SECURITY IN THE DIGITAL WORLD
For the home user, parent, consumer and home office
Graham Day
Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publisher and the author cannot accept responsibility for any errors or omissions, however caused. Any opinions expressed in this book are those of the author, not the publisher. Websites identified are for reference only, not endorsement, and any website visits are at the reader’s own risk. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the publisher or the author.

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form, or by any means, with the prior permission in writing of the publisher or, in the case of reprographic reproduction, in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publisher at the following address:

IT Governance Publishing
IT Governance Limited
Unit 3, Clive Court
Bartholomew’s Walk
Cambridgeshire Business Park
Ely, Cambridgeshire
CB7 4EA
United Kingdom
www.itgovernance.co.uk

© Graham Day 2017

The author has asserted the rights of the author under the Copyright, Designs and Patents Act, 1988, to be identified as the author of this work.

First published in the United Kingdom in 2017
by IT Governance Publishing.

ISBN 978-1-84928-xxx-x

This extract and the publication it is taken from are both subject to ITGP copyright and may not be reproduced, in any form, without any prior written consent from the publisher.
DEDICATION

Sincerest acknowledgement to my wife Brenda - my chief researcher - without whom this 'home project' would never have been released with the hope of informing and enabling others to be information security aware in this digital age.
PREFACE

The Internet and digital technology are the future; they are invaluable resources to be grasped and explored by all. The aim of this book is to empower people to surf safer online and manage their digital presence by being aware of how they might be attacked, how attackers may try to manipulate them or how their information might be at risk.
ACKNOWLEDGEMENTS

I would like to thank Chris Evans, Christopher Wright, Giuseppe G. Zorzino and Maarten Souw for their helpful comments during the review process.
ABOUT THE AUTHOR

Graham Day spent 24 years in the military, including more than a decade as a counter intelligence and security specialist on operational deployments around the globe.

Since retiring from the military, Graham has provided a range of services as a consultant, including, but not limited to, information security, cyber security, business continuity, cyber risk and cyber resilience.

He is currently working as a senior standards analyst for Equinix Ireland, responsible for compliance and instigation of best practice in security, business continuity, data protection and quality management.

Graham is a CESG Certified Professional Security Information Risk Advisor, a Certified Information Systems Security Professional and a member of the Author Group for British Standard 31111 Cyber Risk & Resilience.
CONTENTS

Introduction ............................................................................................................. 12
Personal digital security top ten ................................................................. 14
Chapter 1: The Internet...................................................................................... 18
  1.1 Connecting.................................................................................................. 18
  1.2 Browsers .................................................................................................... 19
  1.3 Browser history .......................................................................................... 21
  1.4 Tabs ............................................................................................................. 23
  1.5 Search engine ............................................................................................. 24
  1.6 McAfee WebAdvisor .................................................................................. 26
  1.7 Spam filter .................................................................................................. 27
  1.8 Ad blocker .................................................................................................. 27
  1.9 Cookies ......................................................................................................... 28
  1.10 Email ........................................................................................................... 29
  1.11 iCloud ....................................................................................................... 31
Chapter 2: The threats ...................................................................................... 32
  2.1 Cyber crime ................................................................................................ 32
  2.2 The who? .................................................................................................... 32
  2.3 The why ..................................................................................................... 38
  2.4 The where .................................................................................................. 40
Chapter 3: The how ............................................................................................. 42
  3.1 Social engineering ....................................................................................... 44
  3.2 Malware ...................................................................................................... 64
  3.3 Ransomware ............................................................................................... 76
  3.4 Trends ......................................................................................................... 80
  3.5 Summary ..................................................................................................... 88
Chapter 4: Operating system – computers and laptops ........................................ 90
  4.1 MacOS ........................................................................................................ 90
  4.2 Windows .................................................................................................... 95

This extract and the publication it is taken from are both subject to ITGP copyright and may not be reproduced, in any form, without any prior written consent from the publisher.
INTRODUCTION

When you lock your home at night you feel secure, confident that no attacker can get into your home without being detected. When you connect to the Internet that changes, you are creating a path for attackers to get into your home, your safe place, your sanctuary.

This book started as a project to help family and friends navigate the Internet safely and have some control of their digital presence. As an information and cyber security professional I continually support international companies in preventing attacks and managing incidents, but I am also very conscious that there is no single resource for the public.

As my personal project developed it was suggested there was too much helpful guidance and advice to not share outside the family. It is my hope that this book helps everyone prevent an attack or manage their online presence; if it does that for just one person then I will be very happy.

It is not my mission to change the world, but I would like to empower everybody to understand the threats and develop the culture to manage their digital presence.

The main caveat is that the information in this book is as good as the day it is written. Since that day there will have been new attacks and also possibly some changes to the actions you need to perform on your devices to be safer online.
Introduction

Technology and threats are ever-evolving, use the information in this book as a baseline, then stay on top of updates, patches and safety settings to manage the risk of becoming a victim of an attack, or having your information used against you.

This book does not suggest companies are irresponsible, failing to protect their customers, or keeping their customers oblivious to the risks and threats to technologies, such as contactless cards. As a user I see various notices and warnings that businesses provide, but I am conscious that there is no single resource that explains how, why and what to do about them, which is what I have tried to create.

There are three things an attack needs: a means, a method and a motive. The means is the Internet or your device, the method is generally social engineering or malware, and the motive is your personal, financial or even work information.

I will go through who may be launching these attacks, as well as why, where and how.

I will also cover some things you can do to your device, the way you do things online, how you use technology and how you conduct yourself – all to protect yourself.

Unless you want to lock yourself away from society at large there is no gold-plated solution to staying safe, but lots of little things will combine into a better security posture and approach, a security blanket in effect that will cover you and give you some protection, that will hopefully help you be more aware and stay safe.

Safe surfing!
PERSONAL DIGITAL SECURITY TOP TEN

The juicy stuff first: here are the top ten things that can be done to put some personal or home cyber security in place. Some of these may already have been done, but there’s no harm in being reminded. These are not in any specific order, but together they will give you a secure foundation;

1. Configure the ‘platform’ – or ‘secure your device’
   - Apply security settings in device config (see section 4.1)
   - Install anti-malware applications (see Chapter 4)
   - Schedule updates and patches (see section 5.1)

2. Manage your accounts
   - Use passphrases or difficult passwords (see section 5.1)
   - Use different security info for different accounts (see section 5.1) and multi-factor authentication whenever it is available (see section 5.1)
   - Do not share your security info (see section 5.1)

3. Have a private life
   - Do not post your personal or private information online (see section 3.1)
Personal digital security top ten

Do not post plans online, these could reveal a time when your home or you could be attacked (see section 3.1)
Do not be afraid to ask friends to take down posts about you, or that you are tagged in (see section 3.1)

4. Be security aware

Check the identification of senders of information, requests and callers (see section 3.1)
Challenge requests of callers if you have any doubts (see section 3.1)
Confirm the request is genuine with the company or organisation (see section 3.1)

5. Manage your information

Only entrust your information with providers you trust (see Chapter 8)
Regularly check your credit rating (see section 3.2)
Regularly search your own name online, as well as the names of your family (see section 3.2)

6. Build a secure web browser – configure your browser

Configure spam and ad blockers (see section 1.8)
Install an Internet security application (see Chapter 1)
Install a virtual private network (VPN) for mobile security (see section 6.3)
Personal digital security top ten

7. Manage the home network and Internet of Things

Change default passwords on devices (see section 10.1)
Configure network security applications (see section 5.1)
Regularly change the network passphrase (see section 5.1)

8. Shop clever

Check the security credentials of the site (see section 8.1)
Don’t save credit/debit card details on websites (see section 8.2)
Use different browsers for different tasks (see section 1.4)

9. Security does not stand still

Regularly review your security (see section 3.2)
Take action if you notice anything different in your online presence or profile (see section 3.2)
Ask friends to inform you if they see anything online about you or that you need to know (see Chapter 11)

10. Think twice, click once

Do not commit to anything online until you have considered it and the impact on you (see section 12.1)
Personal digital security top ten

Do not take everything at face value as it only takes a minute to check (see section 12.1)
Once all points have been considered, reconsider before you act – think before you click! (see section 12.1)

Remember the ‘five Ps’: Platform (secure device), Patches (and updates), Passwords, Privacy and Phishing.
 CHAPTER 1: THE INTERNET

When you use the Internet you are potentially creating a path for an attacker to get into your personal space, or to get your information. There are security controls you can put in place and also a few key behaviours for using the Internet that will better protect your information.

1.1 Connecting

The first thing to do for the internet is secure the connection. The ways to connect to the internet are introduced here as it is logical to understand this before you connect, but they are explained in greater detail in later sections.

Home networks (section 5.1) – this connection is secured by the home network encryption (section 5.1) and secured by password or passphrase (section 5.1).

Mobile network (section 6.3) – this connection is generally used when you are mobile. This connection should be secured with a VPN (section 6.3) if you are accessing important information or using your payment card.

Public wi-fi (section 6.2) – this connection should be used whenever you are in a public place and using provided wi-fi. For example, airports, trains, buses, coffee shops, restaurants, etc. This connection is secured through a VPN.

Note. A VPN is a Virtual Private Network, it is a secure channel created between you and the target website.
1.2 Browsers

There are a number of browsers available that you can use to search the Internet. Each browser has a different profile, how well it integrates with search engines, how fast it responds to requests, what features are built in, how fast it takes to reload, how quickly it downloads, etc. Below are some of the more popular free browsers.

**Mozilla Firefox**

Mozilla Firefox has been around for a number of years but has never been a front-runner. The issues with Microsoft Internet Explorer have, however, led to an increase in the use of Firefox as a default browser.

Mozilla Firefox can be customised to your requirements, is fast and secure, and protects your privacy.

**Google Chrome**

Google Chrome is inarguably the most widely used browser, with a 60% share of the market. It is unique in that it applies a single sign-on managing a number of Cloud-based personal applications, including Gmail (email), a calendar and personal notes. Google Chrome is also an advanced browser in the way security is applied, using two-factor authentication through a person’s smartphone. Google Chrome is regularly updated.

Google Chrome is a fast browser but is not the quickest. It has strong security features and a very simple interface, and other features are available and easily installed.
1: The Internet

**Opera**
This browser has a built-in VPN (see section 6.3 to understand the advantages of this), an ad blocker and a battery saver mode.

**Microsoft Edge**
This is the new browser from Microsoft that has been issued from Windows 10 onwards. It has a good interface, offers good security and supports extensions that can increase the number of functions.

**Vivaldi**
This browser is fully customisable, fast and ‘fun’ to use, although it lacks the features of other browsers.

**Internet Explorer**
This is probably the most widely known Internet browser, but some versions may cause unnecessary risk to home users. The latest versions of Internet Explorer – IE10 and IE11 – remain supported, but any new Windows operating systems will be released with Microsoft Edge, or any later browser Microsoft creates.

**Supported or not supported – what does it mean?**
If a browser is supported it means the developer will issue updates to fix vulnerabilities. If a browser is not supported, no updates will be issued. Whether a browser is supported is very important to the user’s security.

✔ Regularly check the security of your browser. Make sure updates are applied.
Look at the settings in your browser. If necessary, research the settings and apply them to make your browser as secure as possible.

1.3 Browser history

One thing you can do to protect yourself online, especially when you are using a public or shared computer, is to delete your browser history. There are two ways to do this:

**Permanently** – this is done in the ‘Settings’ or ‘Options’. Within this menu there will be an option to ‘Clear browsing data’ when you close the browser. Within the ‘Clear browsing data’ menu there will also be options to clear cookies, cache and other groups such as download history and even stored passwords. All of these things should be selected for as far back as possible; some browsers may offer to do this for a certain period of time, be it hours, days or weeks, or ‘from the beginning of time’.

**Session**, when closing the browser – as well as the permanent option in the browser ‘Settings’ or ‘Option’s menu, there will be a ‘History’ tab that will allow you to clear the session browsing history. This will only clear the browsing history and is not nearly as effective as the permanent option.
1: The Internet

1. To clear your browsing history in Google Chrome go to the browser menu and select ‘Settings’ (3 vertical dots)

2. To clear history, go to ‘Clear browsing data’
3. Make sure you select ‘the beginning of time’ for all options and click ‘CLEAR BROWSING DATA’ as shown above.

1.4 Tabs
Many browsers allow you to open multiple tabs in a session, but this can create a chance for an attacker to get sensitive information. If an attacker has got access to your internet session, then they could potentially access all tabs you have open (a session is from when you open the internet browser until you close it).

Social networking sites are a preferred way for attackers to get access to your online session. By not doing your online banking in the same session as having a social networking site open there is less possibility the online banking session will be compromised or breached.

There are a few things you can do to prevent this.

✔️ Have a browser that you only use to access sites where sensitive information will be used.
1: The Internet

☑ Have a different browser for searches and other general web access, such as Facebook.
☑ If you find an item to buy during a search, open the link to the chosen item in a new window to buy it, closing the first window before buying.
☒ Do not open sensitive sites in the same session as general access, such as searches or Facebook.

One thing you could do is have multiple browsers. For example, you could have three browsers available on your system:

1. One to access sensitive information, such as banks, medical, social, shopping, etc.
2. One to manage your professional profile, email, LinkedIn, etc.
3. One for general things such as searches and to access your social network, Facebook, etc.

1.5 Search engine

There are a number of search engines available, with five introduced below. These five are considered the primary search engines. Each of these search engines are free to use.

As a rule, search engines are financed by advertising. Search engines will return sponsored pages as the initial results of your search, then return the results that appear to be most closely associated with your search topic or feature keywords from your search. There are a number of risks with search engines, with the main one being that you trust the search engine to return genuine and safe results. The
search engine’s results are based on topic and/or keywords, so it is possible that the primary results are laden with malware or misinformation but have been built with keywords featured in common searches.

The main way to protect yourself from potentially malicious websites that exploit search engine algorithms is to be very conscious of the risk that many search terms will return results that may have malware in them, and if you go to the page there is a real risk that your system could be infected. People who want to implant this malware in your system or device will be very aware of the common search topics and will build sites that will be returned as results. They hope that you visit their site so they can infect your system or device, then their malware can change your system, give them access to your system or just bombard you with spam. When you view results, be very careful of the sponsored results that are usually very near the top and those that are not clearly related to your search term.

Another option is to use a search filter or McAfee WebAdvisor (section 1.6), and there are also add-ons for browsers such as Google and Firefox.

**Google.com**

Google has the largest catalogue of web pages available, and it is fast and relevant. Google also has excellent extra features to filter for images, news, maps and more.

**Duckduckgo.com**

Duckduckgo has some very good features, such as the ‘zero click’ information where all your responses are found on the first page. Duckduckgo is a clean, fast and efficient
search engine that also offers prompts to help clarify the question you are asking and has less ad spam than most search engines.

**Bing.com**

Bing is regarded as the second most popular search engine. Until 2009, Bing was known as MSN Search. Bing tries to help you with your search by offering suggestions and gives you various search options.

**Dogpile.com**

Dogpile is a search engine with a quick, clean presentation, a growing index of web pages and helpful cross-link results.

**Yippy.com**

Yippy is a ‘deep web’ search engine: it searches other search engines. If you are searching for obscure material, Yippy is the best option.

**1.6 McAfee WebAdvisor**

McAfee WebAdvisor – previously SiteAdvisor – is an effective tool for protecting users from the ‘dark’ side of the Internet. WebAdvisor is a free to download and use Internet filter and protection application. There are four features in WebAdvisor that McAfee says on its website (www.mcafee.com) do the following:

1. Misclick protection – blocks phishing and malware sites if you click a link.
2. Typo protection – protects you if you incorrectly type a web address, and reportedly “points you in the right direction”.
3. Safer downloads – scans your downloads and tells you if there is a “known risk”.
4. Security check – checks your antivirus and firewall are turned on before you access the Internet.

1.7 Spam filter

A spam filter is an email feature that blocks unwanted spam emails from a user’s inbox. Spam filters work by looking at the origin of an email, the signatures in the email and even the content. There are certain types of origin addresses associated with spam emails: this is the first filter. The second filter is the signatures: spam will have common types of signatures in their properties that the filter will identify and block. The third filter is the content: spam emails are created by applications that send emails to millions of addresses at the same time, and these applications use a common type of language that filters can recognise and block.

There is no guarantee that spam filters will be 100% effective but they will help you manage the types of emails that are received in your inbox. The ideal spam filter will be the filter designed to work with whichever email provider you are using, e.g. Gmail or Outlook.

1.8 Ad blocker

An ad blocker is a software tool that removes advertising content from a website, a web page or even a mobile app.
There are plenty of commercially available ad blockers, including an extension for Google Chrome, plus there are some available free from filehippo.com as discussed in section 4.2.

There is no guarantee that the ad blocker will be 100% effective, but it will block the majority of ads, and help you manage the information sent to your inbox, as well as ads which appear when you are surfing the Internet.

1.9 Cookies

Cookies are little bits of information that websites store on your computer about your visit to their website. For example, a grocery retailer will save cookies when you browse their store. The cookies will tell them what you looked at in the store, and even if there is a particular item that you looked at more than once. The cookies will also tell them if you revisit the store, and what you looked at during your next visit. The retailer will collect all this information and analyse it. If you have an account with the retailer, they will probably send you marketing or even offers for the items you looked at most often. The retailer is banking that if they can get you to do your shopping with them by giving you the targeted offers, based on the cookies collected from your previous visits, you will spend more money in the store than just for the offers.

The retailer will also be able to analyse the cookies from a greater number of people, which can be used to manage its stores and stocks more efficiently. For example, the retailer could work out what brand or type of products are likely to sell in certain areas or regions in comparison to other
products. By working out this information, the retailer can order stock appropriately, but more importantly not order stock that is not going to sell in the area or region.

The retailer can even work out what women buy more than men, what men are looking for before Valentine’s Day, and what products or types of product certain age groups will buy. Along with other information such as the number of men, women, students, married men, parents, etc., the retailer can manage all its stock ordering, offers and displays in certain areas or regions to maximise potential sales and reduce waste or effort.

Websites that collect cookies have to tell you that they are collecting these cookies and give you the option to agree to them doing so. You can refuse to accept the cookies policy, but this could result in you not being able to access a site that you may be registered with.

1.10 Email

There are a number of free email providers available for home users. Attackers may try to attack your email or even attack you by email. Here are five security tips:

1. Do not use an obvious username. Include numbers in your username, which makes it harder to guess as these could be random or only mean something to you.
2. Use a passphrase for your email that only you know and that you can remember.
3. If security questions are used to recover access then think about the security questions that would be used if you forget your passphrase. These security
questions should be easy to answer for you but should not be obvious answers, e.g. not your dog’s name when this is posted on your social profile.

4. Have two-factor authentication if possible. Providers such as Google use this. Two-factor authentication for email uses something you know (your passphrase) and something you have (such as your phone) for you to access, which makes it harder for someone to hack into your account. As an example, if your phone is used as the second factor then a text message might be sent to your registered phone which contains a code, which you must enter into the application to access.

5. Do not save your username and password on computers or devices that you share, and do not share the passphrase to access your email.

**Zoho Mail**

Zoho Mail is a free service that has plenty of features, a thoughtfully designed interface and solid security. With the free account you get 5GB for mail and 5GB for documents. There is also a collection of web-based software to create documents and an integrated calendar.

**Gmail**

Gmail allows email to be easily imported from other accounts and contacts, so switching to the service is very easy. It automatically filters email into ‘Primary’, ‘Social’, ‘Promotions’ and ‘Forums’, it allows you to label messages
instead of using folders, there are many ways to view emails, and overall it is an excellent service.

*Outlook*

Outlook is another excellent service that is comparable to Gmail. There are many very good features, such as the ability to archive emails, sort emails into folders, flag emails, and import contacts from Facebook and elsewhere.

**1.11 iCloud**

iCloud is a service associated with iPhones and iPads. iCloud is a simple email service that comes with 5GB of free iCloud storage. There are folders to organise emails, rules can be created to sort emails as they arrive in your inbox, it has an easy-to-use interface, and you can identify senders as a VIP so their emails always go into the VIP inbox and they will not be missed.
CHAPTER 2: THE THREATS

2.1 Cyber crime
Cyber crime is a criminal activity that involves a computer or digital media and a network – in most cases, the Internet. Cyber crime allows anyone to become a criminal: a person who is technically inept, or who lacks the confidence to challenge another person, or lacks the guile of a fraudster or anyone who is not able to be a criminal in the traditional sense of the word. The computer gives them a shield to hide behind, and gives them the means to attack without being seen or heard, and without being near the victim or having any connection to the victim.

Attackers are slowly discovering all the ways that devices can be used to attack others. As this knowledge develops, the number and sophistication of attacks also increase.

2.2 The who?
There are two very different types of attackers who must be understood to help you protect yourself. There are the brazen, confident, imposing, threatening, violent and overt attackers, while the other attackers are deceptive, covert and manipulative. Attackers who intimidate, threaten violence, are violent or are extremely abusive are the former, and Internet attackers – manipulators, tricksters and fraudsters – are generally the latter. Internet attackers are also technologists, using technology and people’s lack of understanding of technology to get what they want.
Hackers and crackers

There are two types of people who know computers, networks and programming: hackers and crackers. Hackers use their knowledge to find vulnerabilities or weaknesses in computer systems and then try to fix them. Hackers in the truest form are ethical hackers: they are available for hire to attack a computer system or network to test the security in place so that the organisation can improve it.

Crackers use their knowledge for their own benefit or gain. There has been much confusion about these terms, to the extent that ‘hacker’ is now used to describe both types of people without making any distinction as to whether or not the ‘hacker’ is using their skills and knowledge for good.

To avoid confusion, the generalised term ‘hacker’ is used in this book to refer to a person who uses their knowledge and experience to find vulnerabilities or weaknesses in a computer system, whether it is for ethical purposes or otherwise.

Hacking has become an industry in its own right, with hackers advertising their services and distributing their tools as products for sale. They tend to work alone but occasionally collaborate to achieve a common aim, either for a specific period of time or until the common goal has been achieved. From these collaborations groups may form that collectively are very resourceful and clever because they tend to share knowledge and experience, and have more time between them than a lone person.

Groups of computer hackers who use their skills and knowledge to further a political agenda or personal belief are called ‘hacktivists’. ‘State-sponsored’ hackers are
teams that have phenomenal computing resources, as well as the infrastructure and support to dedicate their whole time and effort to an aim.

Among all of these types of hackers are the script kiddies, who try to be hackers without the knowledge and experience. They will collect malware or code from the Internet, copy it or change it slightly, and launch it back onto the Internet. While they lack any real experience or understanding of the tools they use, script kiddies can still be quite destructive simply because they don’t really understand what their tools may be capable of.

Traditionally, hackers have mainly targeted commercial organisations or governments, be it for monetary gain or commercial espionage, or to cause political upset or influence public opinion. However, hackers are now targeting home networks as much as commercial entities or public bodies. Home users are running their own networks, and some professionals are using their home networks to manage company information, but home networks are almost always less secure than corporate networks.

As well as the professional information that could be taken from a home network, there are other reasons these may be attacked. If there is a baby monitor, the images could be sold to child pornographers. There may be personal information that would enable an attacker to steal an identity or financial information, or access credentials that could provide access to financial accounts. With the Internet of Things (IoT), even more information can be gleaned from home networks, such as when the home is vacant, which could be passed on to burglars. A hacker might also try to insert malicious software (malware) onto
The Threats

home networks. Such malware will have a specific purpose, which I’ll discuss later.

<<< END OF EXTRACT >>>

This extract and the publication it is taken from are both subject to ITGP copyright and may not be reproduced, in any form, without any prior written consent from the publisher.
Buy your copy today!

itgovernance.co.uk/shop/product/security-in-the-digital-world
itgovernanceusa.com/shop/product/security-in-the-digital-world
itgovernance.eu/shop/product/security-in-the-digital-world
itgovernance.asia/shop/product/security-in-the-digital-world
itgovernancegulf.com/shop/product/security-in-the-digital-world