SECURITY OF DEVICES IN SMARTPHONES, LAPTOPS AND USB DEVICES

ASSIGNMENT COVER SHEET

STUDENT NAME: SIDDHI KELSHIKAR

COURSE TITLE: MASTER'S OF SCIENCE IN FINANCIAL TECHNOLOGY (MSC)

LECTURER NAME: PETE CASSIDY

MODULE/SUBJECT TITLE: B9FT102 INFORMATION AND CYBERSECURITY MANAGEMENT

ASSIGNMENT TITLE: (CA2)

STUDENT ID: 10627249

TABLE OF CONTENT

1. INTRODUCTION TO PERSONAL SECURITY OF DEVICES

In today's digital era, our lives are increasingly intertwined with online activities, such as banking, shopping, communication, and work-related tasks. However, this reliance on the internet also exposes us to various risks from cybercriminals, hackers, and other malicious actors who are constantly seeking opportunities to commit fraud, steal sensitive information, or cause harm.

As a result, personal digital security has become a critical concern that cannot be overlooked. Safeguarding against these threats requires the implementation of a wide range of resources and tools designed to protect our online identity, data, and other valuable assets. These may include web services with robust security features, reliable antivirus software to detect and remove malware, smartphones with SIM cards that have enhanced security measures, biometrics for authentication, and personal devices with up-to-date security configurations. It also entails staying informed about the latest threats and taking proactive measures to mitigate risks.

As technology advances and cyber threats become more sophisticated, personal digital security has become a crucial aspect of our digital lives. It is imperative to prioritize and invest in robust security measures to protect our personal information, privacy, and online identity in this ever-evolving digital landscape. Regularly reviewing and enhancing our personal digital security practices is essential to stay ahead of potential threats and ensure a safe online experience.

2. COMMON THREATS AND VULNERABILITIES

Mobile phones, laptops, and USB storage devices are susceptible to various threats and vulnerabilities that can compromise their security and expose sensitive data to unauthorized access. Understanding these potential risks is essential in order to take appropriate measures to protect these devices and the data they contain. Here are some common threats to be aware of:

1. **MALWARE:** Mobile phones, laptops, and USB storage devices can be vulnerable to malware, including viruses, worms, and Trojans. Malware can be inadvertently downloaded from malicious websites, infected emails or attachments, or through unauthorized app downloads, and can compromise the security and integrity of the device's data.

2. **PHISHING:** Phishing attacks are attempts to trick individuals into divulging their personal or sensitive information through deceptive emails, messages, or websites. Mobile phones, laptops, and USB storage devices can be vulnerable to phishing attacks that aim to steal login credentials, financial information, or other sensitive data.

3. **PHYSICAL THEFT OR LOSS**: Mobile phones, laptops, and USB storage devices are at risk of physical theft or loss, which can result in unauthorized access to the data stored on these devices. This can lead to data breaches, identity theft, or other security breaches.

4. **WEAK OR COMPROMISED PASSWORDS**: Weak or compromised passwords are a common vulnerability that can be exploited by cybercriminals to gain unauthorized access to mobile phones, laptops, or USB storage devices. Using easily guessable passwords or reusing passwords across multiple accounts can put these devices at risk of unauthorized access.

5. **UNSECURED WI-FI NETWORKS**: Connecting to unsecured or public Wi-Fi networks can expose mobile phones, laptops, and USB storage devices to potential security threats. Hackers can intercept data transmitted over unsecured networks, leading to data breaches or unauthorized access to devices.

6. **OUTDATED SOFTWARE OR FIRMWARE**: Using outdated software or firmware on mobile phones, laptops, or USB storage devices can leave them vulnerable to known security vulnerabilities. Regularly updating the operating system, applications, and firmware can help mitigate potential vulnerabilities.

7. **PHYSICAL ACCESS TO THE DEVICE**: Allowing unauthorized individuals physical access to mobile phones, laptops, or USB storage devices can pose a significant security threat. It can result in data theft, unauthorized modifications, or tampering with the device's settings.

8. **SOCIAL ENGINEERING ATTACKS**: Social engineering attacks, such as pretexting, baiting, or tailgating, can trick individuals into revealing sensitive information or granting unauthorized access to their devices. These attacks rely on human manipulation rather than technical vulnerabilities to gain access to mobile phones, laptops, or USB storage devices.

3. PRECAUTIONS TO MITIGATE THREATS AND VULNERABILITIES

To effectively safeguard your personal and sensitive information, it is crucial to follow best practices and implement measures to prevent threats and vulnerabilities in your mobile phones, laptops, and USB storage devices. Here are some recommended steps:

1. **USE STRONG AND UNIQUE PASSWORDS**: Create passwords that are at least 16 characters long and include a combination of uppercase and lowercase letters, numbers, and special characters. Avoid using easily guessable information and consider using a password manager to generate and securely store passwords.

2. **KEEP SOFTWARE AND FIRMWARE UP-TO-DATE:** Regularly update the operating system, applications, and firmware on your devices. Software updates often contain security patches that address known vulnerabilities and protect against potential threats. Enable automatic updates for added convenience.

3. **BE CAUTIOUS OF SUSPICIOUS EMAILS OR MESSAGES**: Avoid clicking on suspicious links or downloading attachments from unknown or suspicious emails or messages. Be wary of phishing attempts and never provide personal or sensitive information unless you are certain of the legitimacy of the request. Exercise caution even with messages from known contacts, as they may be compromised.

4. **AVOID UNSECURED WI-FI NETWORKS**: Refrain from connecting to unsecured or public Wi-Fi networks, as they can be vulnerable to security threats. Use secured Wi-Fi networks with encryption and password protection, or use a virtual private network (VPN) for added security when accessing sensitive information or conducting online transactions.

5. **USE TWO-FACTOR AUTHENTICATION (2FA):** Enable two-factor authentication on your accounts whenever possible. This adds an additional layer of security by requiring a verification code in addition to your password when logging in.

6. **BE CAUTIOUS WITH APP DOWNLOADS**: Only download apps from trusted sources, such as official app stores, and avoid downloading apps from unknown or third-party sources, as they may contain malware or other malicious software. Always review the permissions requested by apps before installing them and be cautious of granting excessive permissions that could compromise your privacy and security.

7. **REGULARLY REVIEW AND MANAGE PERMISSIONS:** Review and manage the permissions granted to apps on your mobile phone and laptop. Disable unnecessary permissions that could potentially expose your data to security risks.

8. **SECURITY AWARENESS TRAINING**: Educate yourself and your users about best practices for digital security, such as avoiding clicking on suspicious links, being cautious with app downloads, and practicing safe online behaviour. Increasing security awareness can go a long way in preventing threats and vulnerabilities.

By implementing these best practices and measures, we can significantly reduce the risks of threats and vulnerabilities in your mobile phones, laptops, and USB storage devices, and enhance the overall digital security.

4. TOOLS AND TECHNOLOGIES USED TO AVOID THREATS & VULNERABILITIES IN MOBILE PHONES, LAPTOPS AND USB DRIVE

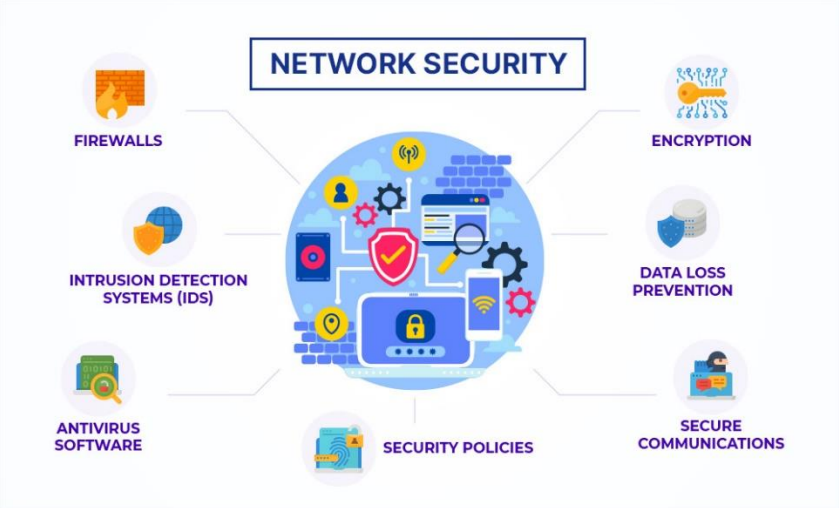
There are several tools and technologies that can be used to enhance the security of mobile phones, laptops, and USB storage devices, and avoid threats and vulnerabilities. These include:

1. ANTIVIRUS SOFTWARE

Antivirus tools are designed to detect and remove a wide range of harmful applications, including viruses, malware, ransomware, and spyware. Some antivirus software can also prevent email phishing attempts, making them versatile in safeguarding against various threats from different sources.

2. FIREWALL

A firewall is a security tool that helps protect against unauthorized access to your devices by monitoring and filtering incoming and outgoing network traffic. It acts as a barrier between your devices and the internet, blocking potentially harmful connections. Next-Generation Firewalls (NGFWs) are particularly effective in preventing malware and application-layer attacks, protecting computers from unwanted traffic.



3. VIRTUAL PRIVATE NETWORK (VPN) GATEWAYS

A VPN gateway is networking equipment that connects two or more devices or networks in a VPN system. It bridges the communication between distant sites, networks, or devices, and provides essential VPN networking services such as IP address assignment, routing, and

maintenance. VPN gateways can be routers, servers, firewalls, or other data transmission-capable equipment. This can help protect your data from interception and eavesdropping on public Wi-Fi networks.

4. NETWORK DEVICE BACKUP AND RECOVERY

Network outages due to hardware failure or configuration issues can significantly impact productivity and revenue. Centralized backup and recovery for network devices is advantageous as it automates the backup process and facilitates rollback or restore procedures. Network configuration management systems store device configurations and states in a secure location, making it easier to implement and undo configuration changes and recover from disasters quickly.

5. DEVICE ENCRYPTION FEATURES

Many mobile phones, laptops, and USB storage devices come with built-in encryption features, such as device encryption or encrypted folders, that can be enabled to protect your data. It is essential to take advantage of these features and configure them properly to ensure maximum security.

It is essential to stay proactive and vigilant in implementing these tools and technologies to safeguard our devices and protect our personal information from potential security risks.

5. APPROACHES TO MITIGATE THREATS AND VULNERABILITIES

Encrypting and securing the data stored in devices such as smartphone, laptop and USB drive is a crucial step in securing personal information, I have used my own devices for encryption in order to test our solution.

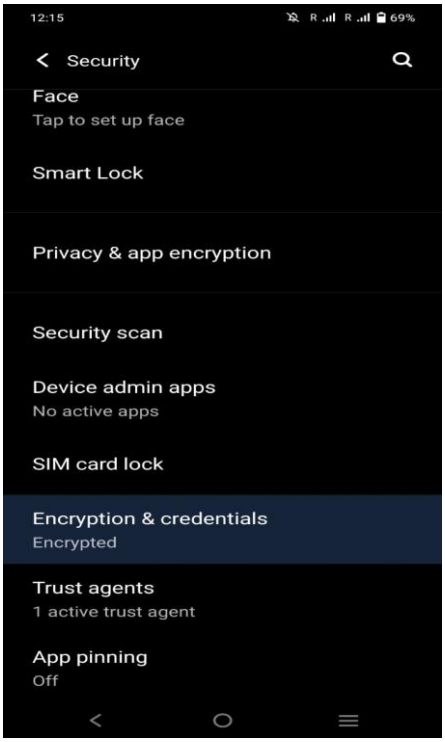
A. SMART PHONE

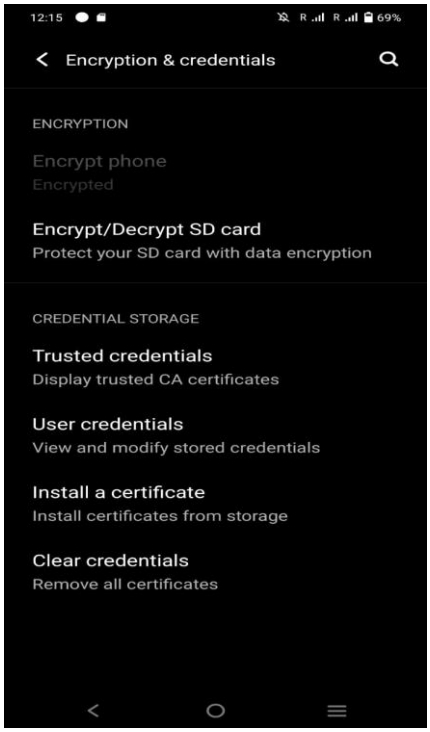
I. ENCRYPTING THE DATA

By encrypting our smartphone's data, we add an extra layer of security to protect our sensitive information from unauthorized access or data breaches

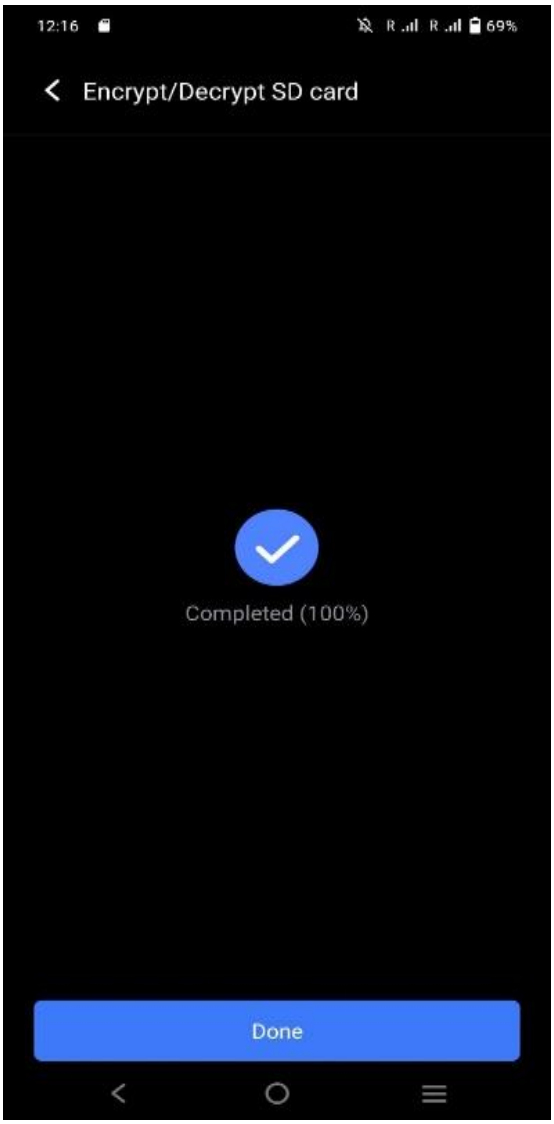
Following are the steps to encrypt the data in Android mobile:

1. Open Security settings menu on your Android device and look for the 'Encrypt Device' or 'Encrypt Phone' option. Tap on it to start the encryption process.





2. Follow the instructions provided on the screen to initiate the encryption process. This may involve setting up a PIN, password, or pattern to be used as the decryption key.

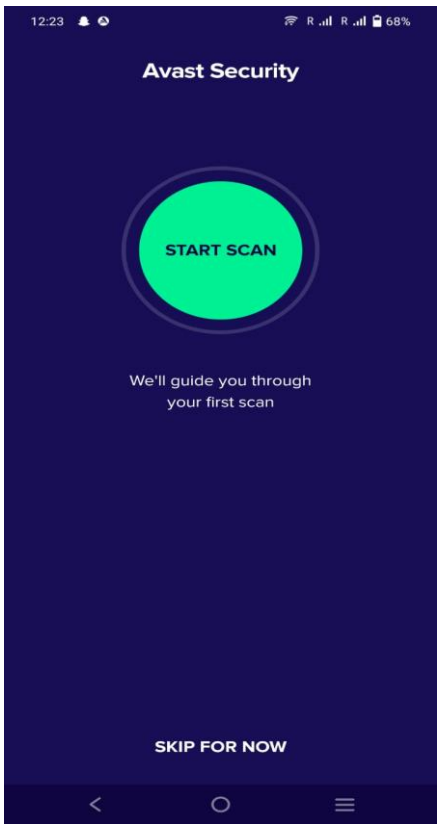


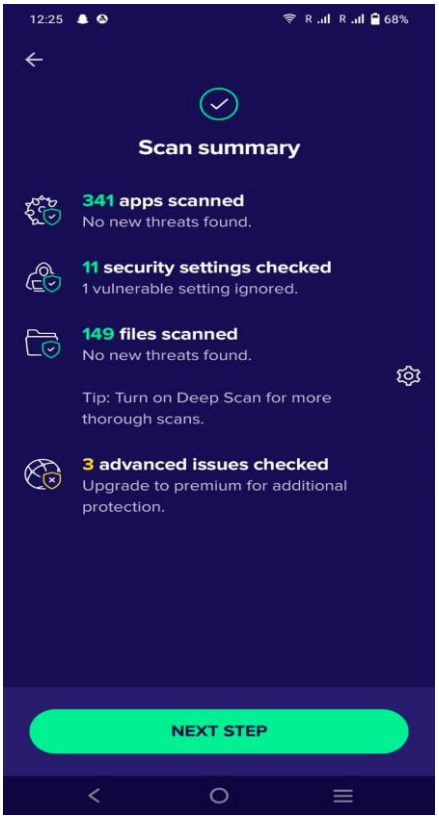
3. Once the encryption process is complete, your device's data will be scrambled and protected from unauthorized access.

4. After encryption, a password or decryption key will be required every time you power on or unlock your device to access the encrypted data.

II. USING ANTI-VIRUS SOFTWARE WITH ANDROID OSS

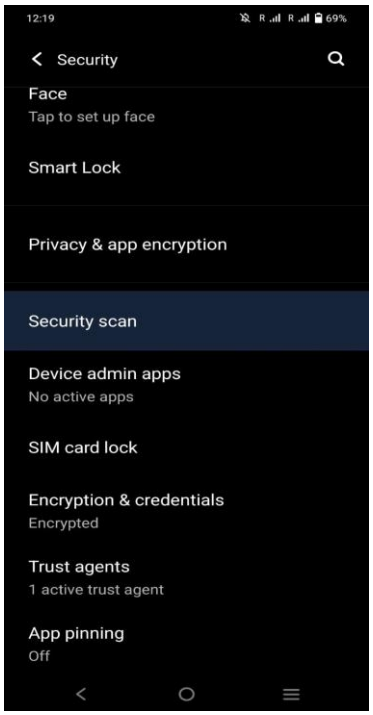
Avast has developed a comprehensive suite of tools to safeguard Android devices against various threats. This software provides a range of essential features for basic Android security. In addition to monitoring network traffic and live-monitoring of running programs, Avast offers robust protection and is highly recommended for Android users who prioritize device security.

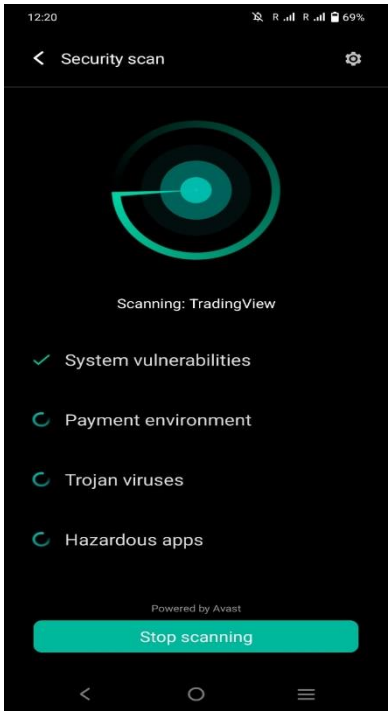


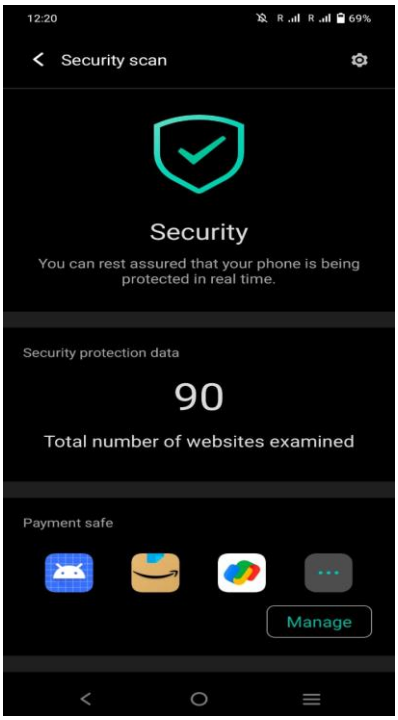


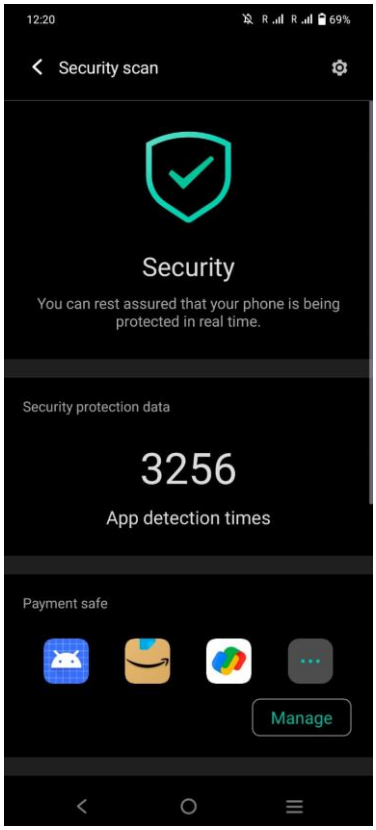
III. SCANNING

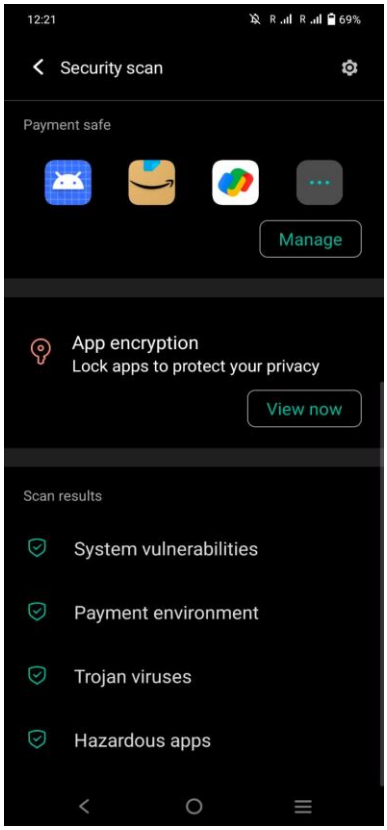
Regularly scanning an Android device for malware, trojans, and spyware is a crucial security measure. Malwarebytes Anti-Malware is a reliable software that can be used for these tasks. It effectively detects and removes malware, as well as identifies potential security risks on Android devices, making it an essential tool for maintaining device security








12:20
69%
Security scan
Security
You can rest assured that your phone is being protected in real time.
Security protection data
3256
App detection times
Payment safe
Manage


12:21
69%
Security scan
Payment safe
Manage
App encryption
Lock apps to protect your privacy
View now
Scan results
System vulnerabilities
Payment environment
Trojan viruses
Hazardous apps

B. LAPTOP

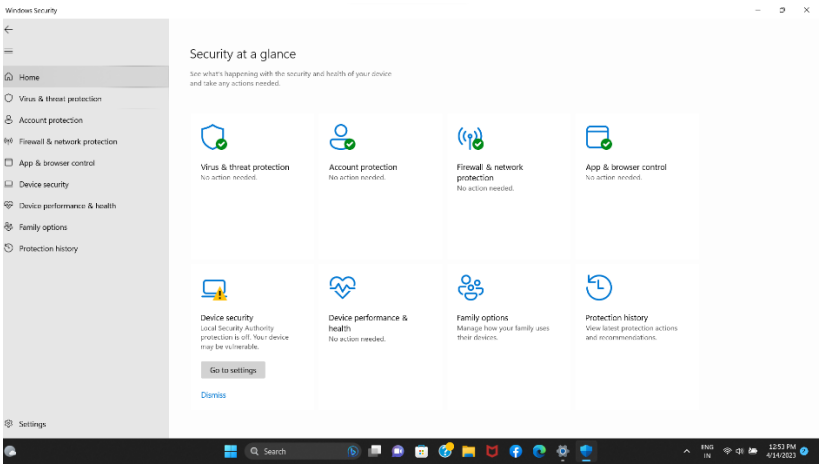
ENCRYPTING FILES & HARD DISK

Encrypting files and hard disks adds an extra layer of security by transforming the information into a jumbled, unreadable format, making it incomprehensible to unauthorized individuals, thereby safeguarding against unauthorized access. This enhanced security measure modifies the data by scrambling it, making it difficult for intruders to decipher the information.

Following are the steps to encrypt the files and Hard Disk in HP intel core i5 windows 11 by using Laptop settings and Bit Locker.

I. ENCRYPTING FILES ON LAPTOP:

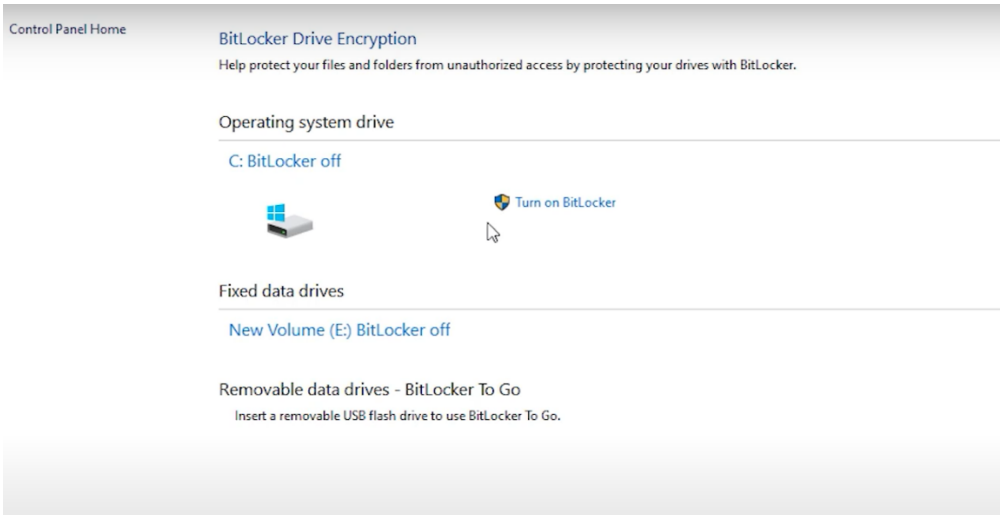
1. Open the Security settings menu on your laptop and look for 'Windows Security'.
2. In the 'Home' menu, you may see options such as Virus and Threat Protection, Account Protection, Firewall and Network Protection, App and Browser Control, Device Security, Device Performance and Health, and Protection History.



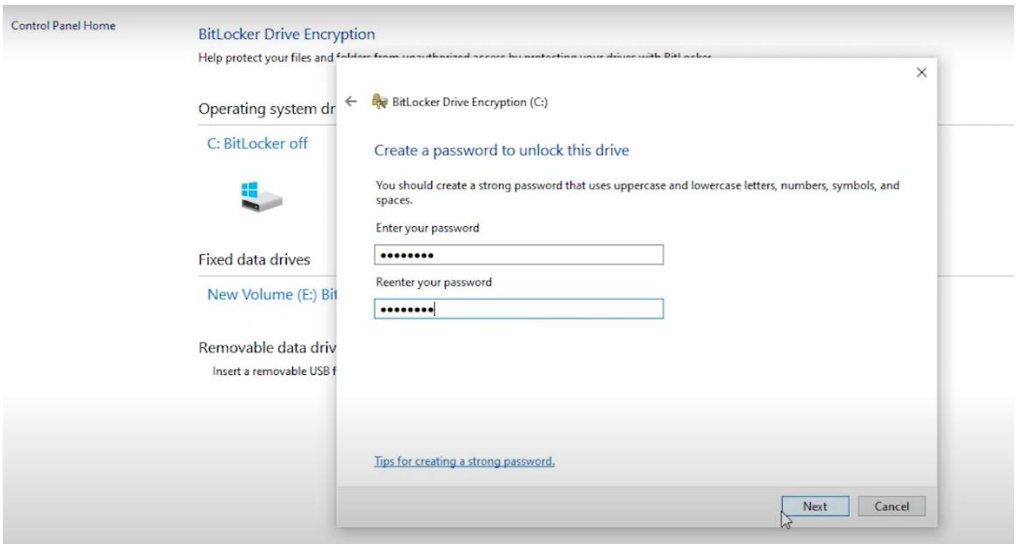
3. Click on each option to access the encryption process for that specific device.

II. ENCRYPTING HARD DRIVE WITH BITLOCKER:

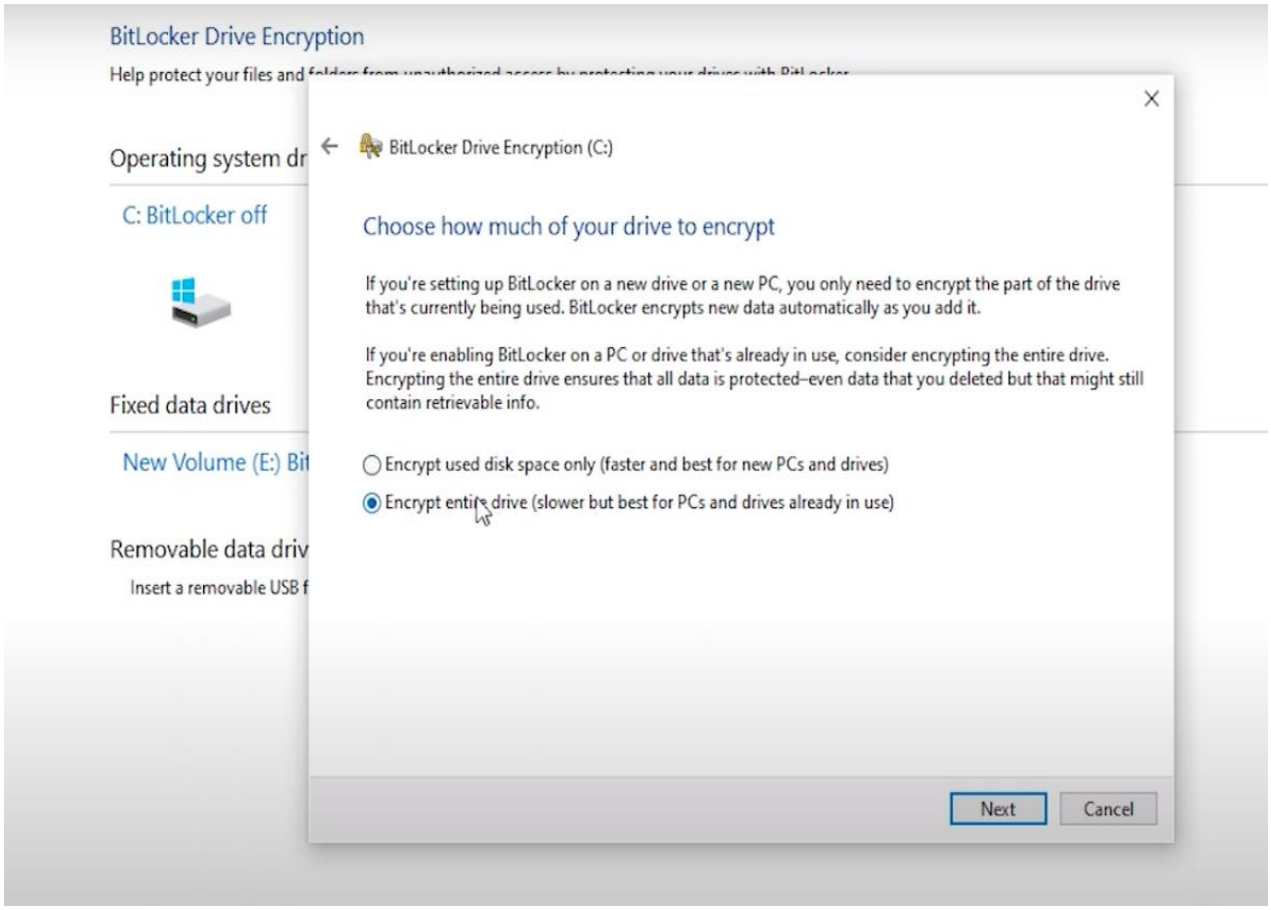
1. Open the Control Panel from the search menu.
2. Click on 'BitLocker Drive Encryption' to start encrypting your data.



3. Turn on BitLocker and create a password to encrypt the files.



4. Save the recovery key in a new folder and restart your laptop to enable BitLocker encryption.



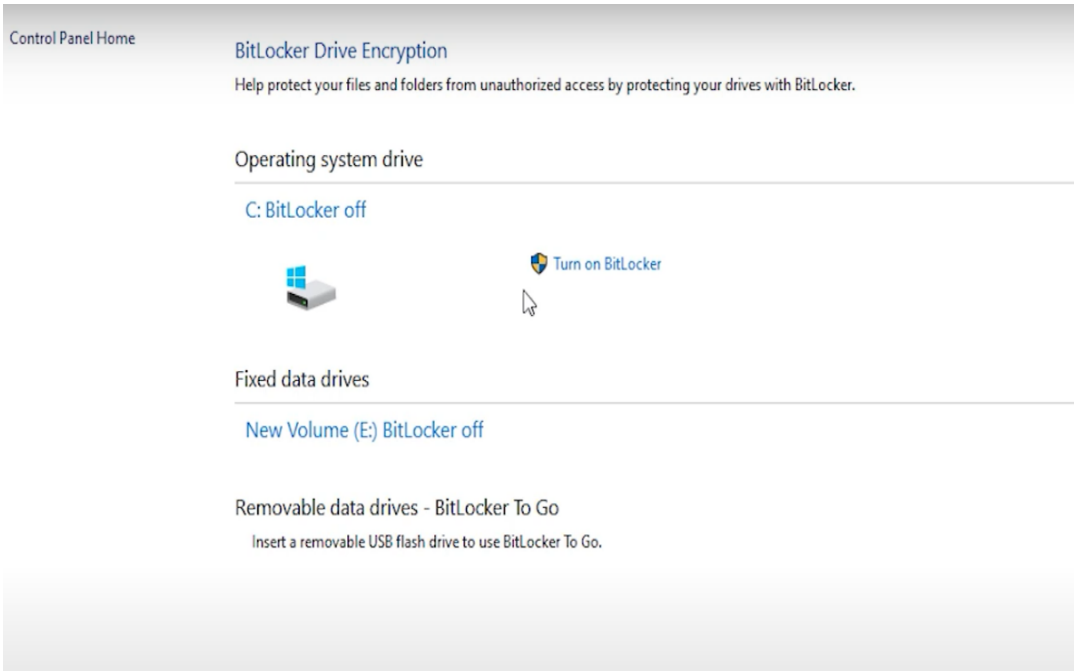
Alternatively, you can also use software like Zulu Crypt and ecryptfs, which provide a graphical user interface (GUI) for performing disk encryption on the local hard disk. This software can offer additional options for encrypting files and hard disks on your HP laptop with an Intel Core i5 processor running Windows 11.

C. ENCRYPTING USB DRIVE

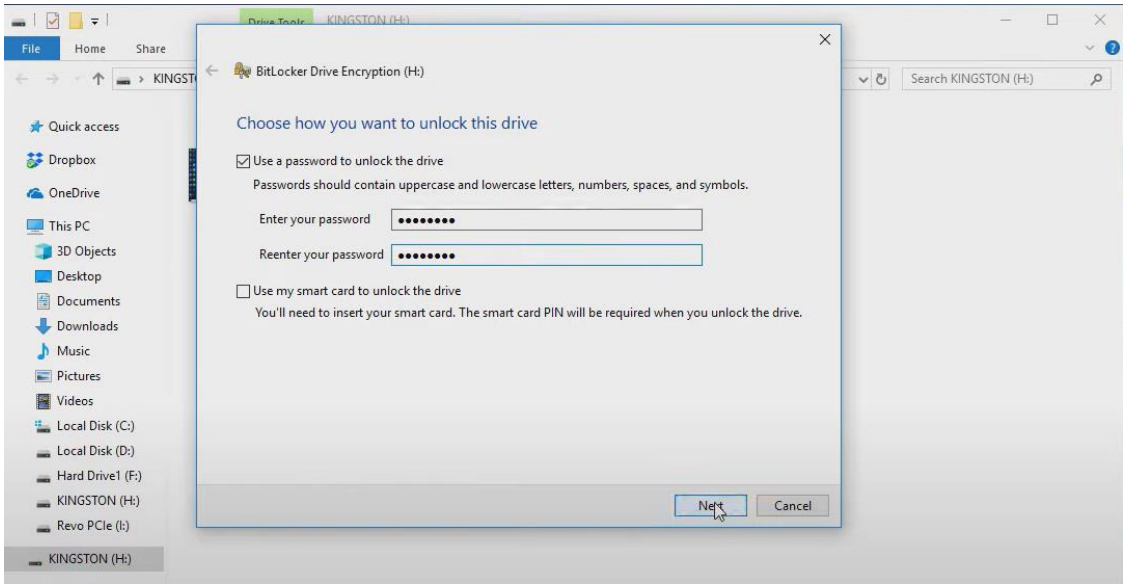
To enhance the security of data stored on USB devices, encryption and password protection can be employed as effective security measures. These measures safeguard the information from unauthorized access, ensuring that only individuals with the correct encryption key or password can view and modify the data.

Here are the steps to encrypt a USB drive on an HP Intel Core i5 Windows 11 system using BitLocker:

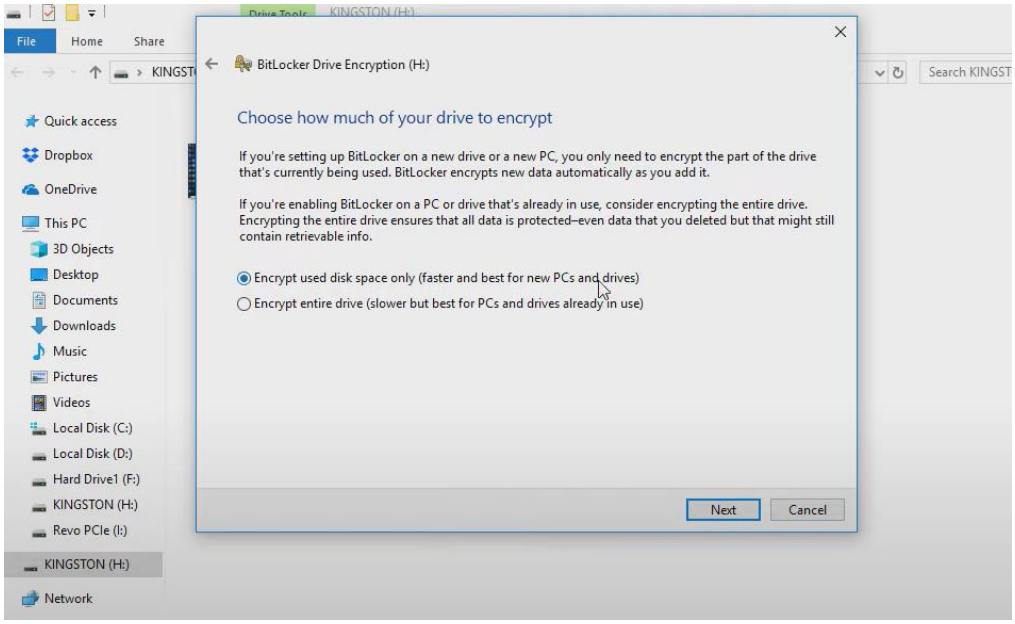
1. Open the File menu.
2. Click on the USB drive that needs to be encrypted.
3. Right-click on the USB drive and select 'BitLocker Drive Encryption' to initiate the encryption process and turn it on.



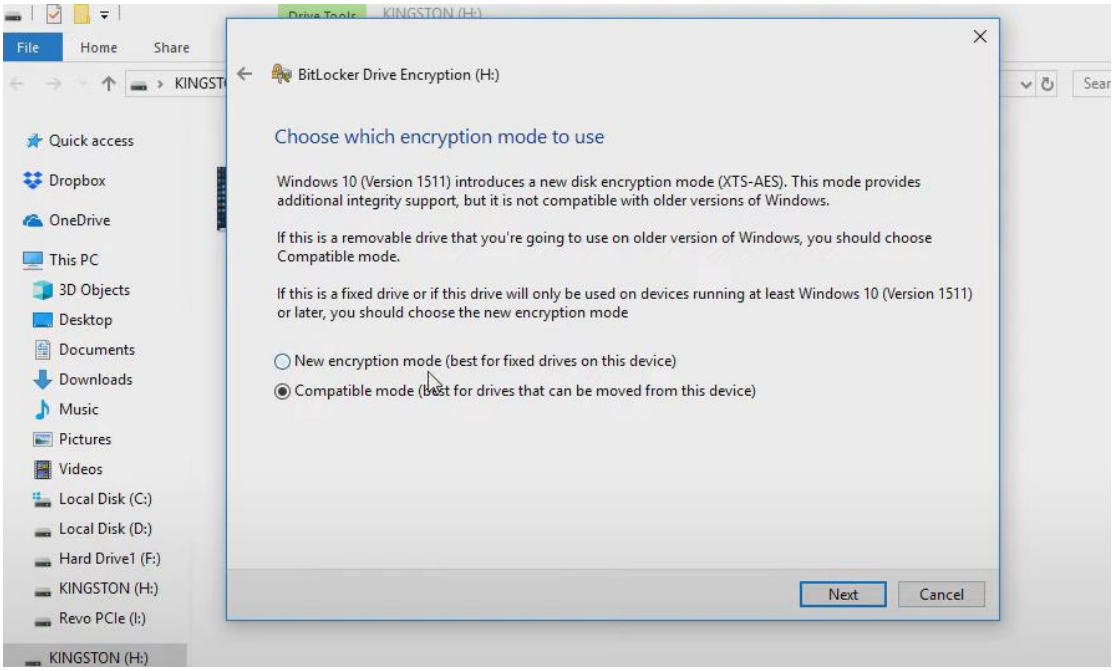
4. Create a password to encrypt the files and save the password securely.



5. Choose the "Encrypt entire device" option to encrypt the entire data on the USB drive.



6. Turn on the compatible mode for further encryption.



7. Finally, click on "Start encrypting" to begin the encryption process.

By following these steps, you can encrypt your USB drive and enhance the security of your data stored on it.

5. CONCLUSION

In today's digital world, personal digital security is vital for protecting sensitive information on mobile phones, laptops, and USB storage devices. Threats like data breaches, identity theft, and financial loss can have severe consequences.

To safeguard against these risks, it's crucial to adopt best practices such as using strong passwords, keeping software updated, enabling device lock and encryption, being cautious with emails and messages, avoiding unsecured Wi-Fi networks, using two-factor authentication, and regularly backing up data. Educating oneself about security best practices and being cautious with app downloads and physical access to devices are also important measures to reduce vulnerabilities.

Additionally, staying informed about security updates, being vigilant about the latest threats, and prioritizing the security of personal information are essential steps towards enhancing overall digital security. Digital security is an ongoing process that requires continuous effort and vigilance. By following these best practices, we can minimize risks and protect personal information from potential cyber-attacks, ensuring a safe and secure digital experience. Stay proactive, cautious, and prioritize your digital security.

6. REFERENCES

Anon., n.d. *Pulsar Security.* [Online]
Available at: https://blog.pulsarsecurity.com/usb-security-risks-when-flash-drives-become-dangerous
[Accessed 15 4 2023].

Anon., n.d. *Tripware.* [Online]
Available at: https://www.tripwire.com/state-of-security/secure-mobile-device-six-steps
[Accessed 14 4 2023].

University, H., n.d. *Personal Device Security Guides.* [Online]
Available at: Personal Device Security Guides
[Accessed 14 4 2023].

Valley, S., n.d. *Network Security Devices.* [Online]
Available at: https://www.sunnyvalley.io/docs/network-security-tutorials/network-security-devices
[Accessed 15 4 2023].

Cassidy, P. (2021). Information and Cybersecurity Management. Pete Cassidy.
https://elearning.dbs.ie/pluginfile.php/1762369/mod_resource/content/0/Lectur e%209.pdf

[Accessed 15 4 2023].

OSINT – OPEN-SOURCE INTELLIGENCE

OSINT – OPEN-SOURCE INTELLIGENCE

As a cybersecurity professional employed by ABC Ltd., a company based in Dublin, I have been requested to support one of our engineers in conducting a security audit for Supermacs. The engineer has specifically asked for an OSINT report to be prepared, which will involve identifying and analysing the digital footprint of Supermacs using open-source intelligence techniques. Supermacs, which opened its first restaurant in County Galway, Ireland in 1978, has become a familiar sight in towns and cities throughout Ireland since its inception, operating as a popular fast-food chain.

OSINT REPORT ON SUPERMACS

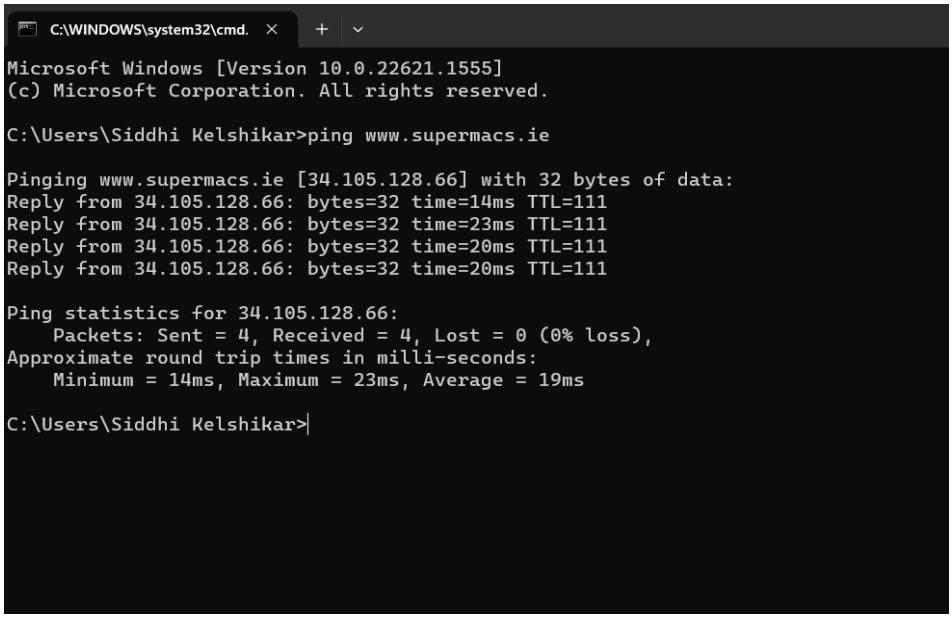
The information included in this report is based on data obtained from Supermacs' publicly accessible website, which can be found at https://supermacs.ie/. All the data used is sourced from publicly available information.

1. INFORMATION ABOUT IP ADDRESS:

- Ping Status = Ping was successful; 4 packets were received
- IP Address =34.105.128.66
- Host name = www.supermacs.ie

The OSINT report will utilize appropriate tools and techniques to gather relevant information on the following aspects:

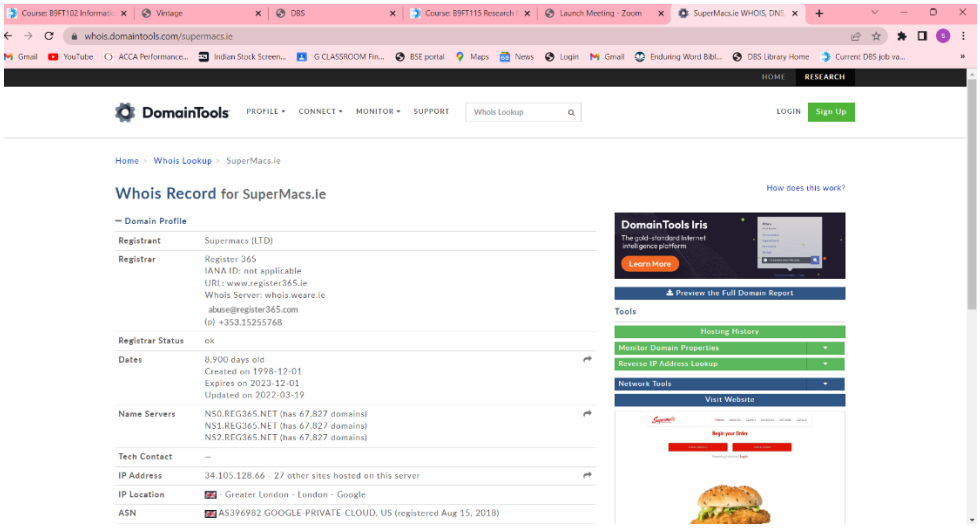
A successful ping test confirms the operational status of the network link between the source and destination hosts, while analysing the response times can help identify any errors or delays within the network



2. DNS ENUMERATION

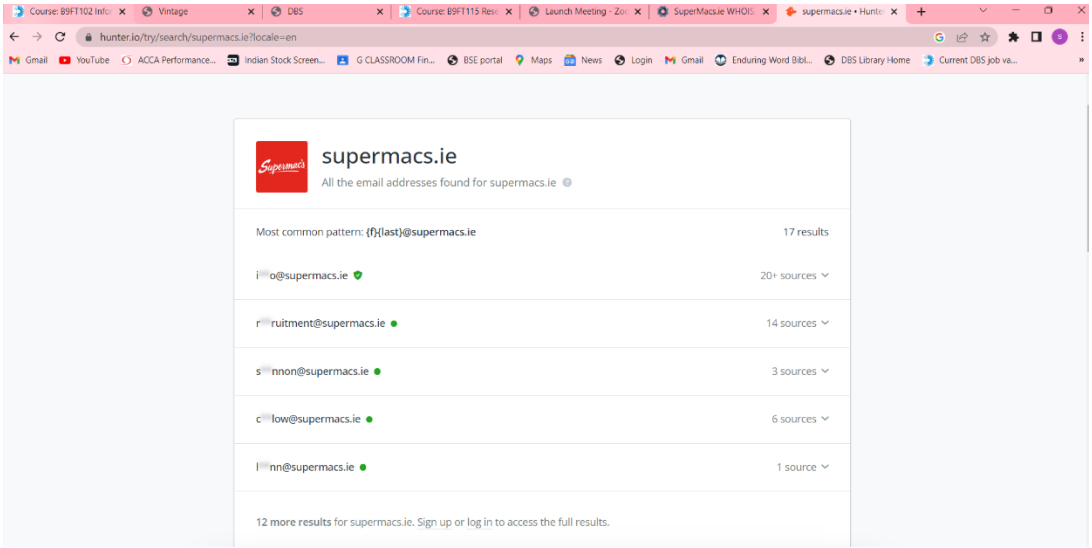
- Registrant: Supermacs (LTD)
- Registrar: Register 365
- IANA ID: not applicable
- URL: www.register365.ie
- Who is Server: whois.weare.ie
- Registrar status: ok

https://whois.domaintools.com/supermacs.ie



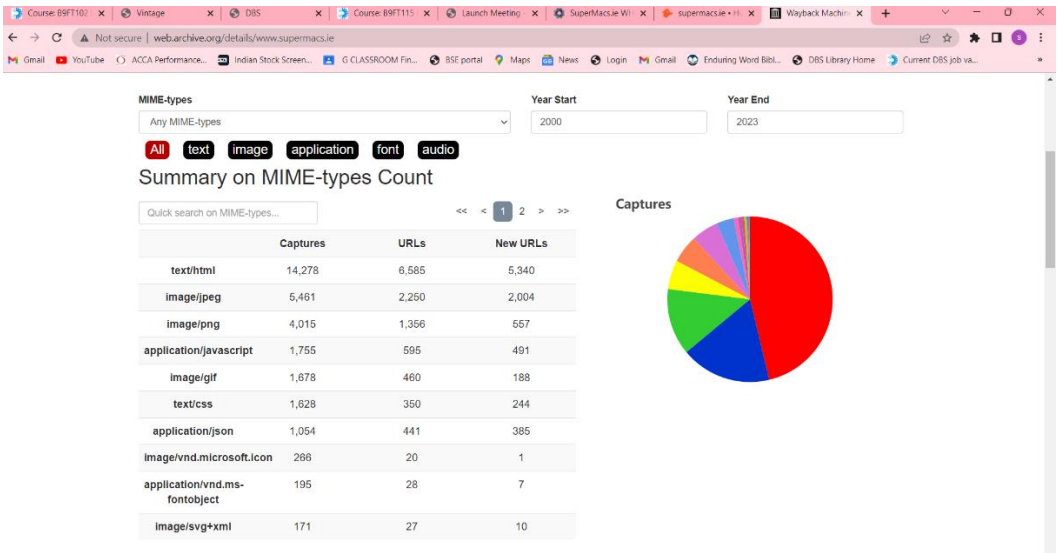
3. LIST OF INTERNAL EMAIL ADDRESSES

The email IDs associated with supermacs.ie have been identified using the Hunter web tool. However, to access the complete email IDs and obtain more information, registration on the website is required.
https://hunter.io/try/search/supermacs.ie?locale=en



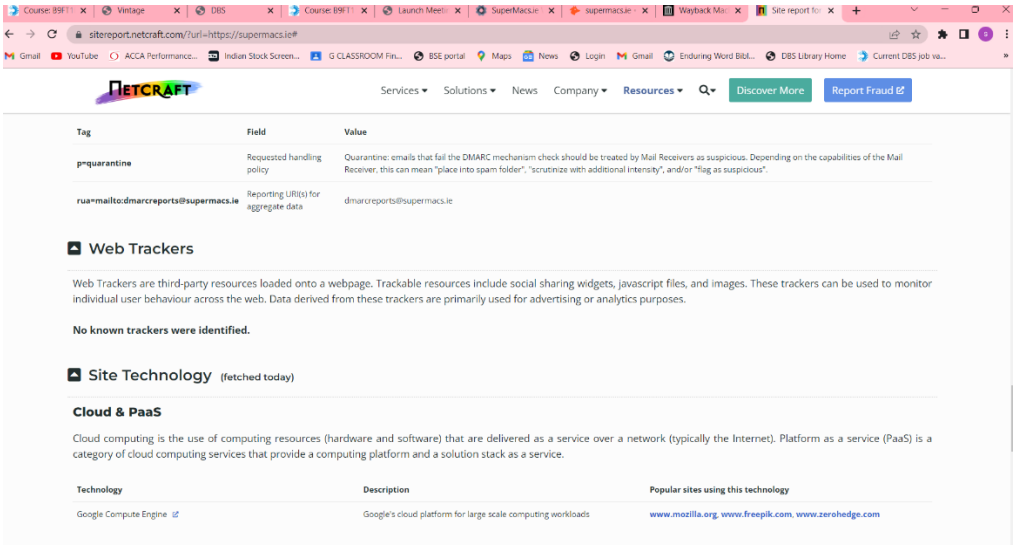
4. SOFTWARE USED BY THE ORGANIZATION

Based on information obtained from web archives, Supermacs primarily utilizes JavaScript and JSON as major software applications.
http://web.archive.org/details/www.supermacs.ie



It has been discovered that Supermacs employs Cloud and PaaS (Platform as a Service) technologies in Netcraft application. Specifically, Supermacs utilizes 'Google Compute Engine,' which is a cloud platform offered by Google for managing large-scale computing workloads.

https://sitereport.netcraft.com/?url=https://supermacs.ie#



5. ANY VULNERABILITIES WHICH MAY BE PRESENT IN THE IT INFRASTRUCTURE

Vulnerabilities related to Supermacs yielded limited information due to resource constraints. However, the findings indicate a medium risk level. For detailed information on the vulnerabilities discovered refer to the following link https://pentest-tools.com/website-vulnerability-scanning/website-scanner

The website of Supermacs has been found to have several vulnerabilities, including:

a. Insecure cookie settings: missing Secure flag
The absence of the Secure flag on the cookie makes it susceptible to interception by an attacker over an unencrypted channel, potentially leading to unauthorized access to a user's web session.
It is recommended to always set the Secure flag for cookies containing sensitive information or session tokens, and ensure they are transmitted only over encrypted channels.

b. Insecure cookie settings: missing HTTP Only flag
Cookies without the HTTP Only flag can be accessed by JavaScript code on the web page, making them vulnerable to theft and potential session hijacking through malicious injection of JavaScript code.
It is advised to set the HTTP Only flag for all cookies to prevent unauthorized access via JavaScript.

c. Vulnerabilities found in server-side software
These vulnerabilities may expose the affected applications to unauthorized access and denial-of-service attacks. Attackers could exploit these vulnerabilities to gain unauthorized access or disrupt system operations.
Upgrading the affected software to the latest version is recommended to mitigate the risks associated with these vulnerabilities.

Vulnerabilities found for server-side software

CVSS	CVE	SUMMARY	EXPLOIT	AFFECTED SOFTWARE
4.3	CVE-2019-11358	jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.	N/A	jquery 1.11.1
4.3	CVE-2020-11022	In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.	N/A	jquery 1.11.1
4.3	CVE-2020-11023	In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.	N/A	jquery 1.11.1
4.3	CVE-2015-9251	jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.	N/A	jquery 1.11.1

In addition, some low-risk findings have been observed, such as missing security headers (X-XSS-Protection, X-Content-Type-Options, Referrer-Policy) in the response headers, and disclosure of server software and technologies used by the company. These findings may provide valuable information to potential attackers for launching targeted attacks against specific software versions.

It is important for Supermacs to address these vulnerabilities and implement appropriate security measures to protect their website and systems from potential security risks.

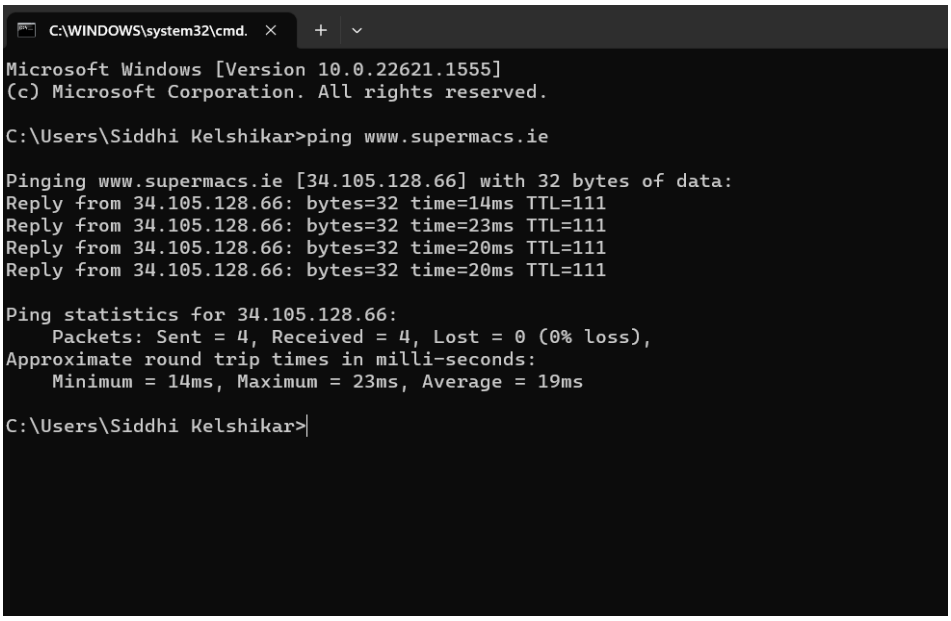
6. ASSESS IF ORGANIZATION WAS SUBJECT TO DATA BREACH OF ANY OTHER CYBERCRIME

In a legal case in 2020, Mr. Justice Barr rejected the use of CCTV footage in Dudgeon v. Supermacs [2020] IEHC 600. Supermacs cited GDPR requests as the reason for not releasing the fast-food CCTV recordings. Under GDPR, individuals have the right to access their personal data, including CCTV footage containing their images. However, data controllers can reject unreasonable access requests, although such denials are rare.

In this case, Supermacs withheld the information due to the ongoing lawsuit filed by the requester for personal damages, referring to Mr. Justice Barr's High Court judgment.
The Data Protection Commission clarified in the court judgment that GDPR access to personal data may differ from lawsuit discovery demands. The statement emphasized that a data controller is still obligated to fulfill access requests for CCTV footage, unless there is a valid restriction under GDPR or applicable data protection legislation.

Supermacs seeks court protection for businesses to prevent unfair advantage of personal injury plaintiffs through the use of CCTV footage. It should be noted that no cases of data breaches or other cybercrimes related to Supermacs have been found online.

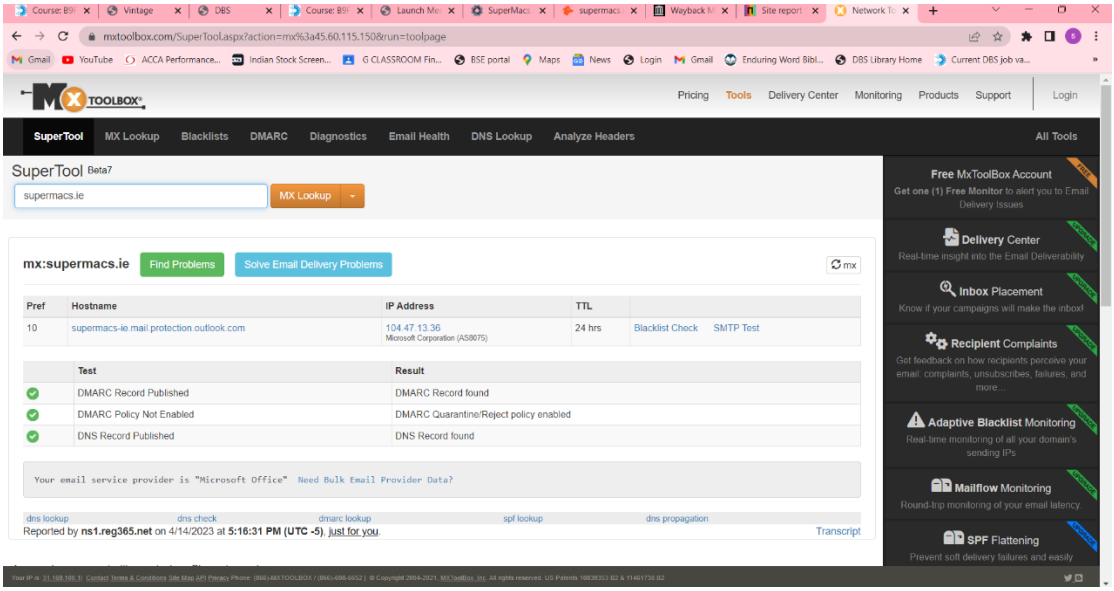
7. IP ADDRESS RANGE (CHECK IF ACTIVE WITH PING).



The IP address range is 34.105.128.66 and is active

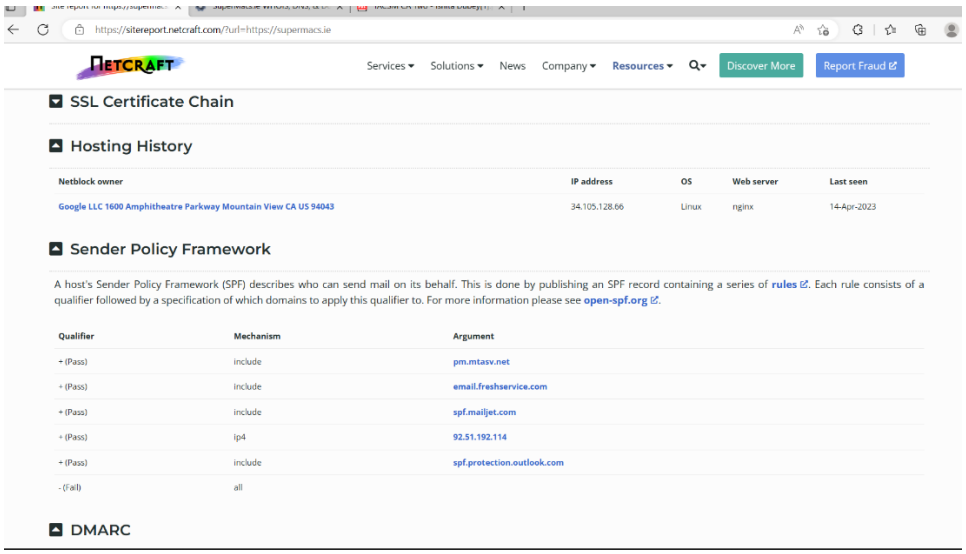
8. EMAIL SERVER

The email server that Supermacs uses is Microsoft Office.
https://mxtoolbox.com/SuperTool.aspx?action=mx%3a45.60.115.150&run=toolpage



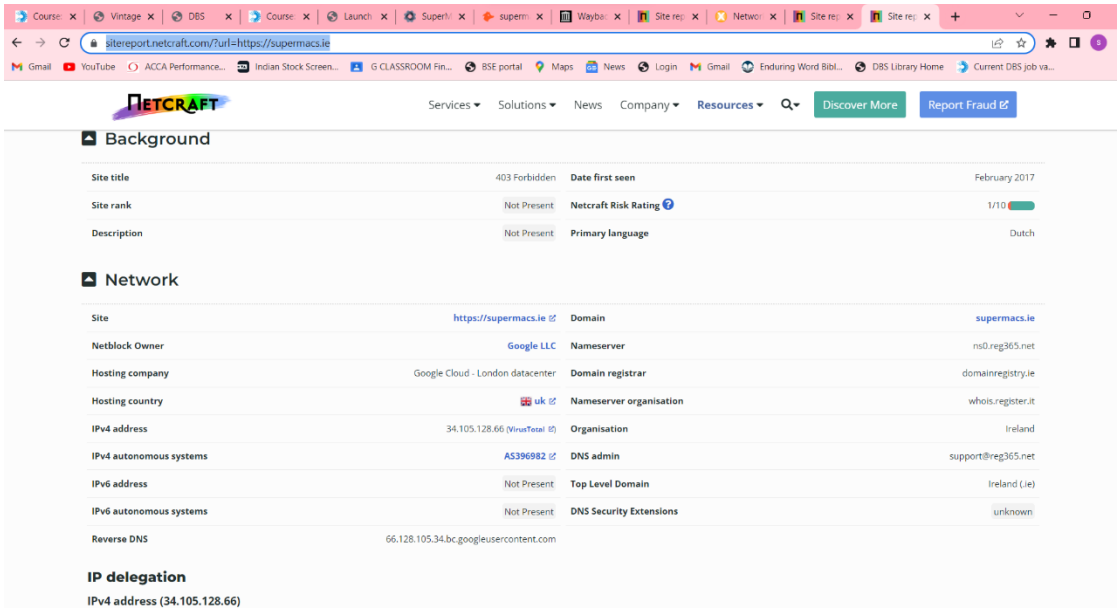
9. OPERATING SYSTEM TYPE

The operating system Supermacs uses is ‘Linux’.
https://sitereport.netcraft.com/?url=https://supermacs.ie



10. HOSTING PROVIDER

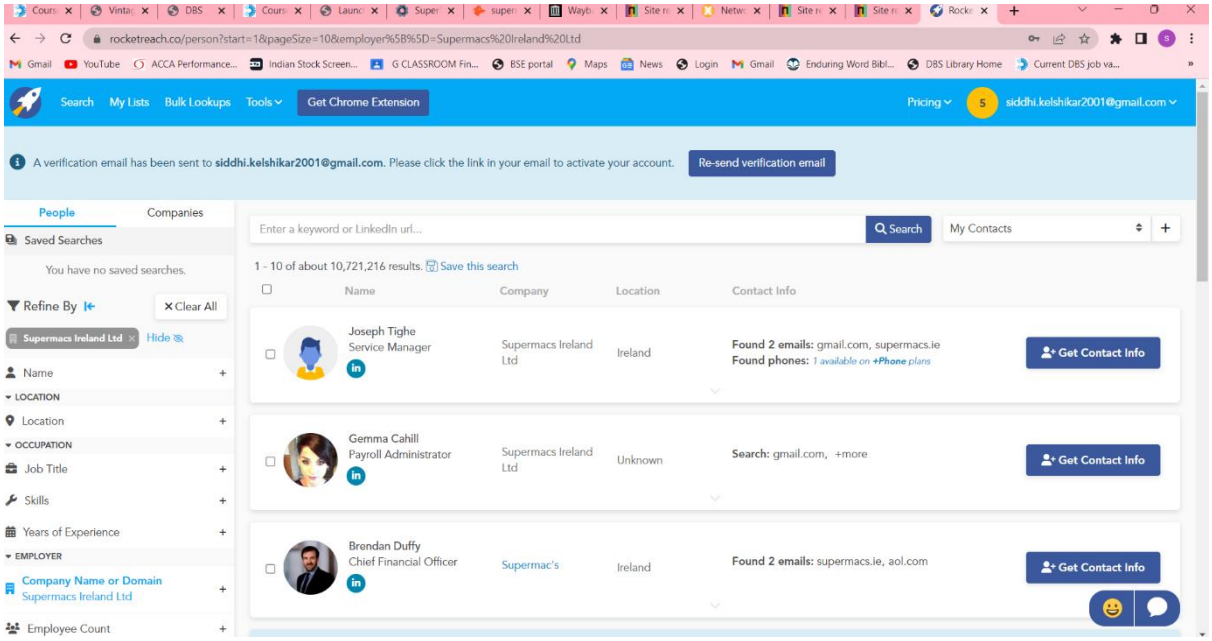
Operating system type The operating system Supermacs uses is ‘Linux’.
The link to find the same is:
https://sitereport.netcraft.com/?url=https://supermacs.ie



11. STAFF MEMBERS PHONE NUMBERS, PERSONAL DETAILS, EMAIL ADDRESSES

The Rocket Reach website has helped me to get the details of the employees.

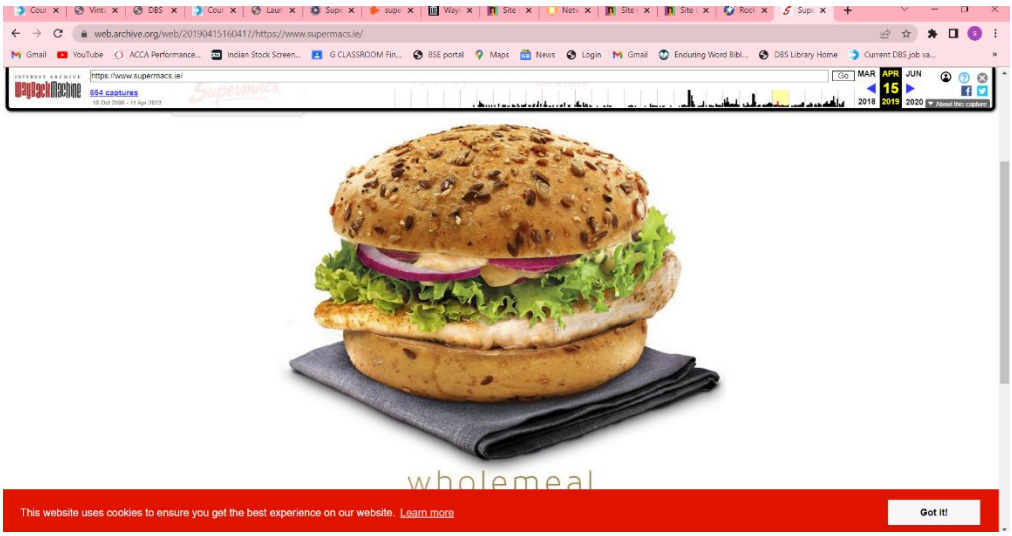
https://rocketreach.co/person?start=1&pageSize=10&employer%5B%5D=%22155424:Supermac%27s%22



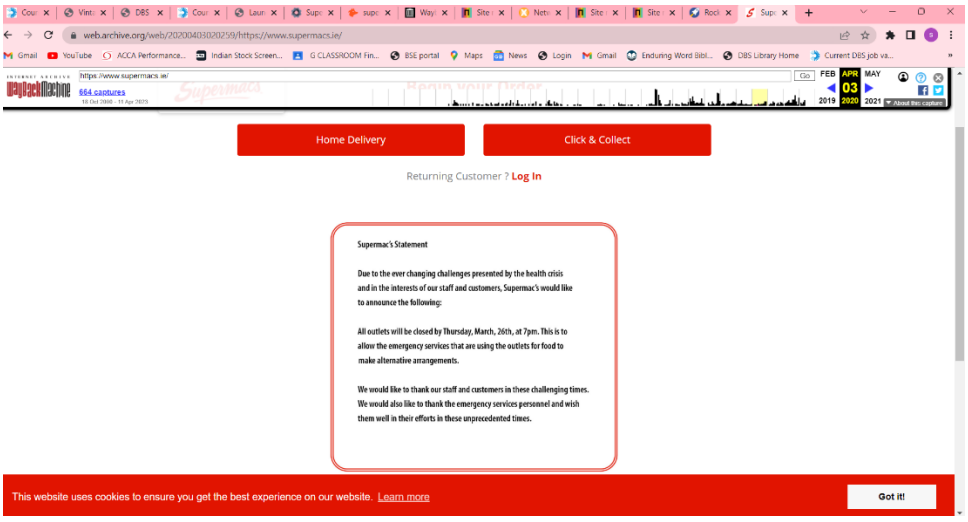
12. REMOVED WEB PAGES

Following are the details of the previous web pages
https://web.archive.org/web/20220720202311/https://supermacs.ie/

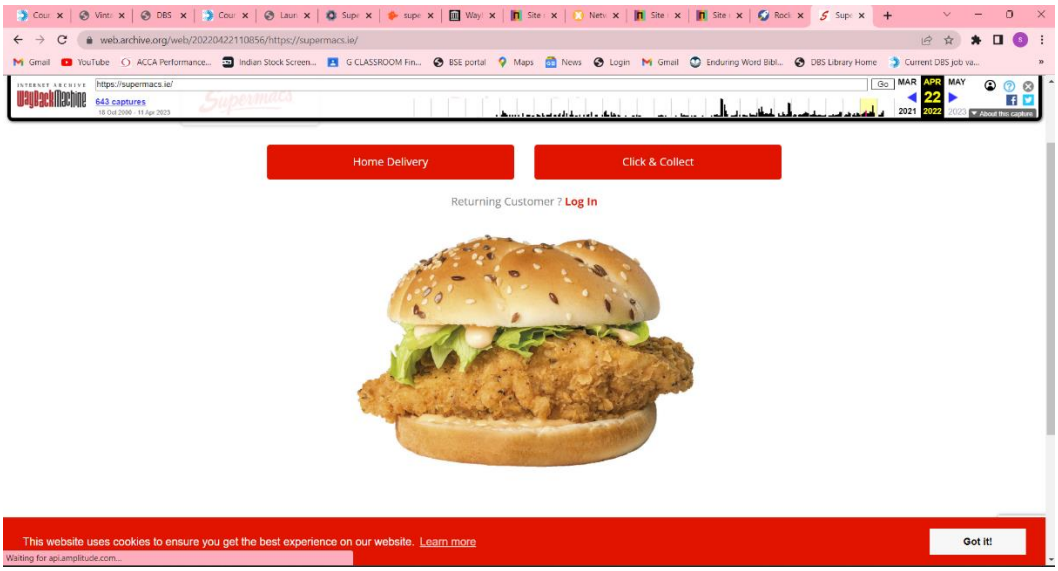
A snapshot of the website from the year 2019:



A snapshot of the website from the year 2020:



A snapshot from the website for the year 2022:



13.REFERENCES

Supermac's Ireland. (n.d.). Supermac's fast food restaurants | About Supermac's | Pat McDonagh. [online] Available at: https://supermacs.ie/about-supermacs/.

whois.domaintools.com. (n.d.). Whois Lookup Captcha. [online] Available at: https://whois.domaintools.com/supermacs.ie [Accessed 14 Apr. 2023].

Hunter. (n.d.). supermacs.ie • Hunter. [online] Available at: https://hunter.io/try/search/supermacs.ie?locale=en [Accessed 14 Apr. 2023]

web.archive.org. (n.d.). Wayback Machine. [online] Available at: http://web.archive.org/details/www.supermacs.ie [Accessed 14 Apr. 2023].

Pentest-Tools.com (n.d.). Website Vulnerability Scanner - Online Scan for Web Vulnerabilities. [online] Pentest-Tools.com. Available at: https://pentest-tools.com/website-vulnerability-scanning/websitescanner.

MxToolbox. (n.d.). Network Tools: DNS, IP, Email. [online] Available at: https://mxtoolbox.com/SuperTool.aspx?action=mx%3a45.60.115.150&run =toolpage [Accessed 14 Apr. 2023].

RocketReach. (n.d.). RocketReach - Find email, phone, social media for 450M+ professionals. [online] Available at: https://rocketreach.co/person?start=1&pageSize=10&employer%5B%5D=%22155424:Supermac%27s%22 [Accessed 14 Apr. 2023].

web.archive.org. (2022). Supermac's | Welcome to Supermac's family restaurants in Ireland. [online] Available at: https://web.archive.org/web/20220720202311/https://supermacs.ie/ [Accessed 14 Apr. 2023]