IT5507 Information Security 1

Assignment 2

Andrew Graff
2231290

Contents

Introduction

Talofa lava,

This report is about Information Security dialling towards three main areas we will venture. We discuss about Privacy, Security and Procedures that we encounter in our day-to-day lives. The occurrent use of technology and the intrinsic links with our personal privacy as consumers of the internet.

We leave footprints everywhere we go, which depending on the terrain or what shoes we choose to wear leaves a little bit of information about ourselves.

In terms of information security, it is up-to us on whether we apply the additional layers of security to protect our privacy and moving with awareness when using the internet. In theory, it involves where we trust ourselves to be and who we share our information.

The first part of this report is identifying risks to Internet Privacy. We will provide two resources that protect your privacy on the Internet and discuss details, it's creator and where this can be obtained with information on how it can protect your privacy online.

The second part of this report is related to mobile phone security. We will analyse the CertNZ Mobile Phone security guide and compare this guide with another guide relating to mobile phone security. Key details will be mentioned along with links, author, company, organization presenting with date of publication, last update, and country. Target audience will be discussed, aspects of the type of language used and whom the group of people is. An expansion of the second guide will discuss mobile network connectivity and solutions for protecting data. I will then advise which of the two guides to be recommended.

The third and final part is identify and apply internet security procedures. I will describe a specific problem with solutions relating to internet security, a specific tool of recommendation and where this tool could be found and its installation process. Another tool will be advised that can also provide solutions with justifications as to why.

Part One – Identify risks to Internet Privacy

“Broadly speaking, privacy is the right to be let alone, or freedom from interference or intrusion. Information privacy is the right to have some control over how your personal information is collected and used” (iapp, 2023).

Resource one: Digital Guardian Blog

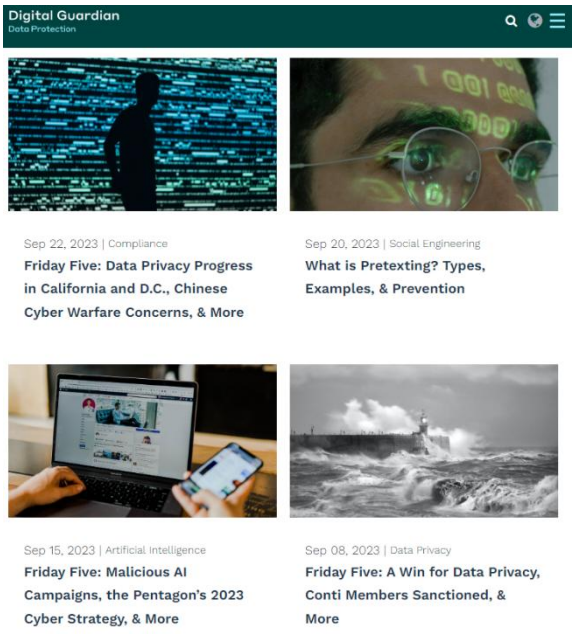
Details about the resource: Digital Guardian is a data protection platform which is part of Fortra’s comprehensive cybersecurity portfolio. The Digital Guardian blog has recent and regular updates.

Founders: Dwayne Carson, Nicholas Stamos, Tomaz Revez (Fortra)

Where it can be found: Digital Guardian Blog | Digital Guardian

Discussion on how it specifically protects your privacy on the Internet:

The Digital Guardian Blog has many insightful information all focusing on privacy and security on the internet. In a few recent blogs posted you will find information spanning in different fields of security of latest news articles with the current happenings.



A recent blog entry we can see here is “What is Pretexting? Types, Examples, & Prevention” written by a Digital Guardian Editor whom has experience reporting and writing about information security.

What is Pretexting? Types, Examples, & Prevention (digitalguardian.com)

In this blog, we learn about what Pretexting is and to familiarize ourselves so we can prevent being a victim of a pretexting attack. Pretexting is a social engineering attack where perpetrators attempt to trick a person into giving up valuable information, granting unauthorized access for cyber criminals to access financial or personal data.

Becoming aware of such information from the Digital Guardian Blog indicates risks to our modern-day internet security. Scammers using the Pretexting method to steal our data and using our personal information unlawfully would be unsettling for anyone. Learning about Pretexting adds to our awareness in being more able and educated in defending our privacy on the internet effectively. Acting with caution when browsing, an increasing vigilance to different aspects of engagement involving information on the internet.

“Cyber-attacks and scams have evolved into a multi-billion-dollar industry, impacting the most vulnerable people in society” (Gale, 2023).

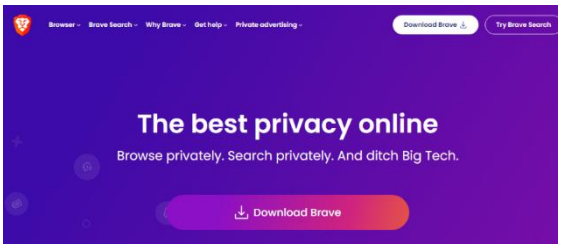
There are many insightful blogs by the Digital Guardian covering many different areas of security and privacy including threats, risks that enables us internet users to be well informed of. The regular updates prove a legitimate source of reliability as technology continues to evolve. Ultimately feeding the endless up to date information we need to protect our internet privacy.

Resource two: Brave

Details about the resource: Brave Firewall + VPN (Web browser – Practical tool)

The creator: Founded by Brendan Eich (Creator of JavaScript and co-founder of Firefox) and Brian Bondy

Where it can be found: Brave Firewall + VPN | Brave



Discussion on how it specifically protects your privacy on the internet:

Brave is an open-source web browser that centre’s itself on protecting your privacy online. Using Brave with VPN for privacy and security include encrypting and protecting anything you do while connected to the internet. “Data encrypted is the process of scrambling or enciphering data so it can only be read by someone with the means to return it to its original state. It is a crucial feature of a safe and trustworthy Internet. It helps provide data security for sensitive information” (Internet society, 2023).

We use the internet as part of our lives to engage in everyday conversations with people, social interactions, performing transactions, managing business where the data involved in these practices becomes almost sentimental.

Protecting these exchanges using the Brave practical tool will prove difficult for anyone to intrude, spy on, steal information online. The Brave VPN stands for virtual private network which is essentially what this particular web browser does. It creates a private space for you and your device when surfing the internet. Allowing the freedom to browse securely regardless of which network you are connected to. It is an enabling effect for the user having full control.

The firewall on the Brave software is an extra security feature that filters incoming and outgoing network traffic and permits or blocks data. “A firewall is the first line of defense for your network. The basic purpose of a firewall is to keep uninvited guests from browsing your network” (Bradley, 2021). This will make sure no other sources try and break into your computer/internet set up.

A common browser such as chrome and edge have potential risks to your internet privacy that include browsing history being accessed, unsafe use of saved passwords, malicious redirects, and unblocked popups. “Web browsers are designed to store information for your convenience, but that information can also fall into the wrong hands” Matteson, 2018.

Brave software with these added features heightens the layer of security with your data secured, browsing privacy, and information encrypted from attackers.

Resource recommendation and justification as to why:

I would recommend Brave web browser as a practical application for other L5 students to use that protect your privacy on the internet. Brave is becoming popular and works well across different devices. We are usually confined to the usual pre-downloaded web browser so Brave does appear as a good option. Sometimes working with other minds alike in the field of IT, it would be great practice to familiarize yourself with moving away from Big Tech companies such as Chrome. Brave respects privacy and have a privacy policy not collecting user's browsing activities which is my justification for recommendation.

Our company does not store any record of people's browsing history. We don't write any personal data to the blockchain. The only way a user's data is stored by Brave is if the user has switched on Rewards or Sync.

Browser Privacy Policy | Brave

Part 2: Mobile Phone Security

1. About "CERT NZ Mobile Phone security guide"

"It's easy to forget that our smartphones are actually just small computers. And that means we need put the same effort protecting our mobile phones as we do our PCs and our laptops" (CERT NZ, 2023).

Key details of guide presenting:

CERT NZ is an organisation that deals with cyber incident reports, tracks security attacks, and provides advice and alerts for customers. This specific guide we are analysing and evaluating is about keeping your mobile phone safe and secure.

URL: https://www.cert.govt.nz/individuals/guides/stepping-up-your-cyber-security/keep-mobile-phone-safe-secure/

Organisation: Computer Emergency Response Team (CERT) NZ

Date of publish/last updated: 2023

From what country: New Zealand

2. About "How to Secure Your Mobile Device: 8 Tips for 2023"

"At Fortra, we're bringing positive changes to cybersecurity. It's about people-first support, a best in-class solution portfolio, and a relentless mission to provide cybersecurity solutions to today's seemingly unsolvable problems" (Fortra, 2023).

Key details of guide presenting:

In this Fortra Guide there are a number of listed practical tips to securing your mobile device. It contains information about the importance of mobile phone dependency and its growing functionalities of how these mobile devices should be protected.

URL: How to Secure Your Mobile Device: 8 Tips for 2023 | Tripwire

Author/Company/Organisation: Fortra

Date of publish/last updated: Posted March 28, 2023

From what country: United States

Description of Target Audience:

The target audience of the CERT NZ guide would be for any mobile phone users. The language is in an easy informal style that has a decent spacing between words and well spread out. The contents break down simple ways to keeping your mobile phone safe and secure. There is no bombardment of words, so it is friendly and free for anyone to read and access. Typing "mobile phone security tips" will lead you to CERT NZ as the first choice of option as it is from a nationwide and certified/trusted cybersecurity team. The target audience could be for anyone residing in NZ.

The target audience for Tripwire Blog is for any mobile phone users and perhaps aimed at an average entry level IT person. The aspects of the language used suits reasonably tech savvy people and could be a little too much for anyone without basic IT knowledge. Although it is understandable, and the guide was created for the general public. The overall website is designed with options to explore as individuals, organisations, and IT professionals.

Discussion: Does the Guide discuss ways mobile devices can connect to networks that are either the same as laptops and PC's or are different from those devices

Clear examples:

In Step 3, the guide advises mobile phone users to utilize a VPN as a way to connect to a public network if you are unsure of the security status of a network. "VPN will shield your browsing activity from public Wi-Fi from prying eyes". Connecting to these networks through this way will protect your private information. A VPN works by using an application that is installed on your mobile device.

"If you want to enhance your digital privacy and increase your security online, you need VPN. It does not matter what device you use, if you do not encrypt your data before it leaves your device, it can be tracked" (Walsh, 2023).

In Step 2, the guide advises to ensure public or free Wi-Fi is protected. This discusses the mobile device owner to use applications as a way to secure connection to a Wi-Fi network to determine the status of connection. It also mentions to turn off wireless connectivity to avoid any unnecessary connection to unencrypted networks. Unprotected Wi-Fi points could lead to vulnerabilities compromising data.

The guide lists an article relating to the ease of cyber criminals being able to hack Wi-Fi. "Today, getting hacked is as common as getting a parking ticket. Every year, millions of accounts and devices get compromised by hackers, who steal sensitive data and use it for their advantage" (Panda, 2023).

Discussion: Does the Guide have any potential solutions for protecting data on phones that differ from other types of computing devices

Clear examples:

In Step 4, the guide advises encrypting your device. The encryption is mostly built in the device itself and helps protect data by scrambling this unreadable to any unauthorized people. The guide elaborates on finding this feature on your mobile phone only none other than a computer, for which the length of time to encrypt depends on the size of data and setting a password.

In Step 1, the guide advises to use strong passwords/biometrics. The biometrics differ from computing devices as some mobile phones have fingerprint or face ID authenticators and computers don't.

"Using a biometric authentication, a system can determine whether a user really is who they say they are by scanning the unique ridges of their fingerprints, examining the micropatterns in their typing behaviours, or by analyzing almost any trait a user displays that's distinctive, repeatable, and measurable" (Rees, 2023).

This increases the level of security on the mobile phone making it very difficult for unauthorized people to gain access. Protecting the valuable and important data for the rightful owner.

Recommendation to L5 Student:

My recommendation would be the Tripwire: How to Secure Your Mobile Device: 8 Tips for 2023. There is an expansion of detail for each tip which further discusses what is being mentioned with a few supporting links. VPN's, encryptions etc are some of the mobile security tips in the guide that wasn't noted in the CERT NZ justifying my reason for selection.

Part 3: Identify and apply Internet security procedures

Describe specific problem intend on solving for family friend. Relating to Internet Security – free to focus on privacy, anonymous browsing, password security, encryption.

A family friend has said they have felt their privacy was compromised while browsing the internet as they discovered unwanted software was installed on their device.

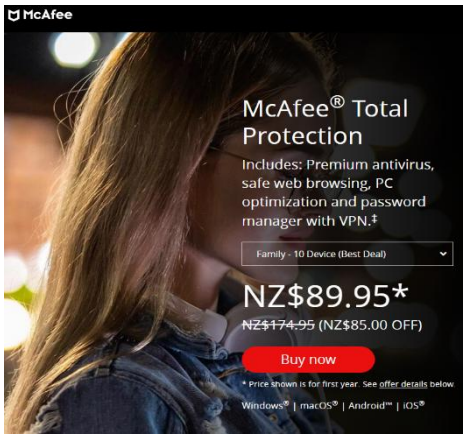
A personal security was breached concerning family friend. This could have been by unauthorized access, or a fraudulent link has been clicked where cyber criminals exploited and took advantage of a weakness in the computer internet security. The software could be very harmful to the data and overall system.

"Once malware is installed, it can monitor user activities, send confidential data to the attacker, assist the attacker in penetrating other targets within the network, and even cause the user's device to participate in a botnet leveraged by the attacker for malicious intent" (Cassetto, 2023).

A family friend asks for a recommendation to better protect their internet security to stop and eliminate unwanted software being downloaded. There are fears of passwords being exposed, data potentially leaked, or files being corrupted.

Explain the specific tool recommending to family friend. Details where tool can be found, overview of installation process (screenshots – referenced) What makes the tool appropriate for the problem to solve.

A recommendation tool is installing McAfee Total Protection as a well-rounded security package. This tool can be found via link McAfee Total Protection | Beyond Antivirus. This tool can be downloaded online with options of security protection for one or multiple devices varying in price.



Downloading this anti-virus protection package will protect the family friend internet security across any devices with access from laptop, mobile phone, tablets etc. The software is cross compatible so it functions as how you would operate it via desktop and mobile.

image: Antivirus, VPN, Identity & Privacy Protection | McAfee

Once the tool is downloaded after a package has been selected with an email address and password set up for the McAfee account. Read and accept license agreements.

Run an immediate and full scan of the whole computer system/files in search for any viruses to identify and destroy. As per image to the right:

This tool is an appropriate solution for the problem because we have learned there was no current antivirus software initially installed as per the suspicious unintended software appearing.

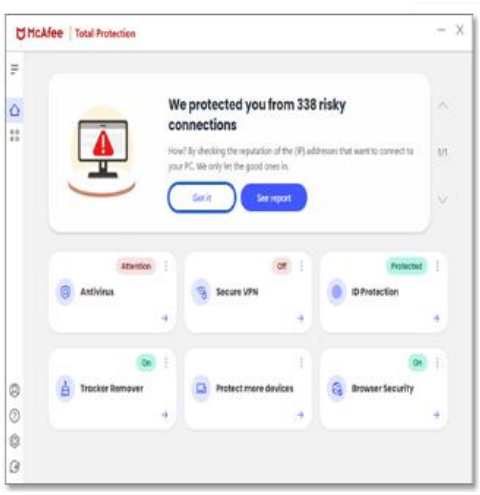


image: Free Security Assessment with McAfee Security Scan Plus | McAfee

As with no internet protection, the malware found its way to the PC. Exploiting a security threat on the family friend's system.

There are key features with this tool such as VPN compatibilities, Firewalls, Password managers etc to fully encompass a strong sense of overall internet security and added benefits to also protect mobile devices and tablets etc.

Another tool that can be used to solve the problem and brief explanation for selection.

A password manager tool called LastPass. Creating a strong password would mean cyber criminals will have difficultly accessing your systems/network.

The risk of unwanted software downloads will reduce having LastPass as a tool for creating a strong password for a better protected network and secure system. Another feature of this tool is it has a dark web monitoring option which alerts you immediately if an email address has been compromised. This will help solve the problem and future problems should malware intervene via email/social channels.

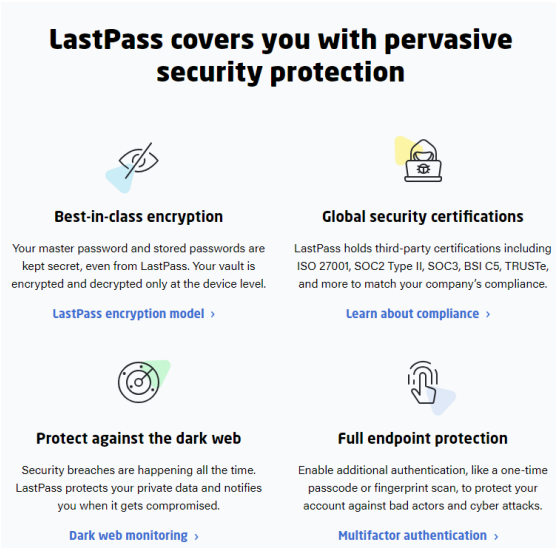


image: #1 Password Manager & Vault App with Single-Sign On & MFA Solutions - LastPass

LastPass is a free download saving you money. It is also a widely reputable software that is used by many IT professionals/businesses around the world. It has received many positive responses with one being awarded the best security product by G2.

Referencing

(Bradley, 2021)	Bradley, T. (2021, Oct 24). *What is a Firewall and How does a Firewall Work?* Home Networking. What Is a Firewall and How Does a Firewall Work? (lifewire.com)
(Cassetto, 2023)	Cassetto, O. (2023, Feb 1). *Cybersecurity Threats: Everything you need to know.* Malware Attack. Cybersecurity Threats: Types and Challenges - Exabeam
(Gale, 2023)	Gale, C. (2023, Sep 27). *Cyber-crime support: A solution to prevent repeat victimisation..* Cyber-crime support: A solution to prevent repeat victimisation | Digital Leaders (digileaders.com)
(iapp, 2023)	iapp. (2023). *What does privacy mean?.* What is Privacy (iapp.org)
(Internet Society, 2023)	Internet Society. (2023) *What is encyption?* Encryption. What Is Encryption? - Internet Society
(Matteson, 2018)	Matteson, S. (2018, April 6). *5 common browser security threats, and how to handle them*. TechRepublic 5 common browser security threats, and how to handle them | TechRepublic
(Panda, 2023)	Panda, S. (2023, Sep 06). *Hacking into Wi-Fi.* Cracking Passwords Wi-Fi Hacking: How They Hack Your Wi-Fi - PureVPN Blog
(Rees, 2023)	Rees, M. (2023, March 28). *What is Biometric Authentication And How Secure Is It?.* Expert Insights. How Secure Is Biometric Authentication? | Expert Insights
(Walsh, 2023)	Walsh, R. (2023, January 31). *Do I need a VPN on my iPhone?).* Do I Need a VPN on my iPhone? | Pros & Cons of VPNs on iOS (proprivacy.com)