in look and feel from anything written so far? We had a chat to find out more…

David: Tell me a bit about what inspired “How to Survive the Internet.”

Paul: *“As the leader of the cyber team on Channel 4’s 'Hunted,' I had the unique opportunity to see the failings of people, in the real world, that were deliberately trying to hide themselves and cover their digital footprints. It was surprising just how much we were able to find on their devices and about them in the online world, and it really dawned on me that people are really bad at this stuff. It was something we all sort of knew, but I really hadn’t put it together in my head as to really quite how bad people actually are. It was at the end of filming Hunted that we created a product around this lack of awareness called a 'Digital Footprint Review' aimed at company directors and high net-worth individuals. We focused this product not just on them but also their families and people close to them, and after analyzing their digital usage, tell them how a hacker was likely to attack them. The Digital Footprint Review was really successful and revealed some really interesting war stories. As I wrote down what we were learning about these users, a colleague of mine suggested that all of this knowledge should really be put down into a book. It was about a year ago that I started forming an outline for a possible book when I realized just how much there is out there that needs to be told.”*

David: How did you go about understanding what the average technology user wanted, and then needed to know, to be better protected?

Paul: *“After the Digital Footprint Review initiative, I wrote a number of short articles that I published to LinkedIn and Facebook, and the feedback from these was really good; it* *media platforms and their devices to protect themselves. As it all came together, I decided I really didn't want to make people paranoid, turn them into 'preppers' or start wearing tin foil hats, instead I felt it important to give them real-world, useful information."*

David: What are some of the things you cover in the book that the average technology user may be unaware represents a risk?

Paul: *"I cover all the essential things like 'Two Factor Authentication,' but I also cover mobile phone settings, the 'Internet of Things,' along with explanations of things like why using public WiFi is a bad idea and what a VPN is for… the sorts of things that we security professionals take for granted but the average person doesn't know about. A lot of research went into the book which saw me setting up many different types of social media accounts so that I could really see where security settings needed to be on each one."*

David: What were some of the challenges to writing the book and how did you overcome them?

Paul: *"Getting a professional editor was invaluable. I found my writing style actually changed from day to day, sometimes it may be very technical, other times it may be very businesslike. Having an editor ensured it all flowed and maintained that easy understandable language I was looking for. Having the book professionally typeset was a massive advantage as well to properly show sources and the tables required to keep things clear."*

David: This was no small undertaking, what was your biggest motivation in doing this?

Paul: *"I've learned a lot over the years, and I wanted to give something back to the greater community. The problem with working in the security community is that we end up living in a bubble and sometimes forget that a lot of people don't know this stuff. What I hope to do is empower people, not leaving them susceptible to all sorts of vulnerabilities. It seems so many people don't fully understand what their digital footprint looks like and how it can be used against them. There are also a huge number of misconceptions that I address as well. I'm not trying to turn people into privacy nuts, I just want to inform people and advise them on how some simple things can make a huge difference."*

David: What were the big things you took away from your experience heading up the cyber team on the "Hunted" television series?

Paul: *"As a massive simulation exercise, it became clear doing Hunted that so many people just don't have a clue about how and where their information is stored and how vulnerable they can be. And it's not because they are stupid, not at all, it's just that it's not common knowledge and nobody has ever made them aware of their vulnerabilities. The* *we did on the program, I found that almost a 'domino' effect took place and we'd end up hacking multiple accounts in rapid succession until we essentially had total control of someone's online life. It was quite shocking to realize just how much information we could glean, and it certainly got me thinking about just how dangerous this could be for someone who was acting maliciously and the damage they could do."*

David: How effective are people who would generally classify as "average" technology users in assessing risk around their digital security?

Paul: *"One big issue is that people don't think like attackers. With over 20 years of experience in ethical hacking, I've learned to think like the attacker, seeing risk and seeing threat. It's not reasonable to think that members of the public think this way at all, nor would it be desirable. What I wanted to do with this book is not have people think like I do, which is not at all realistic, just have them know that if they do certain simple things, they can be much less at risk and with that, they can operate much more confidently in this digital landscape."*

David: Finally, what would you say to those who say they "have nothing to hide"?

Paul: *"It's not about whether you have anything to hide, the real question is, do you have something that someone else can use against you? When you better understand how organizations collect and use your information, your attitude will change. In the book, I give an example about how a diet app was collecting a massive amount of information on users, including when and where they had their doctor's appointments, and where they were at certain times of the day. In an example like this, someone could say they had nothing to hide and even that the risks seem low, but most people really have no idea how their data is being used, how long it is kept and an even bigger question, what about if someone gets unauthorized access to their data? When someone says they have nothing to hide, its almost like an answer to the wrong question. In the book, I also talk about not just phones but all sorts of Internet of Things devices, including smart TVs, and how all of these devices are collecting information that is not necessarily anonymized."*

David: What does the future look like to you in terms of digital privacy and security?

Paul: *"The more we spread ourselves around on the Internet, the more of a problem this is likely to become. If we look at the Millennials, they were adopting many technologies at a time when security settings were poorly understood and not properly set by default. What worries me is that as the Millennials become tomorrow's managers and business leaders, they could be dragging this messy digital footprint behind them that is going to cause all sorts of problems and make them easy targets for criminals and others that wish them ill. I think what is important is that people are able to take back their footprint and to ensure that they become selective in what information they give out and how they give it out. There are a number of concepts I discuss in the last chapter that really give hope to*

"How to Survive the Internet - Protect your family from hackers and cyber stalkers" makes for an engaging read in jargon-free, plain English, and whether you are a digital native or a digital immigrant, chances are you'll learn something valuable.

Available in e-Book or paperback format, you can find out more at https://howtosurvivetheinternet.co.uk You can currently see Paul and his Cyber team in action on the UK hit TV series “Hunted” on Amazon Prime.

Tools, How-To's, and Articles of Interest for the OSINT Professional

How to change your personal Meeting ID in Zoom to make it easier for others to join your meetings

Google "Search On" 2020

Live facial recognition is tracking kids suspected of being criminals (MIT)

Google hit by landmark competition lawsuit in the US over search

How Google will fight off the DOJ's claims of monopoly in search

EU investigates Instagram over handling of children's data

How to search a conversation on Skype and find specific text in old chat thread

Snapchat hits nearly 250m daily users

More than 50% of humans in the world use social media - here's what you need to know

PayPal to open up network to cryptocurrencies

4 Ways to Schedule Posts to Multiple Social Media Platforms at Once

How Google autocomplete predictions are generated

A united front against online piracy in Asia Pacific

Google shuts down Trusted Contacts, its emergency location sharing app

When coffee makers are demanding a ransom, you know IoT is screwed

Photoshop tool could help fight fake images

UTZOO Discussion Forums - An archive of over 2.1 million USENET posts from February 1981 to June 1991, with plans to add more historical data soon

"How to detect deepfake faces": Computers are getting better at dreaming up “deepfakes”, photorealistic human faces created using a technology called a generative adversarial network, or GAN. This illustrated guide looks at what deepfakes are and how to spot them.

Atlas of Surveillance: The Atlas of Surveillance contains several thousand data points on over 3,000 law enforcement agencies throughout the US, allowing users to review details about technologies police are deploying, and check what devices and systems have been purchased

"Blacklight" is a new privacy awareness tool that reveals what trackers are running in the background of websites without you having to visit those websites first, including the particularly problematic Facebook Pixel tracking tool

Neeva: A new search engine founded by former Senior VP at Google, Sridhar Ramaswamy. Neeva claims it will not "serve you ads or sell your data" and will search the web and your personal files for $10/mo (free until the end of this year).

Follow us on Twitter for daily articles, tools, and other interesting industry updates.

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

Subscribe | Past Issues | Translate ▾