5 Hygiene and the cyber-minefield

The symbolic map of cyberspace in Figure 1 shows areas inhabited by criminals and terrorists as well as a military area and unexplored areas (*Terra Incognita*). Many parts of cyberspace also contain the electronic equivalent of landmines, intended to cause you emotional, rather than physical, injuries and, at the very least, considerable inconvenience.

It is regrettable that, so far, the little legislation there is for cyberspace does not properly address the issues listed in this part of the book and therefore you are largely on your own when visiting the many cyber-minefields which, unlike the one photographed here, are not marked.

Figure 14: Demining operations
CC BY ANZ Cluster Munition Coalition, ND

5.1 Spam and scams

What is this?

"Spam": the name given to unsolicited bulk electronic mail sent indiscriminately to millions of people, mostly for advertising purposes but many are also "scams", confidence tricks that aim to abuse weaknesses in human nature.

Typical **spam** messages are easily recognized – do you really want to buy medication without a prescription from an unknown supplier who may be located somewhere far away and certainly in a remote jurisdiction who, having taken your money will send you nothing or a fake product. Of course there also many who are legitimate and will fulfil your order but how do you know in advance?

Scams are numerous and some are well thought out – they may tell you that the nephew of a minister in a distant country needs to transfer millions of dollars to another country and that if you help them there will be a large fee… except that they need you to give them some money in advance to facilitate the process. Incredible as this may sound, hundreds of people continue to fall for such scams.

A more sophisticated one uses the compromised e-mail address (and contacts list) of someone you know to send you a message that they were mugged during their travels, lost their passports, money and telephones. Therefore they urgently need you to send them money to help them return home.

Why is this an issue?

Two reasons – spam fills your electronic mail inbox with trivia or worse. Scams can cost you financially and, if have fallen victim to one, make you feel truly stupid.

What you should do about it

Get a spam filter. Many e-mail service providers include one in their offering but some spam will get through.

If it sound too good to be true, it almost certainly isn't. Never reply to spam, not even to take up their offer to "remove yourself from the mailing list". Doing this confirms that your e-mail address is active and that you have read the message. This is an invitation to receive much more of it.

Don't give money to anyone before you have confirmed his or her situation. The person supposed to be travelling may well be at home, and if not, should be in a position to give you a way to reach them.

Many e-mail service providers offer an anti-spam service that lets you verify what they detected as spam in case there are false-positives, i.e. messages you wish to see.

5.2 Phishing and spear-phishing

What is this?

The generally accepted definition is "an attempt to obtain confidential information by pretending to be a trusted entity in cyberspace". Well designed phishing attacks may use electronic mail details that appear genuine (the address of the sender looks like a genuine organization, for example a bank, and may include a link to a fake website designed to look like the real thing, where the victim is asked to enter confidential information (login, password, credit card details, etc.) and/or infect the victim's computer with malware planted on the fake web page.

Spear Phishing is a more sophisticated form of this attack that targets specific individuals (often corporate managers) using messages that indicate knowledge of the person (title, nickname, other) with the same intent. The plausibility of the message makes it easier for the message to be accepted as genuine.

Why it this an issue?

Because this has become a widespread practice done well enough to take advantage of the unaware. The most likely targets are those who have visibility due to their professional roles.

What you should do about it

First and foremost, remember that a government department, business or any other entity, will often accept and even encourage you to transact online – at **your** initiative and will have taken adequate precautions to protect your data. This applies to doing your tax returns online, electronic commerce, online learning and much more.

On the other hand, these entities would NEVER send you a request asking you to provide sensitive or confidential information by e-mail, particularly one including a link to follow.

If in doubt, question the entity that sent you the (potentially phishing) message as to its authenticity by phone, not by e-mail as the e-mail address may be a fake.

Spear phishing practices include faking the e-mail address of somebody you may know to send you an attachment with a plausible name that contains a purpose-designed item of malware. You should not download or open such an unexpected attachment as it may include software that can run infect your machine and those of others in the same network.

Deleting such e-mails may be an unexciting chore that adds to the pressure of your daily activities. It's good to remember the title of a book by Andy Grove (Intel's CEO in its early days). It was "Only the paranoid survive".

5.3 Attachments

What is this?

One of the useful features of electronic mail is that of being able to add files to a document. Such files can be documents, photographs, video clips, music, etc.

Unfortunately, it is also possible to add files that can run a program, usually referred to as "executable" and these can infect your computer with malicious software or perform functions that prejudice your security – by, for example, capturing your logins and passwords.

Every file (a single document in digital form) has an extension that describes what it is. Extensions are of the format "dot followed by three or more letters", for example **.mp3** describes an audio or music file, **.pdf** describes an item as being in Portable Document Format**, .jpeg** sometimes .jpg describes a graphical item in Joint Photographic Experts Group format, etc.

Why is this an issue?

Opening an attachment that is a form of executable file (software that can run on your device) can infect your computer. Once infected, your device could infect other devices, those of people you share data with. Hackers wanting to penetrate a corporate network often use the faked e-mail identities of someone you know to send attachments including professional quality malicious software that collects logins and passwords and gradually allows them to acquire confidential information and penetrate networks.

What to do about it

Gain an understanding of what the many types of file do and learn to distinguish "safe to open" files from executable files.

A search engine query for "dangerous file extensions" or "malicious file extensions" will return a long list of file extensions including: **.exe, .com, .bat, .cmd, .lnk, .vbe, .vbs, .jar** and dozens of others. Beware of files that have been compressed to the **.zip** format as you cannot tell what they contain until they have been decompressed (unzipped). If in doubt about it's origin check with the sender. If unexpected, delete without opening.

It is good practice to download only files that have a safe-to-open extension and this requires you to ensure the file extension is visible – some operating systems hide file extensions by default and it is up to you, the user, to modify the settings so that they are visible (search engine to the rescue!).

Hackers can change file extension so that they appear to be a safe-to-open one. Ensuring that the true and complete file extension is seen will show files that should NOT be opened. Your antivirus software should be set to scan files as they are downloaded and, in any case, before they are opened.

Attachments to e-mail from people you do not know (and unexpected attachments from people you know) should be treated with care – better safe than sorry… In any case, if you did not expect it, you will not miss it.

5.4 Click here to follow the link

What is this?

The World Wide Web functions through links. By clicking on a link (usually in blue and underlined) your browser will open a new page from the website to which the link took you. This is great stuff and one of the many factors that has made the Web so popular as this is easy to use.

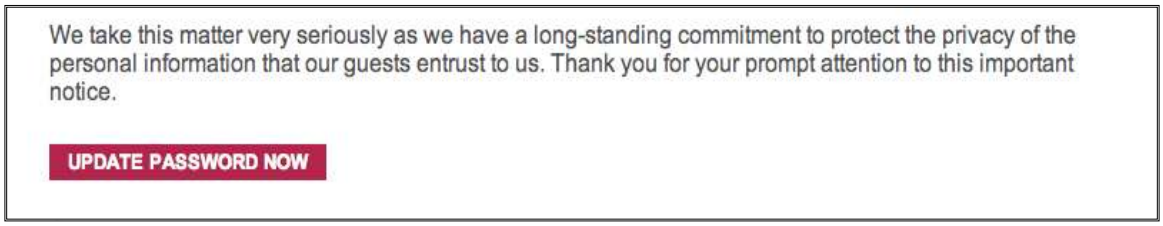

Figure 15: Screen capture of a phishing email sent to the author. He reported this to the company from which this was supposed to originate.

Why is this an issue?

Because some links are not there to help you but to take advantage of you in many different ways, ranging from taking you to fake web pages that resemble the real thing, to take you to genuine web pages where the content may be doubtful (quality, intent, potential infection).

What you should do about it

When you are dealing with a legitimate and reputable organization (a government department, electronic commerce, academia, etc.), there should be reasonable confidence that there is little risk and using the links in their pages should be safe enough.

When the link has been sent to you in an e-mail, the decision whether or not to follow it by clicking on it, should reflect your knowledge of the sender and the confidence you place on their communications. For example, several electronic commerce sites regularly send the author mails with links announcing new releases or new products. These links can be assumed to be right and proper.

Check and think before clicking and rely on your intuition, experience and antivirus software to confirm you are doing the right thing.

5.5 Unencrypted "free" WiFi (or WLAN)

What is this?

A widely practiced commercial incentive to attract customers that exploits the perceived need of many people who feel the need to be permanently connected. The Internet has also created an illusion that information and access to it should be "free" – why pay if you don't have to, right?

Why is this an issue?

WiFi (also known as a Wireless Local Area Network or WLAN) is great and convenient. When it is free, it is also unencrypted which means that others connected to the same network could (with a little bit of skill and the right tools) capture all your data traffic, including your e-mail address, login and password and whatever else you may be doing online. The same is true for having Bluetooth enabled in your devices.

What to do about it

If you are simply surfing the World Wide Web for non-sensitive and non-critical tasks, for example reading newspapers online, looking at the weather forecast, etc., it's basically OK.

For anything more sensitive – checking your bank balance, your credit card activity, buying something online or even using your e-mail, think twice before using an unencrypted network. The charges for using a secured network are mostly reasonable. From the several encryption protocols available for such wireless networks, WPA2 is regarded as the strongest The basic WEP encryption can be broken in minutes.

5.6 Encrypting your domestic WiFi

What is this?

Many of us have at least one home network and this network is, increasingly, wireless. These networks connect multiple devices, including other computers, tablets, smartphones, external storage, printers, etc. Such wireless networks have a fair range – in the order of 20 meters inside a building, more outside. The range of Bluetooth networks is smaller and these support wireless devices (keyboards and mouse) as well as smartphones.

Why is this an issue?

A third party could make parasitic use of an unencrypted network if it can find such a hotspot. These hotspots are easily found. If no password is required your data can become theirs

What you should do about it

- When installing a wireless network at home using a router, the supplier provides installation and configuration instructions which include an encryption algorithm such as WPA2 (Wi-Fi Protected Access also called RSN Robust Secure Network) and a long and impossible to memorise a long password that can be between 24 and 63 characters long. Keep a copy of this password in a secure place so that it can be re-keyed if necessary, although this is unlikely to be a frequent need
- Activate the Media Access Control (MAC) to ensure only your devices are paired with the WiFi router (detailed instructions can be found in the documentation and/or online).

- Change the default Service Set Identifier (SSID) so that a scanner looking for WiFi hotspots cannot know to whom the router belongs.
- Ensure the router software, firmware and related device drivers are up to date.
- Use your firewall to prevent incoming data traffic through the router.

5.7 Bluetooth

What is this?

Bluetooth has become a de-facto standard for low power, short-range wireless communications and it is extensively found in electronic devices. Early applications of Bluetooth were found in wireless keyboards and pointing devices such as a mouse. This has expanded to include other devices (such as printers and scanners – many of which also support WiFi such as headphones, loudspeakers, etc.

The most frequent use of Bluetooth is in mobile devices such as smartphones and tablets and the environments where these are used – for example enabling hand free phone calls while driving a car.

Why is this an issue?

While considerable attention has been given to security features in Bluetooth, the emergence of Internet enabled appliances and the Internet Of Things make Bluetooth an essential protocol over which you – as an individual – may wish to exercise control.

A key feature of Bluetooth is that while appliances may exchange data and recognize each other, in theory at least, they require an individual user to intervene to pair the appliances. However like with most security vulnerabilities it is also important that the end users be aware of what they are allowing to run in their devices. Hackers create tools to compromise vulnerable devices. Bluetooth has been hacked and known attacks included processes called bluejacking, bluesnarfing, bluebagging and bluetoothing. Several hacking tools are readily available if you know where to look.

The potential for interfering with appliances – cars that drive themselves, heart pacemakers, insulin pumps and other medical implantable devices, surgery robots, electronic locks for home use and so-called "smart" appliances are all potential targets.

What you should do about it

Use a search engine to learn more about the various ways in which Bluetooth can be compromised.

- Keep Bluetooth **off** when you are not using it and make sure you are pairing with known devices whenever you need too.
- Monitor devices and links for unauthorized Bluetooth activity.
- Make devices discoverable (visible to other Bluetooth devices) only if/when absolutely necessary.
- Make devices connectable (capable of accepting and completing incoming connection requests) only if/when absolutely necessary and only until the required connection is established.
- Pair Bluetooth devices in a secure area using long, randomly generated passkeys. Never enter passkeys when unexpectedly prompted for them.
- Maintain physical control of devices at all times. Remove lost or stolen devices from paired device lists.
- Use device firewalls, regularly patch Bluetooth devices, and keep device anti-virus software up to date.
- Comply with all applicable corporate directives, policies, regulations, and guidance.

5.8 Log out of everything you do online

What is this?

Many websites, particularly social media ones would like you to be permanently connected to make it easy to interact with your friends/followers/contacts, etc. all the time. Many of them do not make it entirely obvious that you remain connected and that logging out requires finding how to do it and then remembering to do it.

Why is this an issue?

Using small files (cookies) that get installed in your device by most webpages allows them to collect data about you, even after you have logged out, allegedly for "security purposes and aggregate statistics". In fact this may allow a website or social network to track and map you usage of the World Wide Web. They can also track your physical location and keep records of it.

What you should do about it

In the first place ensure that you actually log out from all websites that require a login. This may not be enough if the website has installed tracking cookies in your device, therefore:

- Find out how to delete individual cookies from your computer. The way to do this varies from one browser to another, and essentially the process requires you to identify which cookies have been planted and delete them – every time you visit the relevant sites.
- Alternatively, you may install a separate browser (there are many to choose from – Firefox, Chrome, Opera, etc.) and use it exclusively for your social media activities. Some of them accept third party software plug-ins that are designed to block cookies and tracking cookies.