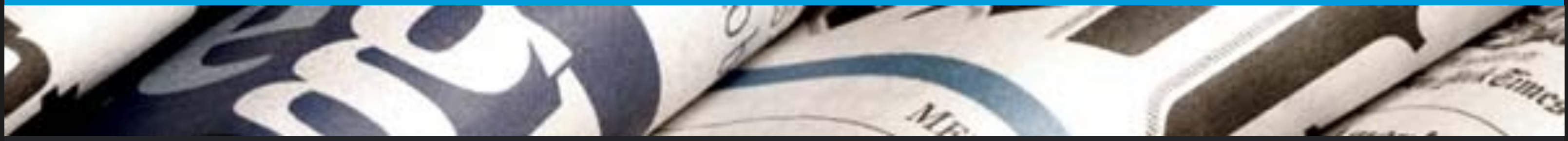
News, Resources and Useful Information for the Online Investigative and OSINT Professional from Toddington International Inc.



Toddington International Inc.

Online Research and Intelligence Newsletter

February 2016 EDITION

In This Edition

Welcome to the Newsletter

The start of 2016 has the team at Toddington International busy as we soon launch a new website, a number of new courses and prepare to make some exciting announcements.

We are also pleased to welcome UK based Ben Owen to the TII team as he takes on the role of Operations Manager. With an award-winning military career in the Royal Air Force Regiment (including active service in Safwan and Basrah during the second Gulf war) Ben brings us over a decade of front-line tactical and strategic intelligence operations experience.

Ben Owen, Operations Manager TII

Retiring from the military in 2005, Ben joined the British intelligence service and was tasked with intelligence gathering on some of the highest profile counter-terrorism operations to date, eventually leading covert intelligence operations teams throughout the UK.

Ben entered the private sector in 2014, developing rapid-response, covert operations teams to combat serious and organised crime in the financial services industry, utilizing online and offline OSINT, HUMINT, SOCMINT and SIGINT to prevent over £1 million loss resulting from fraud and organised crime, in less than 12 months.

With extensive experience in national and international intelligence-led operations, including large-scale security operations such as the London Olympic Games and Glasgow Commonwealth Games, Ben's knowledge of OSINT, and digital and covert operations, is a valuable addition to our rapidly expanding global training and operational offerings.

Ben appears as Second in Command of the Incident Command Centre, alongside David Toddington and Julie Clegg on the critically acclaimed Channel 4 television series "Hunted".

Congratulations to the following students who have successfully completed the 40 hour **Using the Internet as an Investigative Research Tool™** e-Learning program:

- Steffen Koy - Earnest & Young
- Colin Steeksma - Xpera Risk Mitigation & Investigation
- River Cheung - Commonwealth Bank
- Sarah Bunder - Investigative Research Group
- Michelle Welsh - Xpera Risk Mitigation & Investigation
- Adele MacDonald - Progress Investigations
- Juanita Prinsloo - Johannesburg Housing Company
- Brian Armstrong - Ontario Provincial Police
- Isabel Coates - Canada Revenue Agency
- Lisa Greenough - Department of Justice (Nova Scotia)
- Alan Chung

Start the Year Upgrading Your Online Research Skills

Using the Internet as an Investigative Research Tool™ E-Learning Program

INTERNET RESEARCH SKILLS FOR FINANCIAL INVESTIGATORS
TODDINGTON INTERNATIONAL eL
INTERNET RESEARCH SK
FOR FINANCIAL INVESTI
USING THE INTERNET AS AN INVESTIGATIVE RESEARCH TOOL
TODDINGTON INTERNATIONAL eLEARNING
USING THE INTERNET AS AN
INVESTIGATIVE RESEARCH TOOL

Time-limited Offer!
Sign up now for just $399 CAD *(Regular price $750 CAD)*

Faster Learning and Higher Retention

Did you know e-Learners experience significantly higher rates of retention than classroom course attendees, and they learn in 30-60% less time than attending a comparable classroom course? Various recently published studies show that ***individuals taking online courses often retain up to 100% more information than if they took a comparable classroom course.***

Trusted by Thousands

Initially launched in 1998, continually updated and recently redesigned, this highly acclaimed program has been successfully completed by over ***eight thousand investigators***, researchers, and open source intelligence professionals worldwide.

Cost Effective

For a fraction of the cost of a classroom-based training course, this flexible and interactive virtual classroom environment allows students to progress at their own pace and competency level with ***a qualified personal instructor on hand at all times to ensure success.***

Accredited and Tax Deductable

As a HRSDC certified educational institution, TII provides Canadian students with a ***T2202 Tax Receipt and a Certificate of Completion from the Ontario Police College***.

Easy and Immediate Enrollment

Enrollment takes only a few moments; online credit card payments are accepted, and group discounts and licensing options are available.

Visit the TII e-Learning page to find out more and instantly register, or contact us directly with any questions

Setting Up a Covert Email Account: How Hard Can it Be?

Image by brianklug via Flickr

By Norm Wilhelm,
Associate, Toddington International Inc.

A month ago while I was teaching a course, a student had wanted to create a new email address. The email address needed to be under a proxy name and require only a minimal amount of personal information. It would be used for investigative purposes without any attached information that could indicate this person's real name, real location, real contact information, real occupation, or the law enforcement organization he worked for. This turned out to be a more difficult problem than one would think it to be. So, what made this so difficult? The problem is that getting an email address is getting more complicated for two main reasons: (a) email server providers are asking for a lot of personal information; and (b) users want to provide less personal information.

As most people know, the email address has become the linchpin to gaining access to the contents of almost every surface-web social networking website around the world. You need an email address to create an account, and then sign into an account. The account is a requirement for accessing almost every major social networking website, regulating users who want access to more details, more content, or want to contribute information. Without that account, you see just what any general member of the public sees, or you might get to see nothing at all.

For those who like a few facts, here are some for emails and social networking accounts. A report from 2014 projected that there are over 4.3 billion email accounts worldwide, of which over 1 billion are corporation-related and over 3 billion are consumer (personal) accounts. The same report assesses that there are over 3.6 million social networking accounts. The article does not specify if these statistics include every account ever created, or considers persons having duplicate accounts. Either way, even with each person online probably having multiple email addresses and multiple social networking accounts, thats a lot of potential for personal information.

As to the problem of getting an email, more and more email service providers appear to be wanting more and more mandatory information about you before they will give you that email address. They want your real name; they want your current address; they want your telephone number; they want your postal code. Others want your birth date, gender, language preferences, and nation of origin. Some may even slip in security questions asking about your high school, mother's maiden name, or your pet's name. To make sure you aren't just making information up, they may even include verification checks, such as cross-checking your IP address location against the postal code you provide, rejecting any data you enter that doesn't match.

If you were to query Internet sources, you would find that there are valid reasons for this level of mandatory information, which can range from due diligence efforts, to national security, to the acquisition of marketing data, to the prevention of identity theft. But that still wont convince people they should provide that mandatory information. Especially when those people are involved in intelligence, security and/or law enforcement efforts, where the wrong person getting access to this mandatory information could jeopardize lengthy investigations, undercover operations (etc.) or personal safety. Regardless of whether they are criminals, hackers, up to no good, private security, law enforcement, or just plain regular folk, many people active on the Web today want to remain anonymous too. If not anonymous, then to provide as little information as possible about themselves.

Now comes the problem, just like this student faced - which email service should he use? I can provide you suggestions in the classroom, but for an article being published in the public domain, I need to be a bit impartial and not specifically point out which is the best in my point of view. And, with a potentially worldwide audience reading this, one solution for a person in North America isn't neccesarily going to work for everybody else around the world. Instead I will show information that will help people with making that choice for themselves.

For the purposes of this article, the following thirteen email services providers were reviewed to determine what level of information they deem mandatory for gaining an email address from their service: AOLwebmail, Fastmail, Gmail, GMX Mail, Hushmail, iCloud, Lycos, Maildotcom, Outlook, QQMail, Yahoo Mail, Yandex Mail, and Zoho. These were selected as representing (a) the most popular worlwide and (b) anyone could potentially apply. Of note, while there are many ways that an email service can be assessed or evaluated, this list is not intended to identify the best one; the listing will focus only on those aspects related to mandatory information.

AOL Webmail (Est. 1993, USA) - Free; AOL domain

Required Information:

First name Last name
Username Password
Birthdate Gender
Postal code Security question

Fastmail (Est. 1999, USA) - 30-day free trial; Over 100 domains available.

Required Information:

Nickname
Username
Password

Gmail (Est. 2004, USA) - Free or paid; Google domain, also supports custom domain

Required Information:

First name Last name
Username Password
Birthdate Gender
Country

GMX Mail (Est. 1997, Germany) - Free or Paid; Two GMX domains

Required Information:

First name
Last name
Username
Password
Birthdate
Gender
Country
Security question
Customer number assigned

Hushmail (Est. 1999, Canada) - Free or paid; Five Hush domains

Required Information:

User name
Password

Apple iCloud (Est. 2011, USA) - Free; links to user's Apple devices

Required Information:

First name
Last name
Username
Password
Birthdate
Apple device information

Lycos (Est. 1995, USA) - Free or paid; Lycos domain

Required Information:

Username
Password
Cell phone number
Country
PIN code sent to your device

Maildotcom (Est. 1995, Germany) - Free or Paid; Over 250+ domains

Required Information:

First name
Last name
Username
Password
Birthdate
Gender
Country
Security question
Customer number assigned

Outlook *aka Hotmail, Live, MSN* (Est. 1996, USA) - Free or paid; Numerous domains

Required Information:

First name
Last name

Username
Password
Birthdate
Gender
Country
Postal code
Telephone number
Alternate email address

Tencent QQ Mail (Est. 1999, China) - Paid; QQMail domain

Required Information:

Nickname
Username
Password
Birthdate
Gender
Country
Province
City
Customer number assigned

Yahoo Mail (Est. 1997, USA) - Free or paid; numerous Yahoo domains

Required Information:

Firstname
Lastname
Username
Password
Telephone number
Birthdate
Gender
Language
Alternate telephone number

Yandex Mail (Est. 2000, Russia) - Free or paid; Yandex domain

Required Information:

Firstname
Lastname
Password
Telephone number
Security Question

Zoho (Est. 2008, USA) - Free or Paid; Create custom domain

Required Information:

Firstname
Lastname
Email address
Password
Contact email address

After reviewing the results, the following patterns of mandatory information were found:

- ***First name/ Last name**: 8 out of 13 required identifying your first and last name; 1 additional service has your name as part of device registration.*

- ***Nickname:*** *2 out out of 13 asked for a Nickname instead of a First name / Last name*
- ***User name****: 8 out of 13 required a User name in addition to the First name/ Last name, or Nick name; 2 services only required a User name by itself*
- ***Password****: All required a password.*
- ***Birthdate:*** *6 out of 13 required a Birth date; 1 additional service may have your birthdate as part of device registration.*
- ***Gender****: 7 out of 13 required you to identify your Gender.*
- ***Language:*** *1 out of 13 specifically asked for your language preference.*
- ***Postal Code, Country, Province/State or City:*** *7 out of 13 required some form of location information; 1 additional service may have your location as part of device registration.*
- ***Security question:*** *4 out of 13 had additional security questions.*
- ***Customer number/ PIN code:*** *3 out of 13 assigned the new user a unique company identification number in addition to the email address; 1 additional service will have assigned you a unqiue customer service number as part of device registration.*
- ***Cell phone number/ Telephone number****: 5 out of 13 asked for a cell or telephone number.*
- ***Alternate telephone number:*** *1 out of 13 asked for a second cell or telephone number.*
- ***Alternate email address:*** *2 out of 13 asked for an alternate email address.*
- ***Cost:*** *1 out of 13 was completely free; 10 out of 13 offered free and paid versions of accounts; 2 out of 13 required payment for creating an account;*

As you can see, signing up for a new email account can involve quite a bit of personal information depending on which service provider you choose. Out of the thirteen reviewed, the Canadian-based Hushmail asked for the least amount of information, only a user name and a password. Outlook asked for the most mandatory information, requiring not just personal information, but also a telephone number and alternat email address; it is also linked to multiple accounts and devices. If you are using a paid account, the provided credit card information may also be linked to your account. And who knew that 'Gender' was such an important part of signing up for an email address?

In closing, this article isn't about telling you which service provider to use. Instead I can point out some suggestions that might help with selecting which service provider would be best for you.

1. Stay inside your nation: If you are not worried about being the target of queries, it is best to stay within your own national borders. In this way, if someone does gain access to your information through that service provider, being in the same country as you increases your options for legal action.

2. Or, go outside your nation: If you are concerned about being the target of queries from nationally-based organizations (be it civil, criminal or other), you might want your information outside the country. It is difficult for legal courts and law enforcement requests to compel organizations to provide information when they are located in another country.

3. Which country?: Without pointing any fingers, some countries have different interpretations about the 'privacy' of personal information. You might want to choose a service provider in a country that applies the concept of 'privacy' in a manner that you agree with.

4. Personal information: Whether you use your real information or false information to get a personal email account for personal Web surfing is your decision. However, if you are using this account for work (security, law enforcement, regulatory, investigation, intelligence, etc.) you need to put as much thought into your email information as you do when you create an account on a website. What name will you use? What will your nickname be? What birthdate will you give? Where will you identify yourself as living? If you choose an option like Hushmail, these questions are unimportant; otherwise you may need to make sure this information meets organization policy and the applicable case law.

5. Truely anonymous?: Very few email service providers offer complete privacy, or the capability of complete privacy. As business organizations, they are subject to the the court systems for law enforcement warrants, and national laws of the country they are in regarding cooperation with security and intelligence organizations. If you truly need or want to be completely anonymous it requires at the very least these two things: don't provide the personal information when you register, and don't access the account in a way that allows your actual location to be identified.

6. Cost: For most email service providers, the cost is just for extra storage space. If you don't need the extra storage space, then you can probably make do with a free account. Plus, there isn't much sense in trying to create an anonymous email account, hen pay for it with a credit card that has your name on it.

7. How do I want to appear?: Due to the enormous amount of spam and scam mails out there, choosing a recognizeable email domain name could be important. Names like AOL.com, Gmail.com, and Yahoo.com tend to lend a level of credibility to your online identity. Emails from persons using less well known domain names could be regarded with suspicion by people, or could be immediately sent to the junk folder by protective filters and programs.

For your regular person who just wants to surf the Web, these details can be unimportant. For others, it can be very important. Or you could just lie about your personal information like many people do, as indicated by several research studies. But for those in the security, law enforcement, investigation, and intelligence fields it can be a bit trickier, as they might not want any of their actual personal information being used. Depending on what type of work you are doing, and who might be looking closer at your personal information, it might require a bit of thought and planning.

Upcoming Training - Australia and Hong Kong

TODDINGTON
INTERNATIONAL INC.

Knowledge Powered
by Intelligence™

ADVANCED INTERNET INTELLIGENCE AND ONLINE INVESTIGATIONS TRAINING

AUSTRALIA: February 29 to March 2, 2016
HONG KONG: March 7th to 9th, 2016

Acquiring useful and relevant open source intelligence (OSINT) requires much more than just an ability to surf the web. Many valuable sources of intelligence are unknown and untapped by investigators who simply don't know what they don't know about finding information online.

Delivering advanced search and analysis techniques for web and social media based information, this advanced program will examine a number of case studies that highlight successes and failures. Tools to ensure data and communication security will be examined, as well as techniques being used by the others to conceal identity, location and behaviour.

Click here for more information, a full brochure and to register, or email with any questions

Resources for the OSINT Professional

FlashDisable - Firefox add-on for disabling Flash or accepting from trusted sites only

Oscobo - Privacy oriented search engine that claims to not store or share data

IXMaps - Shows the route your "local" Internet data packets follow (from Canada through the US)

ZenMate - Free browser-based VPN

TunnelBear - Browser extension for private browsing that allows you to choose a VPN server location from 15 countries

AVulnerabilityChecker - Check if your malware protection is vulnerable to exploitable constant Read-Write-Execute (RWX) addresses

Slikk - Live view search engine

Newspaper Archive - Scanned Newspapers

Mention Alerts - Social Media Alerts

Web Annotator - Add annotations to webpages (available as a Chrome extension or bookmarklet)

Onion Cab - Tor/Dark Web search engine

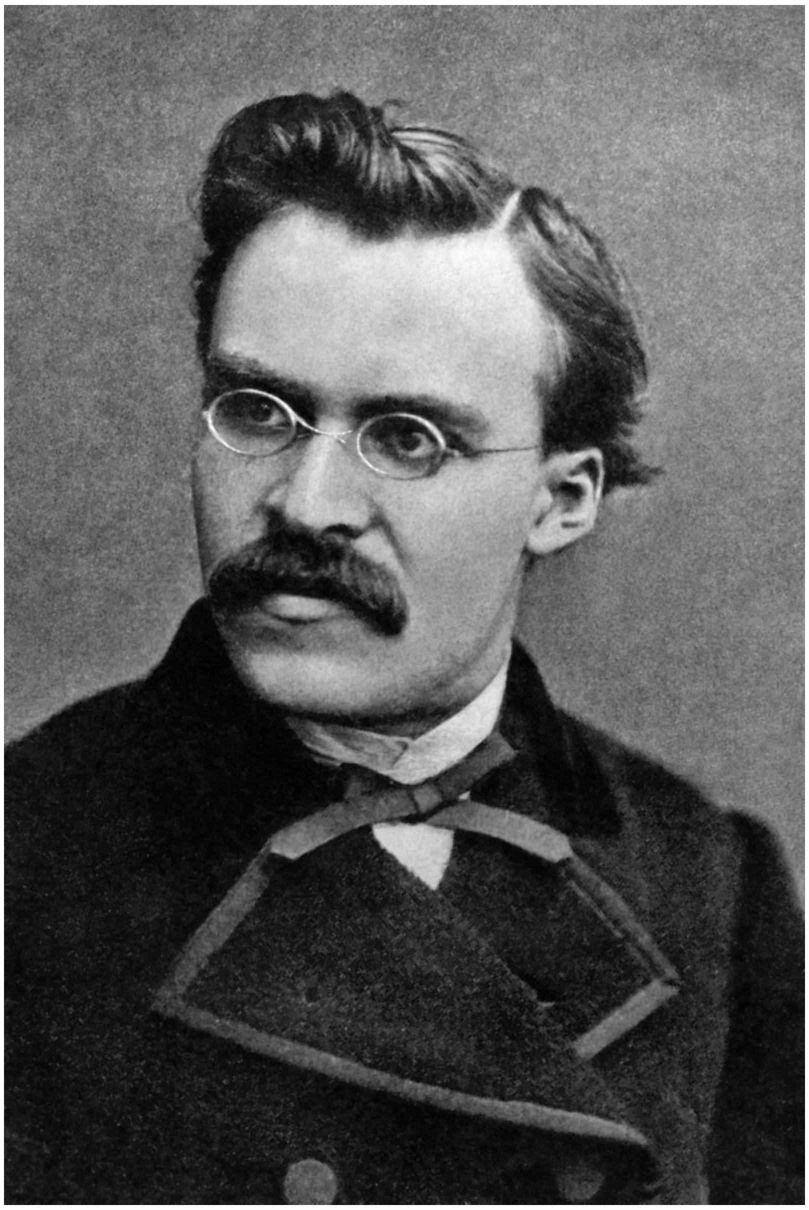
CacheBrowser - Proxy-less tool for bypassing Internet censorship

Criptext - Encrypted email software that lets you "unsend" emails (Available for Chrome and Safari; Firefox and Outlook extensions in development)

Carrot2 - Clustering meta search engine

Metapicz - Online metadata and exif viewer

Thoughts for Investigators and Intelligence Analysts...



“It is precisely facts that do not exist, only interpretations...”

The Portable Nietzsche (1954) by Walter Kaufmann

Also of Interest to the OSINT Professional

“How to: find local Twitter reaction to a national event”

“How To Use Reverse Image Search”

“How to Find Someone On Facebook Without Logging In”

“16 Hidden Chrome Settings Worth Tweaking”

“How to: Remove yourself from all background check websites”

“Traffic Cameras in Bing Maps”

“Here’s What Tor’s Data Looks Like as It Flows Around the World”

“Bangladesh lifts ban on social media”

“Which Search Engine Should You Be Using Today?”

"DuckDuckGo: “Save time with these search tips”

“Google has gotten incredibly good at predicting traffic — here's how”

"Canada’s military plans to monitor the world’s social media"

“Cybercriminals will target Apple in 2016, say experts"

“At School And At Home, How Much Does The Internet Know About Kids?”

“Tumblr the new tool for teenage thieves”

“Facebook quizzes: What happens to your data?”

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