**CYBERSECURITY**

by Simon Moss

|  |
| --- |
| **Introduction** |

Until their computer or accounts are breached, many people underestimate the significance of cybersecurity. Unfortunately, many people, including research candidates and supervisors, are often the victims of these breaches. For example

* many people are duped by emails that banks or other legitimate organizations have purportedly sent—and refer you to a website that looks authentic—but are actually designed to obtain sensitive information about you, such as passwords. This act is called phishing. Analogous texts are called smishing; analogous telephone calls are called vishing.
* similarly, people may receive emails from addresses that include the name of a friend or reputable company, but are actually sent from hackers, called email spoofing
* when researchers click on links or attachments from these websites, their computer may become infected with malware, such as computer viruses, worms, or Trojans. Even attachments that seem innocuous, such as txt files, might not actually be txt files
* some research candidates and supervisors receive emails in which they are informed that, if they do not pay a specific ransom, their details will be publicized or their computer blocked—called ransomware

On Yammer, the university publicized a course in cybersecurity to all staff at [www.knowbe4.com/homecourse](http://www.knowbe4.com/homecourse). The password was homecourse. This document summarises this course—a summary that may be helpful to research candidates or supervisors who need reminders about this course or cannot access this course.

|  |
| --- |
| **Passwords** |

Hackers utilize a variety of software programs to crack passwords. These programs can integrate many sources of information on the internet—such as the name, birthdate, postcode, relatives, and interests of a person to guess passwords. The programs can then attempt many variations of these guesses until they identify the right password, called brute force attacks.

**Quality of passwords**

The website <https://howsecureismypassword.net> can be used to test the quality of your passwords. In particular, you merely enter a password. The website then estimates how long before a brute force attack would uncover the right password. For example, if your password was secure11, most programs could uncover your password within about 1 minute. The following table presents estimates for other passwords.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Password | Estimate of time before the password is identified |  | Password | Estimate of time before the password is identified |
| hello | Instant |  | hellofriends | 4 weeks |
| hello11 | 2 seconds |  | hellofriends11 | 5 thousand years |
| Hello11 | 1 minute |  | Hellofriends11 | 10 million years |
| Hello11! | 9 hours |  |  |  |
| Hello11!1 | 4 weeks |  |  |  |
| Hello11!5 | 4 weeks |  |  |  |

As these illustrations shows

* passwords that comprise a mixture of upper and lower case letters as well as numbers are hard to identify—especially if they include special characters
* instead of passwords, pass phrases—a sequence of words—are even harder to identify and sometimes easier to remember
* but, if the program can access and utilize information about you—such as details you specified on social media—passwords that comprise post codes, birth dates, pet names, or other personal numbers and words are easy to identify
* if you swap particular letters with numbers, such as an l with a !, the password is hard to identify.

**Password practices**

Besides suitable passwords, you might also need to abstain from practices that could increase the likelihood that passwords are hacked. The following table illustrates some examples

|  |  |
| --- | --- |
| Practice | Justification |
| Do not permit computers to remember passwords, such as “Remember me”, unless you are using a computer that nobody else uses | * Sometimes, people might choose “Remember me” when using a friend’s computer. * Unfortunately, if someone else later borrows or purchases this computer, problems can unfold |
| Refrain from sharing your password with other people | * Unforeseen problems can unfold. * They might inadvertently expose your password to someone else, for example. |
| Do not use the same password for every site. | * If one site is compromised, all your computer accounts might be hacked * Instead, perhaps record all your passwords in one secure file—so you need to remember only one password * Even in this file, use codes to obscure passwords, such as “first\_pet” instead of the actual name of this pet |
| If you forget your password, some websites will also present security questions, such as “What is your mother’s maiden name”. You should adapt the answers | * For example, rather than “Smith”, you might always begin with your initials, such as ABSmith * Otherwise, hackers can utilize online information, such as your Facebook friends, to determine answers like maiden names. |
| Whenever possible, opt in to a 2 phase or multiple phase authentication | * Sometimes, for example, to access a site, after you enter a password, you need to a code that appeared on your phone * This 2 phase or multiple phase authentication tends to enhance security * If granted the choice to opt in or opt out of this security option, you should opt in |
| Change your passwords every 2 to 3 months if possible |  |

|  |
| --- |
| **Protecting your identity** |

Occasionally, researchers may receive emails from a bank or other renowned companies—such as Apple, Google, Paypal, Yahoo, and Netflix—in which they are informed that some problem has arisen. To solve the problem, the bank or company needs specific information, such as a password or another personal detail. Although the website, email, voice message, or text might seem legitimate, the message was actually designed to collect your personal details and to hack your accounts. Sometimes, the website, email, text, or voice message is immediate suspicious because

* the grammar is poor
* some unexpected names or words appear in the email address or web address
* the email address, web address, or hyperlinks entails misspellings or slight deviations from common words, such as wikipedio
* the message was unexpectedly sent at a time outside usual business hours
* the message instills a sense of urgency to prevent some problem
* the message refers to a common friend, or some other shared interest, but with limited context
* the individual utilized a medium you did not expect; for example, a person who telephones you maintains he is a member of the IT team, yet the IT team usually email.

Websites that present sexual content, support gambling, or offer free downloads are especially likely to infect computers with malware. Nevertheless, many websites or emails that infect computers do not appear to be suspicious. Because you cannot readily ascertain whether the request is legitimate, you should apply the practices that appear in the following table to protect your identity.

|  |  |
| --- | --- |
| Suitable practices | Clarification and illustration |
| Never press a link in an email that a company has sent you. Instead, open a separate tab, and visit the website directly | * If a bank or another website has asked you to send personal information, open a new tab and proceed to the website of this bank rather than click a link * Log in * If the bank actually needed personal information, you should receive another request after you log in * Never enter personal information into a website, unless you have accessed the website yourself rather than merely responded to a link |
| When you do utilize a website, check the web address begins with HTTPS | * HTTPS implies the website is more secure; that is, the information is encrypted using TLS or Transport Layer Security * Nevertheless, not all HTTPS websites are legitimate |
| Whenever you enter sensitive data, such as passwords to banks, do not use public WiFi | * You could wait until you return home * You could use your mobile hotspot |
| Contact your bank, or peruse the bank policies, to assess how the organization protects you from breaches to security | * Clarify your liability in response to these breaches * Clarify whether you are insured against fraud |
| In social media sites, withhold some personal information | * Do not include too many details that hackers can use. * For example, hackers might use this information to feign they know a common friend or a representative of a relevant organization. * The use of such information is called spearphishing |
| Be alert to psychological manipulations. | * For example, to gain access to a building, people might pretend they have forgotten their swipe card and look embarrassed * Naturally, you might want to help—but you should be aware this person might be attempting to access some information they could use nefariously |
| Protect key numbers | * Bank numbers and license card numbers, for example, should be concealed and protected whenever possible |

|  |
| --- |
| **Avoiding malware** |

The following table outlines some, but not all, of the main variants of malware—software that is designed to damage computers or computer systems. Malware is often downloaded onto your computer after you press a specific link or email attachment.

|  |  |
| --- | --- |
| Term | Definition |
| Computer virus | * Malware that replicates and thus modifies other computer programs, usually by inserting specific code |
| Computer worms | * Malware that replicates and spreads to other computers on a network—in contrast to viruses that primarily spread to other programs on one computer |
| Trojan horses | * Malware that appears to provide a useful function but actually provides a harmful function to the computer or network |
| Keylogging malware | * Malware that records every key that someone enters and sends this information to a hacker * Some malware will even activate your video to record your behavior or voice. |
| Rootkits | * A collection of software programs that enable someone to access a computer or software to which they are not permitted to access |

To prevent malware or to diminish the effect of malware, you should

* purchase anti-virus software; the software needs to be updated regularly to prevent recent advances in malware, but these updates might cost some money
* update your software when prompted, especially updates that relate to security.

|  |
| --- |
| **Protecting children online** |

Hackers often exploit children as well. To contain the likelihood and consequences of this problem, children should be informed that

* websites or emails in which individuals can earn free coins or tokens for a specific games are often designed to install malware or collect personal information
* entries on social media platforms are usually permanent; even if these entries are deleted, they can be retrieved by some programmers and hackers
* if you would not perform some act in person, do not perform this act online—such as begin a conversation with a stranger

Even responsible children, however, can experience a range of problems online. They might, for example, inadvertently violate copyright laws—a violation that can attract hefty fines. Thus, to help parents monitor the online behaviour of their younger children, software developers have introduced many parental control devices. The following table outlines some of these options. In addition, you can use the search filters in most browsers.

|  |  |
| --- | --- |
| Parental control device | Details |
| TeenSafe | * Enables parents to discreetly monitor the phone location, phone calls, texts, and social media interactions of their children |
| Limitly | * Enables parents to block specific apps, set time limits on these apps, and review which apps your child is accessing * A free program |
| Bark | * Notifies parents when messages contain cyberbullying, sexting, and signs of depression or suicidal thoughts * The program does not monitor or interfere with safe behaviors |
| ESET parent control | * Determines which apps and websites your child can and cannot access, partly depending on the age of this child. |
| OpenDNS | * Options on your Wifi that can prevent phishing and filter unsuitable content |

|  |
| --- |
| **Securing your home network** |

Sometimes, people nearby can hack into your Wifi and thus install malware, culminating in a range of complications. To diminish the likelihood of this problem, consider the following practices.

|  |  |
| --- | --- |
| Practices to secure your  home network | Details |
| Change your SSID—or surface set identifier. | * The SSID is the ID associated with your Wifi and often includes the manufacturer of your router or ISP, such as NETGEAR1424 * If you Google this manufacturer or ISP, you might be able to access information on how to change this name * If you do not change the name, hackers know the router’s manufacturer and can use this information to hack your network |
| Adjust the security options of the configuration settings of your router | * For example, one option might be to permit a password under WPA2 to enable encryption * You may also be able to set up a firewall |
| If guests are staying in your house, activate the guest network, if available | * They can then use internet but without access to anything else |

|  |
| --- |
| **Physical breaches** |

Cybersecurity is not limited to emails, websites, or mobile telephones. To illustrate, individuals may utilize physical encounters to breach security. The following table outlines some examples.

|  |  |
| --- | --- |
| Use of physical encounters | Details |
| Tailgating | * Individuals might follow you as you enter a secure building * Individuals might loiter with a group of people—such as a group of smokers—and then enter the building with this collective * Individuals might pretend they have misplaced their security card and ask you to open a door for them * Individuals might wear a uniform to feign legitimacy * Individuals might instead ask about the organization while loitering in the cafe * Once they can access a network—such as a computer at reception—they might instill a device that monitors the network, called a sniffer |
| Shoulder surfing | * Individuals may actually watch someone from behind type a password or some other information |
| USB | * Individuals might deliberately misplace a USB in a conspicuous location * The USB, when inserted into a computer, could then infect this network. * The USB might be labelled, such as “Payroll”, to elicit a sense of urgency or importance * The USB could be sent from a purported vendor * Even after individuals attempt to reformat and thus delete the files—using right click, format, and start—the malware will tend to persist |

|  |
| --- |
| **Reporting spam** |

If you receive an email or message that may be spam but want to check, email [report-Spam@cdu.edu.au](mailto:report-Spam@cdu.edu.au).