Increasing Anonymity, Privacy and Security on the Internet

Introduction

This short document is intended to outlay some considerations which may help **increase** our anonymity, privacy and security online [hereafter generally referred to as *security* – even though the three terms are not identical]. As probably none is fool proof, it is important to not develop a false belief of ever having **complete** security. Even worse might be to implement one or two fundamental measures but overlook others (e.g. using a secure browser & email, but ignoring the copious data your operating system is sending back 'home').

If it is vital that an important message must remain completely secure, perhaps the safest way to deliver it is in person (after, of course, sweeping the room for bugs!).

As with home security, the many precautions needed can easily become overwhelming. You would probably not wish to make your home so secure that it resembles a prison. Likewise, you may not want to become so obsessed with security that your internet activities cease to be enjoyable.

One option, should you happen to have a spare older computer, might be to continue using your everyday computer largely as you do now, but to install a more secure operating system and applications on the second machine. Or, to *dual boot* with two operating systems on a single computer.

This document is not intended to show you how to implement these measures. It is simply a checklist with a very brief overview of some of the options.

Here we are focusing primarily on personal computers. However, smartphone precautions may be similar, with perhaps additional awareness of the tracking capabilities inherent in our mobile phones.

Anonymity vs. Privacy vs. Security

Anonymity

- To be anonymous is to hide or conceal your identity.
- You can be anonymous by preventing online entities from collecting or storing data that could be used to identify you.
- Anonymity also often overlaps with *privacy*.
- Generally, you'd want to be anonymous anytime you're doing something you wouldn't want to be traced back to you.

Privacy

- Privacy is the ability to keep certain data and information about yourself exclusive to you and control who and what has access to it.
- Think of privacy as owning a smartphone—unencrypted and without a password. Everyone around you knows who the phone belongs to, but they don't know what's on it.
- When it comes to online privacy, it's a matter of how much personal information you can keep to yourself.

All information is presented for entertainment purposes only. Use at own risk.

Security

- Security is a set of precautions and measures for protection against potential harm to your person, reputation and files directly or indirectly from malicious parties.
- Security incidents can cause direct harm to their victims. This could be a data breach that compromises passwords and other critical information, or a virus that damages your files and hardware—by turning off your device's cooling fan, for example.
- You need security to protect any type of information that others could use against you, such as private images and financial information.

Useful links:

- https://www.businesstechweekly.com/cybersecurity/data-security/security-privacy/
- https://www.makeuseof.com/privacy-anonymity-security-mean/
- https://www.securityweek.com/cyberspace-anonymity-and-privacy-are-not-same

Operating Systems

Microsoft Windows

- Perhaps the least anonymous or secure.
- In recent versions tracking options are generally switched **on** by default. While many of them can be switched off, a major update may reactivate some of them.

Linux

- Inherently more secure than Windows.
- Open source and free.
- Often faster than Windows on older machines.
- Many varieties are available, but Linux Mint seems to be a popular, user-friendly option for Windows users.

Tails (The Amnesic Incognito Live System)

- Perhaps the ultimate in secure operating systems.
- A very secure Linux version.
- Runs off a live USB or DVD (hence does not replace your existing operating system).
- Connects to the internet exclusively via the *Tor* browser (see below).
- Once removed, leaves no digital footprint on the computer.
- Recommended by Edward Snowden.

Useful Links

- https://linuxmint.com/
- https://linuxhint.com/most-secure-linux-distros-personal-use/
- https://techlog360.com/secure-linux-distributions-privacy-protection/

All information is presented for entertainment purposes only. Use at own risk.

Android

- Herewith a momentary digression to the realm of smart phones running Google's operating system.
- You can easily view all your interactions (from all devices) with Google's services, and check your settings, by going to https://myactivity.google.com/myactivity.
- You might also consider the information listed in the segment entitled *How to Stop Google from Listening on Android*, at https://www.makeuseof.com/tag/stop-google-android-listening/.
- There is at least one seller on Trade Me currently offering refurbished phones that run a "de-googled" version of Android known by the catchy name "/e/". More details are on the E Foundation's website at https://e.foundation/e-os/.
- Another privacy consideration for your smart phone may be to purchase a small protective Faraday bag (currently available on Trade Me for around $10 - $30).

Web Browsers

Google Chrome

- Virtually everything you do in this browser is tracked by default.

Microsoft Edge

- Presumably ditto.

Firefox

- Better, especially if some settings are modified.

Brave

- Blocks adverts, cross-site trackers and cookies by default.
- Has its own search engine.
- Has a *Tor* mode.
- Offers a *VPN* service (not free).

Tor (The Onion Router)

- Probably the ultimate.
- Developed by the US Naval Research Laboratory.
- Directs Internet traffic through a free, worldwide, volunteer overlay network, consisting of more than six thousand relays for concealing a user's location and usage.
- Using Tor makes it more difficult to trace the Internet activity to the user.
- While it may not be possible for your Internet Service Provider to trace your activity, I believe they will likely be aware that you are using Tor. This alone might draw attention?

All information is presented for entertainment purposes only. Use at own risk.

Useful Links

- https://www.bitcatcha.com/blog/most-secure-browser/
- https://nordvpn.com/blog/best-privacy-browser/
- https://www.zdnet.com/article/best-browser-for-privacy/

Email

Overview

- Email security includes the techniques and technologies used to protect email accounts and communications.
- Email is used by virtually everyone online and enables users to communicate quickly, easily, and with a variety of devices.
- Email is therefore the primary target of phishing attacks and can be used to spread malware.
- Emails travel between networks and servers, some vulnerable and unsecured, before landing in an inbox. Even though an individual's computer may be secure from an attacker, the network or server the email has to travel through may have been compromised.
- While hardware and software protection can be effective, sometimes **human gullibility** can undo even the best protection. Often a spammer will, for instance, attempt to panic a user into clicking on a link or malicious attachment. For example, "Unless you access your account by clicking on this link [to a fake bank website] before midnight, your payment of $2500 to Fred Nerks Investments will proceed."
- Email privacy is a broad topic dealing with issues of unauthorized access to, and inspection of, electronic mail, or unauthorized tracking when a user reads an email. This unauthorized access can happen while an email is in transit, as well as when it is stored on email servers, on a user's computer, or when the user reads a message.

Providers

- **Gmail** is by far the most popular email service, with more than 1.5 billion active users. According to Proprivacy.com, Google is a company that holds vast amounts of data about internet users and it is known to scan email subjects and contents.
- **Yahoo Mail** Yahoo Mail is rated by Proprivacy.com as perhaps the most controversial and insecure email provider on their list. Yahoo's reputation was dealt a severe blow in 2016 when it was revealed that the company had provided government snoops with backdoor access to hundreds of millions of user accounts.
- **Outlook.com,** according to Proprivacy.com, is not as invasive as some of the other services but it is still not an email service that can be considered secure. "This shouldn't come as a surprise because Microsoft is known for engaging in high levels of surveillance capitalism – primarily by collecting sizeable amounts of telemetry via the Windows Operating System."
- **ProtonMail** is, however, a secure email service, based in Switzerland which offers end-to-end *encryption* and can be used with the Tor browser.
- **Mailfence** is a similar secure email service, based in Belgium. It also offers end-to-end encryption and *OpenPGP* encryption. [See below for links to ProtonMail and Mailfence].

- Other secure providers which may be worth investigating: Securemyemail, Zoho Mail, Posteo and Mailbox.org.

Encryption

- Encryption is a process which converts original information into unreadable *ciphertext*.
- Encryption and decryption generally uses an encryption key generated by an algorithm. The length of the encryption key is an indicator of the strength of the encryption method.
- **OpenPGP** is the most widely used email encryption standard. It is free.
- An overview of the use of OpenPGP can be found here.

Disposable Email Addresses

- Can be very useful to preserve anonymity when signing up to an email service which requires an already existing email address for verification. Most temporary addresses are removed after a period of time (10 minutes up to a couple of days).
- **EmailOnDeck** offers a very simple two-step temporary online email account service.
- Several other disposable services are listed here.

Two Considerations

1. While apps such as OpenPGP can be used with insecure providers, presumably both sender and recipient must know how, and be willing, to use public and private keys.
2. No matter how secure the sender's email provider, if an unencrypted message is sent to a recipient who is using an insecure provider the message ceases to be confidential.

Useful Links

- https://protonmail.com/
- https://mailfence.com/
- https://www.openpgp.org/

VPN

Overview

- A VPN (Virtual Private Network) creates a secure connection between you and the internet. When you connect to the internet through a VPN, all your data traffic is sent through an encrypted virtual tunnel. This has multiple advantages:
  - You'll be more anonymous on the internet: your real IP address and location will be hidden.
  - You'll be safer on the internet: the encrypted tunnel will keep away hackers and cybercriminals and your device won't be as vulnerable to attacks.
  - You'll be freer on the internet: by using different IP addresses, you'll be able to access websites and online services that would otherwise be blocked.

Security

- The quality & security of VPN services vary considerably. Some, for instance, are free – many are not.
- Some features to consider include a kill switch, multifactor authentication, encryption, no log policy and no unnecessary app permissions.

Accessing a VPN

- Increasingly a number of apps & even browsers (e.g. Opera, ProtonVPN and Avast's SecureLine VPN) are bundling a VPN into their services.
- Again, you generally get what you do (and don't) pay for. Some VPN's, for instance, can considerably slow down your browsing speed. Others offer a very limited number of overseas servers to connect to.

Useful Links

- https://vpnoverview.com/vpn-information/what-is-a-vpn/
- https://techviral.net/how-secure-is-a-vpn/
- https://proprivacy.com/vpn/guides/what-is-vpn-beginners-guide

Further Areas to Consider

Due to the fact that half a dozen pages on these subjects are probably more than enough, I will halt this 'brief summary' now.

However, there are a number of other topics which should be investigated in a more complete overview of anonymity, privacy and security.

Some of those areas are (in no special order):

Browsing in a 'private window'

- Also the importance of emptying your browser's history & cache on closedown when not using a 'private window'.

Social Media Accounts

- Are believed to be closely monitored by 'them'.
- This belief was confirmed very recently by an article in Stuff entitled, "Government hires firm to monitor New Zealanders' social media to inform Covid-19 response".

Anonymous Proxy Servers

- Your ISP will be able to see that you have connected to an online proxy, but probably not where you went beyond that connection.

Firewalls

- Optimum security settings.

Internet of Things

- Is your smart TV really listening to you?

Webcams

- Apparently even the head of the FBI and Mark Zuckerberg both put tape over their webcams.

Photos

- Is everyone aware of the many *EXIF* (Exchangeable Image File format) privacy details likely to be included their digital photos (such as location, date and time) and how to remove them before uploading?

Public vs. Private Wi-Fi

- Possible risks of connecting via public Wi-Fi in places such as coffee shops.

Index.dat file

- A hidden Windows file containing records of your online and some local activities.
- How to remove the information in *index.dat*.

Secure deletion of Sensitive Files

- Deleting from the Recycle bin does **not** erase a file.
- To effectively do so, a file generally needs to be overwritten a number of times.
- This can be achieved with a number of security and maintenance applications, such as Glary Utilities

Anti-virus

- Importance of effectively using an anti-virus program.
- Dangers of malicious software such as key-logging & network-aware infections.

Webcam Surveillance

- Is your webcam secretly watching you?
- Which applications in your Windows settings are allowed to access your webcam?

Passwords

- The importance of using a variety of secure passwords & not using the same password for everything
- A moderately long sentence can make remembering passwords easier, and is not easily cracked e.g. *vaccinesaresafeandeffective*.

All information is presented for entertainment purposes only. Use at own risk.

- A free security app, such as KeePass Password Safe, can be used to (securely) record multiple passwords.

Purchase & Payment Anonymity

- EFTPOS vs. cash vs. crypto.
- Cash is king – but becoming less & less accepted.
- EFTPOS - records name, location, date & time, amount spent etc.
- Crypto – has become primarily a means of speculation rather than trading? 'Mining' can require **huge** amounts of electricity (According to an article in The New York Times, "Bitcoin uses more electricity than some countries"). Inaccessible when internet off.

____

All information is presented for entertainment purposes only. Use at own risk.