How to Stay Safe Online

By James A. Cruickshank

Computers and Integration SCIO

4 St James's Place, Inverurie, Aberdeenshire, AB51 3UB

Charity No. SC010617

Contents

Preface

The Web is an extremely useful application of the Internet. You can obtain information, catch up on TV programmes, get the latest news headlines and much more. Unfortunately, cyber criminals use the Web to steal your personal information such as debit card and credit card details. This means that staying safe online is a constant challenge.

This book is divided into 12 chapters and each chapter deals with a separate aspect of staying safe online.

This book will help and encourage you to:

- Protect your privacy
- Secure your log-in details, debit card and bank account details
- Choose strong passwords
- Hide your Facebook profile from strangers
- Surf the Web with a secure Web browser
- Scan your computer for malicious software
- Keep your anti-virus software up-to-date
- Stay clear of software that spies on you
- Prevent the installation of malicious software or Trojans
- Prevent bad guys from taking over your computer
- Stay clear of fake security software

Chapter 1 — Protect your privacy with CCleaner

If you want to easily delete traces of your Internet activity from prying eyes, you can download a free tool called CCleaner.

To obtain a copy of CCleaner:

Step 1. Using your chosen web browser, from the address bar, type in: www.piriform/ccleaner and then hit Enter.

Step 2. From the “CCleaner” page, click “Download”.

Step 3. Click “Download” again.

Step 4. Click “Run” when prompted.

Chapter 2 — Secure your log-in details with Trusteer Rapport

Malicious software and phishing (or trick) e-mails allow cyber criminals to access your computer, account numbers and personal information. And moreover, it can take days or even weeks for antivirus software to detect the presence of such software.

Financial malware is constantly evolving to evade antivirus solutions. However, Trusteer Rapport prevents malware from getting access to your personal information. It is basically a browser add-on that sits next to the address bar and changes colour to let you know it's working.

Banks and building societies use Trusteer Rapport to secure the log-in details of their customers.

You can download Trusteer Rapport from https://www.trusteer.com/ProtectYourMoney.

A good rule of thumb is to use Trusteer Rapport for each and every website you log into to protect your log-in credentials.

Chapter 3 — Protect your bank details with Paypal and shop online securely

When you shop online, you should use Paypal as your method of payment since it prevents you from having to hand over your debit or credit card details to websites. Certainly, Paypal is supported as a method of payment by a wide range of websites, including Argos and you can pay using just an e-mail address and password.

Chapter 4 — Choose strong passwords and protect your online accounts

Passwords are an important part of your online life. They help to keep your personal details safe. As such, it's important that you choose good, strong passwords that nobody can guess.

To create good passwords:

Do not

- Do not pick passwords which someone that knows you can easily guess, such as nicknames or the names of your pets.
- Do not pick passwords based on words you find in a standard dictionary.
- Do not use the same password across lots of different websites.

Do

- Do pick one password and add a few letters to the start of it related to each site your logging into.
- Do pick a phrase that helps you to remember your password.
- Do try to include some numbers and special characters in your password to make life hard for a criminal.

Chapter 5 — Hide your Facebook profile from strangers

Facebook is a very popular website with over a billion users. As such, you've probably already heard of Facebook. But in case you haven't heard of it, Facebook is a website that makes it easy for you to keep in touch with friends and family. To put it another way, Facebook enables you to chat with the people you care about and share all the moments in your life, good and bad.

That said, while Facebook allows communication to thrive, it also has a very public aspect. This means that if you happen to have a "profile" page on Facebook, you may be sharing your personal information with strangers. This is because when you share something on Facebook, you are sharing it with the world by default, unless you change your "Privacy Settings".

Clearly, this is very dangerous, especially since identity fraud is the fastest growing crime. So, to reduce the risk of someone stealing your identity via Facebook, you should only share your personal information with people you trust.

Only share content with "friends"

A good rule of thumb for staying safe on Facebook is to just share content with those individuals you designate as "friends". Certainly, this is easily achieved. Just set your "Privacy Settings", and everything that appears on your profile page, to "Friends".

Chapter 6 — Surf the Web with Avast SafeZone Browser

Avast SafeZone browser is the best web browser to use if you want to stay safe online. Basically, it gives you an extra layer of protection since it prevents rogue programs from running on your computer.

Avast SafeZone browser comes with the popular Avast! Free Antivirus software.

To obtain a copy of Avast! Free Antivirus:

Step 1. Using your chosen web browser, from the address bar, type in: www.ninite.com and then hit Enter.

Step 2. From the “Install and Update All Your Programs at Once” screen, look under “Security”, then select “Avast”.

Step 3. Click “Get Installer” when you’re ready to setup your new security software.

Step 4. Click “Run” when prompted.

Chapter 7 — Scan your computer for malicious software with Malwarebytes

Every so often you should scan your computer for malicious software, or malware, using Malwarebytes AntiMalware. This is to rid your computer of malicious software.

To download Malwarebytes AntiMalware:

Step 1. Using your chosen web browser, from the address bar, type in: www.ninite.com and then hit Enter.

Step 2. From the “Install and Update All Your Programs at Once” screen, look under “Security”, then select “Malwarebytes”.

Step 3. Click “Get Installer” when you’re ready to setup your new security software.

Step 4. Click “Run” when prompted.

To run Malwarebytes AntiMalware:

Step 1. From the main Malwarebytes AntiMalware screen, select “Perform full scan”.

Step 2. Click “Scan”.

Chapter 8 — Keep your anti-virus software up-to-date

Viruses are hidden pieces of software that wreak havoc and they are quite common threats to computers.

They tend to be transmitted via websites, e-mail attachments and removable media devices, such as USB flash drives. They hide in files and spread from computer to computer, generally wreaking havoc.

To reduce the risk of your computer becoming infected with a virus:

- Keep your anti-virus software up-to-date.
- Scan your computer for viruses once a week.
- Keep Windows, and the other software applications you use, up-to-date. Viruses often exploit security holes in your computer so that they can run without your knowledge.

Chapter 9 — Stay clear of software that spies on you

Spyware is software that spies on your online behaviour. Its main goal is typically to steal sensitive information from you, such as your credit card number or your bank account details.

Spyware is often hidden in software applications you download.

To reduce the risk of your computer having spyware on it:

- Only download software from trusted websites, such as www.download.com.
- Keep your anti-virus and anti-spyware software up-to-date.
- Scan your computer for viruses and spyware once a week.

Chapter 10 — Don’t install malicious software or Trojans

Trojans are software applications that pretend to do something useful, but in reality they do something devious.

They are quite dangerous as they often hide within files that look harmless, aiming to trick you into installing malicious software on your computer.

To reduce the risk of installing a Trojan (horse) on your computer:

- Only download software for your computer from trusted websites, such as www.download.com.
- Only click on e-mail attachments you’re expecting.
- When you receive an e-mail from a colleague or friend that insists you launch a file, first check with them what the file is. If you can’t check, delete the e-mail.
- Don’t ever click on an e-mail attachment that ends in .bat, .com, .exe, .pif, .scr and .vbs.
- Be especially wary of an e-mail with a zip file attached. As a precaution, always scan zip files with your anti-virus software before you open them.

Chapter 11 — Don’t let bad guys take over your computer

Worms are a nasty net borne disease. They spread from computer-to-computer without the intervention of people. And they are often used by bad guys to send junk mail from your computer without your knowledge.

To reduce the risk of your computer becoming infected with a worm, you should check and make sure that the Windows Firewall is turned on. If it’s turned off for some reason, you should definitely turn it on.

The Windows Firewall is part of Windows and its aim is to block people, or worms, that you don’t want entering your computer.

Chapter 12 — Stay clear of fake security software

Fake security software, or scareware as its known, is becoming a growing problem. This is mainly because it's deliberately designed to look like anti-virus software from well-known software providers.

Basically, scareware is designed to trick you into believing that your computer is infected with nasty software. Its main goal is to con you into buying software to clean up your computer.

Scareware is often delivered via the Web, and you can easily avoid downloading it.

To avoid being tricked by scareware: don't believe websites that tell you that your computer is infected with lots of viruses.