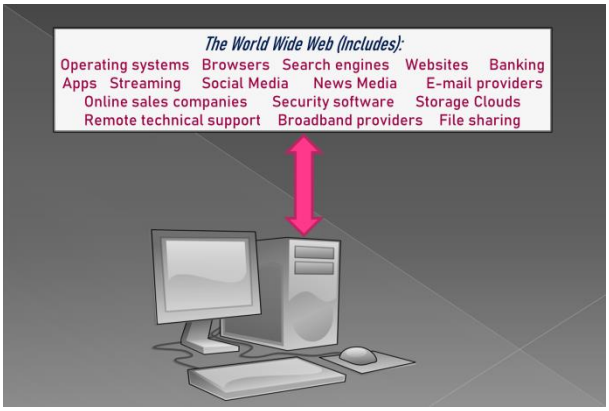
RNIOA Article 15 [17/05/2020]

# Digital Safety & Security

Lt Cdr Mike Rose RN ©

## Introduction

Prior to the introduction of the internet, personal computers for home use were self-contained in that the operating system was bought and installed by the supplier/user, and external communications using the PC were not yet technically developed. The most likely risk therefore was the possibility of someone switching on unattended, non-password-protected computers and copying sensitive information onto an external memory device. Essentially, users were in control of their computing equipment and paid real money for the services and software they used to a known vendor.




With the introduction of the internet, however, the issues of 'payment for services' and external software connections (often hundreds and to 'unknown' destinations) to our PCs and other devices have introduced numerous risks, as well as benefits, that can overwhelm the average user, including those who have high levels of IT skill and competence. The rapid expansion of so-called 'free services' also challenges the economics principle of Adam Smith that 'there is no such thing as a free lunch.' The 'mirage' of free services provided is therefore the 'elephant in the room,' with economic benefits being accrued by providers by means of targeted advertising, which requires the known or unknown acquisition of users' personal characteristics linked to their IP address to enable 'tracking.' Where internet-based criminality is involved, the acquisition of banking and credit card data is often the main objective.

The aim of this article is to help people understand the risks they face and how to attempt to mitigate them. So, whether you're accessing the internet with your mobile phone, PC, tablet or laptop, you're potentially exposed to every hacker, digital thief and spammer across the globe. Not to mention that viruses, trojan horses, spyware and adware are always just one click away. You wouldn't drive without insurance, a seat belt and a GPS device, so, similarly, when you "surf the net", you need to make sure that you are well "buckled up" and well-informed. This article is written as a guide to "safe surfing" and is just as important for personal users as it is for large tech companies.

## Malicious websites

Spyware, which is software that steals your sensitive data without consent, lurks in many corners of the internet; often in places where you'd least expect it. All it takes is to be in the wrong place at the wrong time to compromise your digital safety. Let's set the scene:

- You open your web browser and start surfing;
- Curiosity takes you to a new, interesting site and then one of the following may happen:
    1. A pop-up appears, and you click on it - even just to close it;
    2. You click on a link which falsely claims to take you to a site you are wishing to access;
    3. You click on a graphic to enlarge it;

You may have unknowingly fallen into a spyware trap. Software is downloaded onto your device and a digital "spy" is installed. Your personal information is now at risk.

Sometimes, simply opening a web page can initiate an undesired installation.

## Malicious E-mails/Messages

Let's set another scene:

- You open an e-mail that seems innocuous (if it is an HTML email, you already could be in trouble) and then you click on a link or document or image within the email;
- The HTML email starts an installation – a virus or spyware is downloaded to your device without your knowledge;
- Your device is infected and your personal information may well be at risk without safeguards.

## How do I know if I have been affected?

The effects or symptoms of viruses or spyware include: stealing sensitive information such as credit card numbers, usernames and passwords, directing your browser to suspect sites, changing or deleting your files, pestering you with endless pop-ups, and slowing down your device.

Internet safety can be deceiving. Seemingly reputable sites may contain spyware traps, or the sites themselves may be counterfeit - "phishing" sites posing as the real thing. The path away from internet safety often begins innocently enough; however, certain sites are more prone to be sources of spyware, including:

- Adult sites
- File sharing sites
- Social networking sites

## Recommendations

1) Avoid questionable websites, and avoid websites that contain "flash" elements, since this (old) software can be a source of malware. Your browser should either warn you if a site contains flash, or block you altogether.

2) Only download software from sites you trust and carefully evaluate free software and file-sharing applications before downloading them.

3) Update your operating system regularly (often done automatically by the principal providers). There are still many companies around the world using older versions of operating systems and are therefore extremely vulnerable to hacker attacks and viruses.

4) Increase your browser security settings, for example: block "tracking", automatically delete cookies and cache data after each session, avoid a "master password", block pop-ups, prevent sites adding "add-ons" to your browser without your approval, prevent accessibility services from accessing your browser, don't automatically send usage data, block dangerous content, block camera access, block certificate requests, etc.

5) When you visit a company's website, it's always better to type it into the address bar of your browser, or use a bookmark (more efficient), instead of clicking on a link which you find in an email or text message.

6) Make sure that you have reputable and reliable security products installed on all your devices:

- Antivirus protection (and scan your device regularly). You don't need to pay a lot for protection, in fact many are free for personal use, such as **AVG,** but it's important always to read the terms and conditions.
- Firewall (Windows includes one, so you can simply enable it).
- Antispyware/adware software (and scan your device regularly). Not all antivirus software scans for spyware or adware. You don't need to pay a lot for protection; in fact, many are free for personal use, such as **ADW Cleaner.**
- VPN (Virtual Private Network). This is particularly important if you regularly use free WiFi in restaurants, airports and other establishments. It's invaluable as free WiFi networks are notoriously risky (others can "observe" what you are doing). Another

advantage is the freedom of web surfing away from the prying eyes of big companies and governments - a VPN service doesn't allow advertising entities to know where you are or what you're doing – you, with some degree of confidence, have absolute privacy. However, some VPN providers, theoretically, can trace your true location and pass on data about you and what you do on the internet, but all providers claim that they do none of these things. So, before you pay for such a service, make sure you trust the provider. The Opera browser comes with a free (limited) VPN service built-in, so research similar deals. You may also wish to install an "ad blocker" to your browser.

7) Always use strong passwords (maybe consider using a password generator) and avoid a single (master) password. If you need to store your passwords somewhere, store them off-line, preferably not on your device and change them regularly. If you want to keep them on your device in a single document password-protect and/or encrypt the document.

8) Always password-protect your device access, as you never know who could use it in your absence.

9) Never pass on or tell anyone your password(s). If you ever forget a password to a website, it is usually possible to set a new one by clicking on a link such as "Forgot/Reset my password".

10) When you install software, always read every step of the installation carefully. Sometimes spyware or adware comes piggy-backed on the downloaded software. Select "No" or "Skip" on the options to install secondary applications.

11) When you make an on-line purchase, it is little effort to type in your credit card details, so consider carfefully whether you need to store those details on the company's website/database. Such information is often sought after by cyber criminals.

12) If you need technical assistance, it is advised not to allow someone to take remote control of your device unless you trust them, since it would be feasible for them to install malicious software or steal your personal information. There have also been many cases of customers being charged exhorbitant fees for services provided remotely which weren't even necessary.

## Open source software

There is an ever-growing international community of open source software programmers, designers, advocates and supporters. Consequently, there is already an immense library of such software available, so much so, that it is easily possible to have a fully-functional personal electronic device with no paid software at all. Open source alternatives are usually as robust and secure as expensive programs. Here are some examples:

a) Operating systems: **Unix**, **Linux**. There are many versions of Linux available, and several of them are nearly identical to MS Windows in their usability. Currently, there are virtually no viruses which can attack Unix or Linux, so simply switching your device to one of these operating systems would already be an enormous step in the "safe" direction (although a little programming knowledge is needed to migrate to this potentially safer option).

b) Browsers: **Tor**, **Firefox**.

c) Search engines: **Duck Duck Go** (which states it has no tracking, no cookies, no history).

d) VPN: **OpenVPN**, **Libreswan VPN**, **SoftEther VPN**, **Openswan VPN**, **Freelan VPN, ProtonVPN**

e) Office software: **Open Office**, **Libre Office** (both of these provide near-identical functionality to the MS Office suite of applications, and work largely seamlessly with MS Office documents).

f) Image editing software: **GIMP**, **Krita**, **Pinta** (these provide functionality that may well rival the best of paid programs such as PhotoShop).

g) FTP client: **FileZilla**

## Android and Apple apps

You should only download apps from the official Android and Apple app stores. Even so, some apps can bombard you with ads, demand money after a free trial period, and may require access to your contacts, images etc. These are often undesirable consequences. If in doubt, delete an app and look for another, similar one.

## Wi-Fi routers

Many households have a Wi-Fi hub/router although most routers are simply switched on and never configured securely. You should change the default access password for "root" (the master user) and (ideally) regularly check who is connected to it. Access to the router is made through a browser, usually using an address such as "http://192.168.100.1/".

## HTTPS (Secure websites)

The entire web is gradually leaving HTTP behind and switching to HTTPS. The "S" in HTTPS stands for "Secure". It's the secure version of data transfer between computers on the internet. When your web browser communicates with websites, HTTPS ensures a much more secure and private connection. So, when you visit a company's website, and it is not using HTTPS technology, you may want to reconsider and seek out another company, particularly if you intend to share sensitive or financial data with that company. Most reputable companies have already switched. Most browsers show an image of a padlock with a red line through it next to the web address, if a website is HTTP, and not HTTPS. Although the RNIOA website is not currently using HTTPS technology, we take great care to ensure the privacy and security of our contributors' data, with no login or payment data issues.

## Conclusion

If all this seems complicated and difficult, then you may be tempted to ignore it and continue as you are ("I've been surfing for years without any problems, so why should I do anything differently?"). One useful option would be to ask a friend or colleague with good IT knowledge to assess your device for risks, and change your configurations and/or installations as required.

One final issue of immense importance is that of **backups.** Having worked with IT for around 30 years, I have witnessed many regrets on this issue. A computer hard disk crashes, a power supply blows, a CDROM gets scratched, or a pendrive is suddenly unreadable – this is no problem if you have a backup, but a potentially giant headache if not. Backups are often forgotten until it's too late. Try to develop the habit of making at least one copy of your important files on a regular basis – daily, weekly or monthly. Many choose to automatically backup their files to "the cloud". This is fine, but be aware that the cloud is external to your device and potentially vulnerable to hackers, so avoid uploading sensitive or financial data to cloud backup environments.

As illustrated in this brief article, devices which access the internet are no longer simply "useful" or "fun", they offer many opportunities for abuse which can have serious consequences. So, surf cautiously and carefully, and have safe fun!

## Acknowledgements:

I would like to express my thanks to the Editor of the RNIOA, John Nixon, for his helpful comments and suggestions.

## Disclaimer

The information provided in this article is for general advice only, based on the extensive personal experience of the author. Neither the author nor the RNIOA endorse any products that are mentioned – readers should undertake their own research to determine actual products to use.