martin Petik

ID 279832

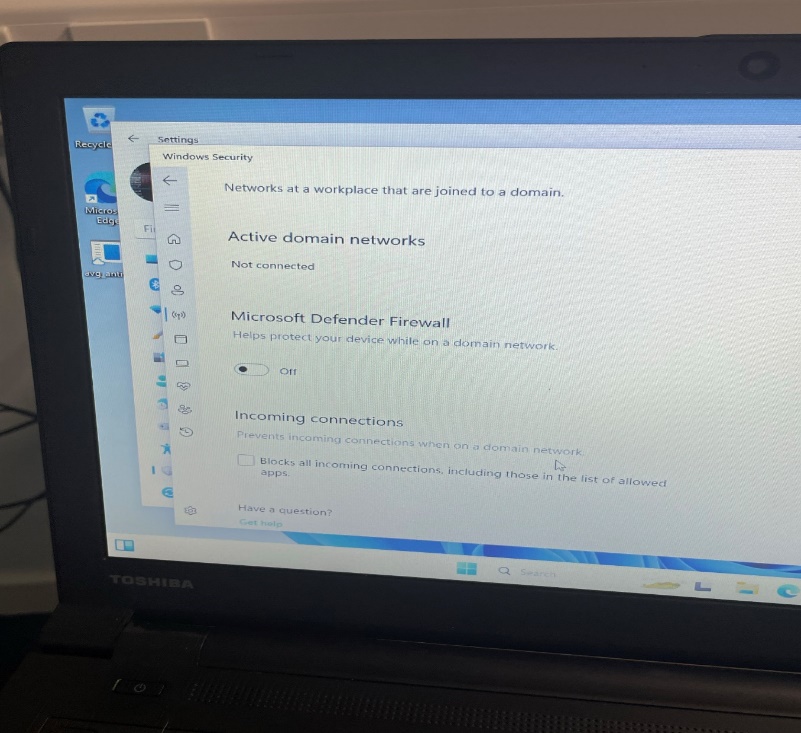
Unit 22 Task C

P4 Client Requirements/introduction

I have read the client requirements I understand from these requirements that I am required to implement and refine the enhanced security measures to protect a technology system. I have been asked to create security plan to test the modified system for functionality purposes and I have also read brief and I should take into consideration of the tools and techniques used for the technology system. I have also read that I must follow all health and safety guidelines I need to follow to avoid any accidents.

Furthermore, I have read tasks given and I am going to install updates changes the setting of the security software, next I am going to use and schedule a malware/antivirus scan and evidence that I have completed this. In addition, I have to resolve any technical difficulties that

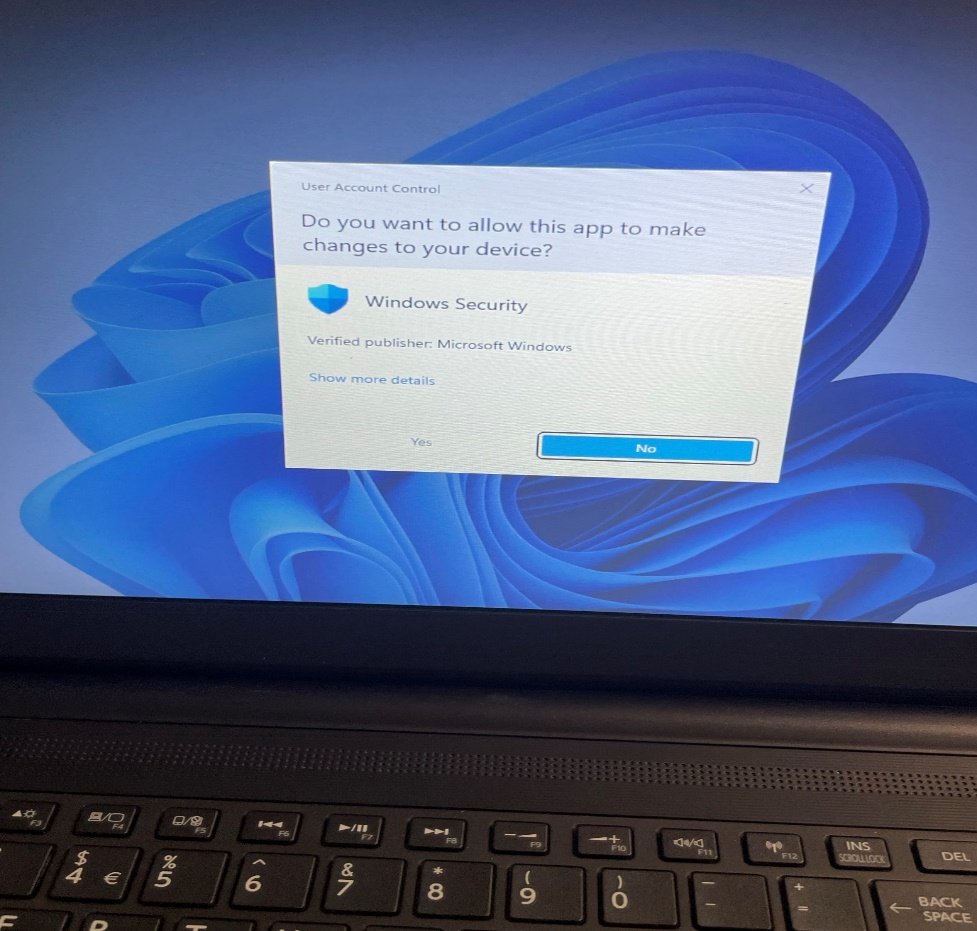
Setting up firewall

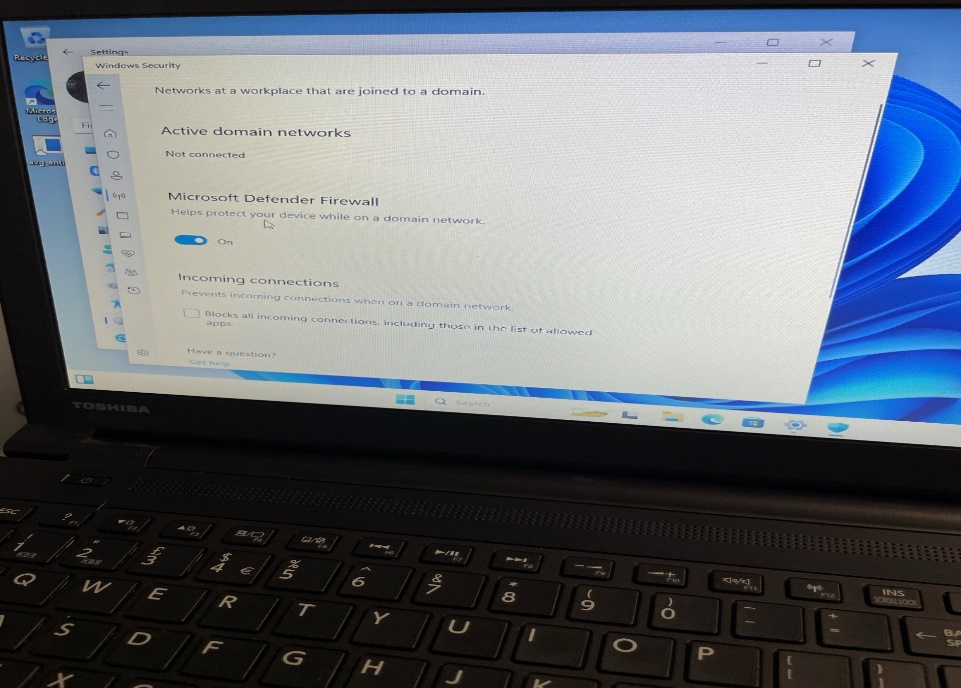


Fist I went on setting to check if the firewall was off, it was off so I turn it on

Because generally, you should never turn off the firewall on system Firewalls block malware and other malicious data that could sneak past a router or gateway's built-in firewall. They also block infected apps and programs installed on your computer.

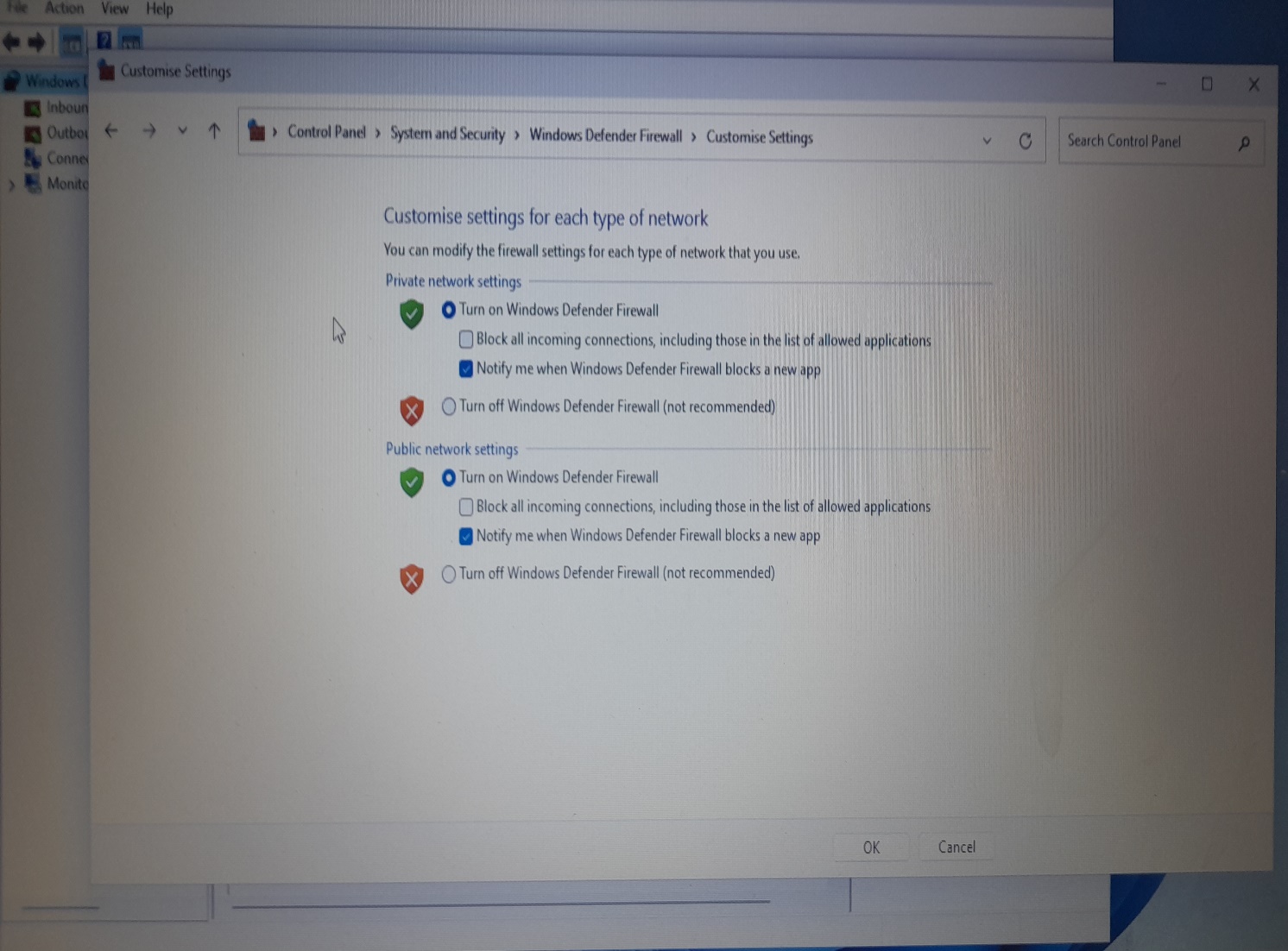
Then I was asked to allow this change to let the windows turn of firewall and modify system settings I click yes





I turned on because Windows Defender helps prevent hackers and malicious software from gaining access to your pc through the internet or network. Your organization might require you to turn it on before you can access their network resources from your device

Then I check if the firewall setting and enable the recommended setting and turn on a windows defender firewall



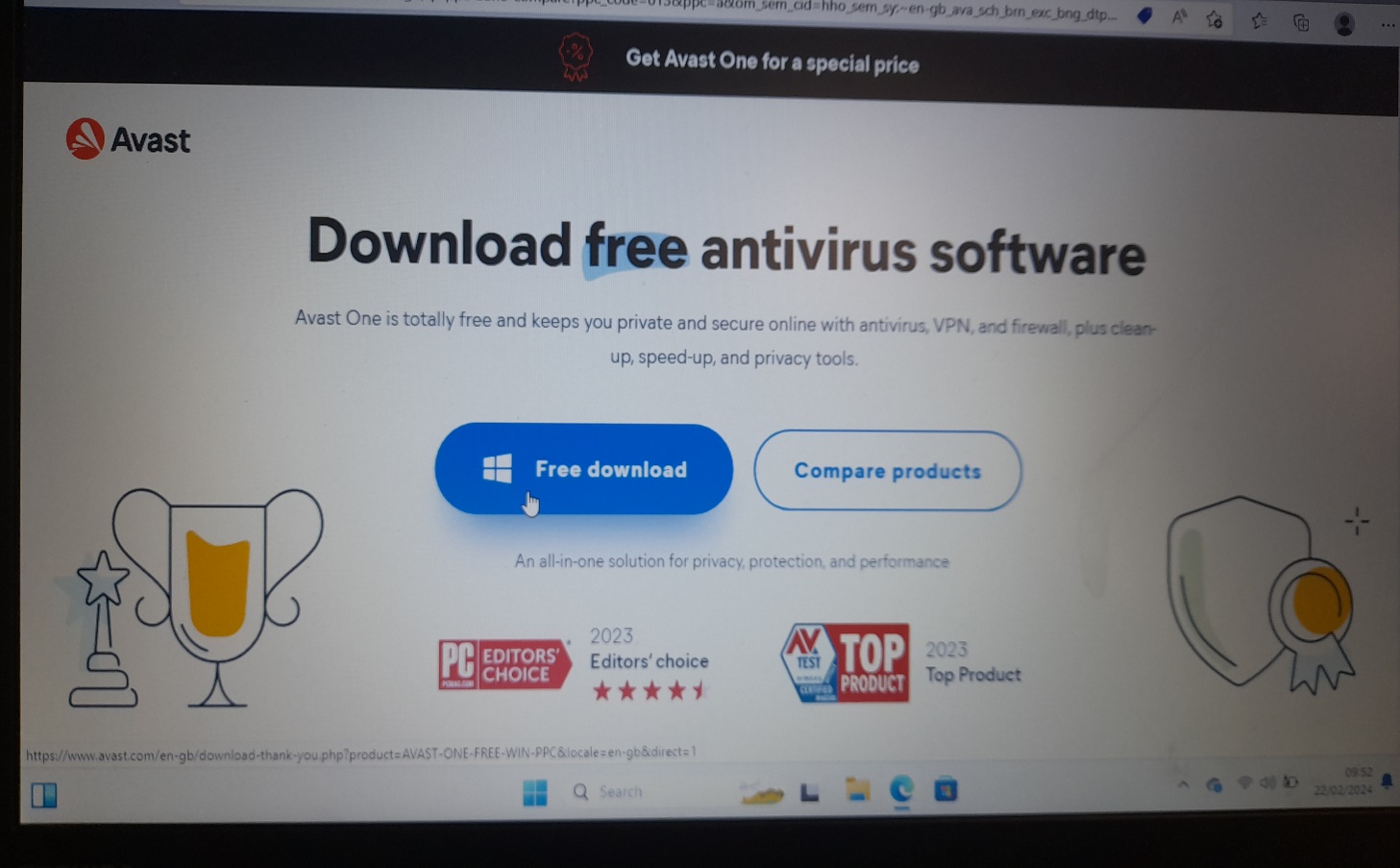
I choose recommended settings because it recommended by a system because “it just works” better without any confederation.

Also, why you need firewall?

Without a firewall, you could leave yourself open to accepting every connection to your home network without a way to detect incoming threats. This open access could leave your devices and personal information exposed and vulnerable to being accessed and used for malicious purposes.

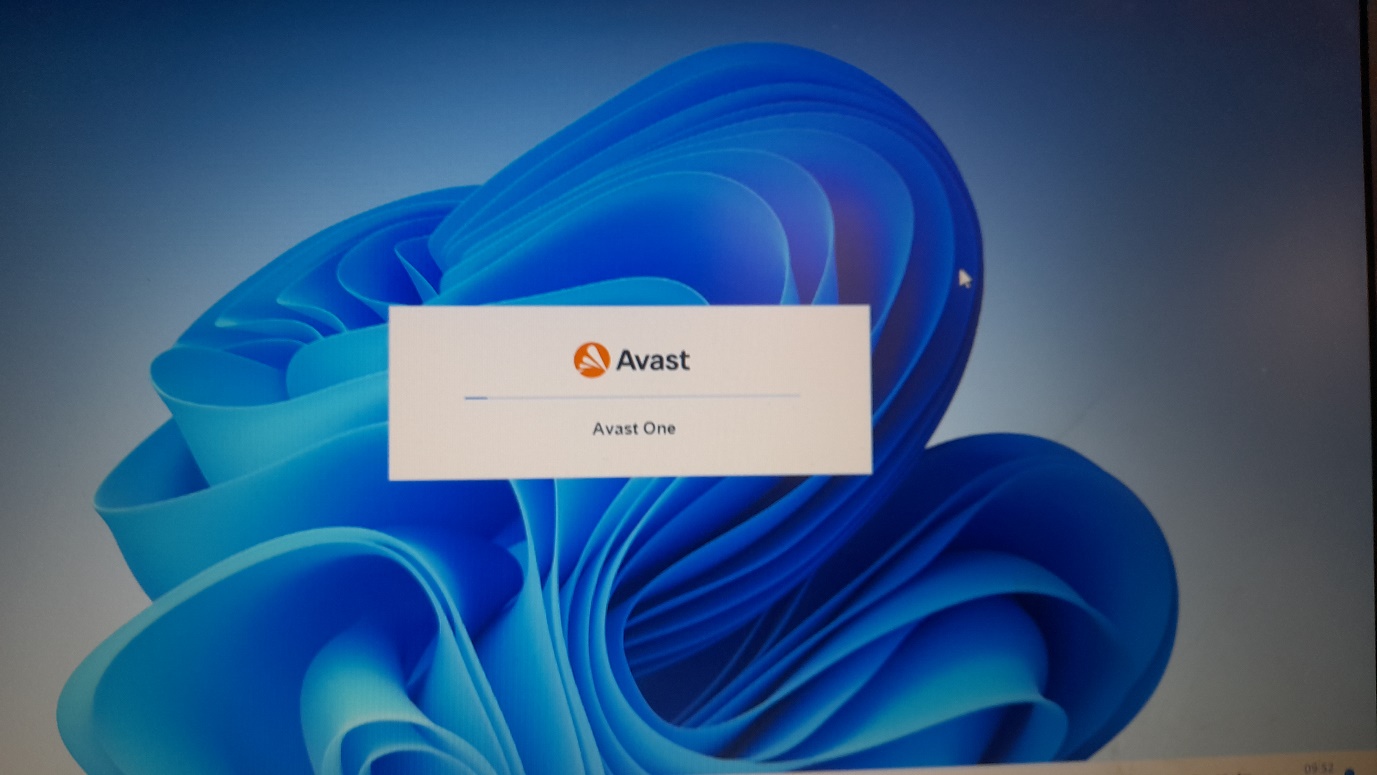
Setup up for Antimalware/antivirus software

Next, I downloaded a freeware antivirus/antimalware software that is called Avast and installed on computer



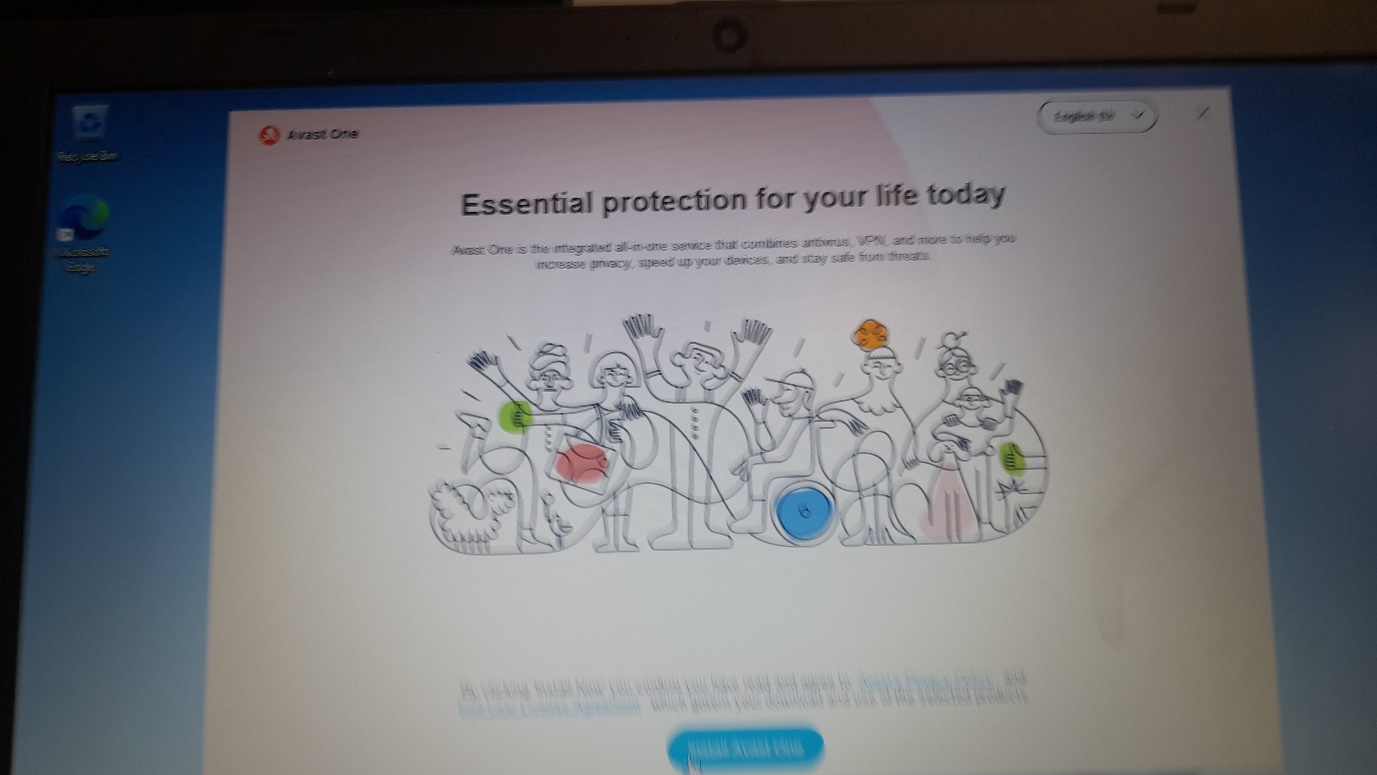
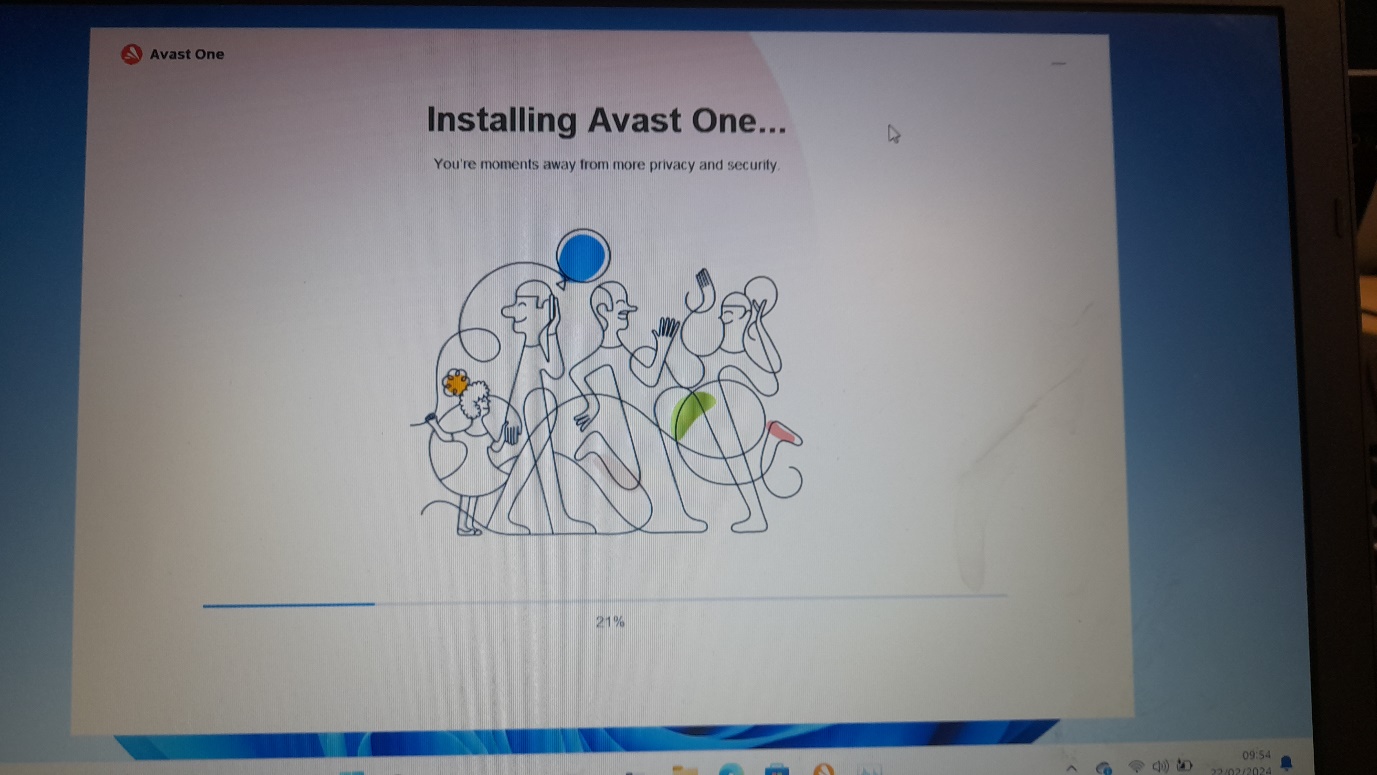
I choose Avast because as expected, Avast offers protection through malware scanning. It runs in the background to keep malware at bay whenever we open files or do something on our laptop – also known as on-access scanning – but it also lets us scan on-demand through the app's Smart Scan button.

After this the antivirus/antimalware installation process begin



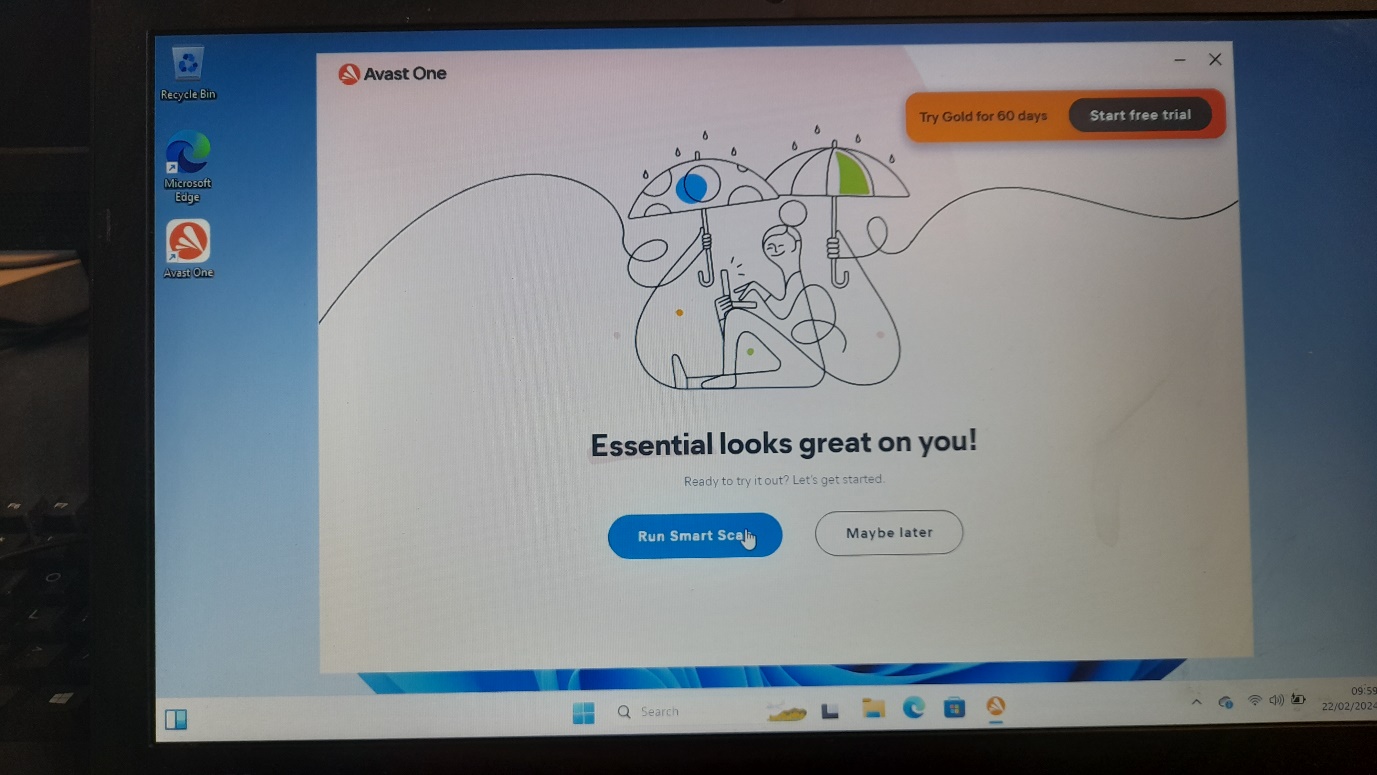


The installation of Avast is finished



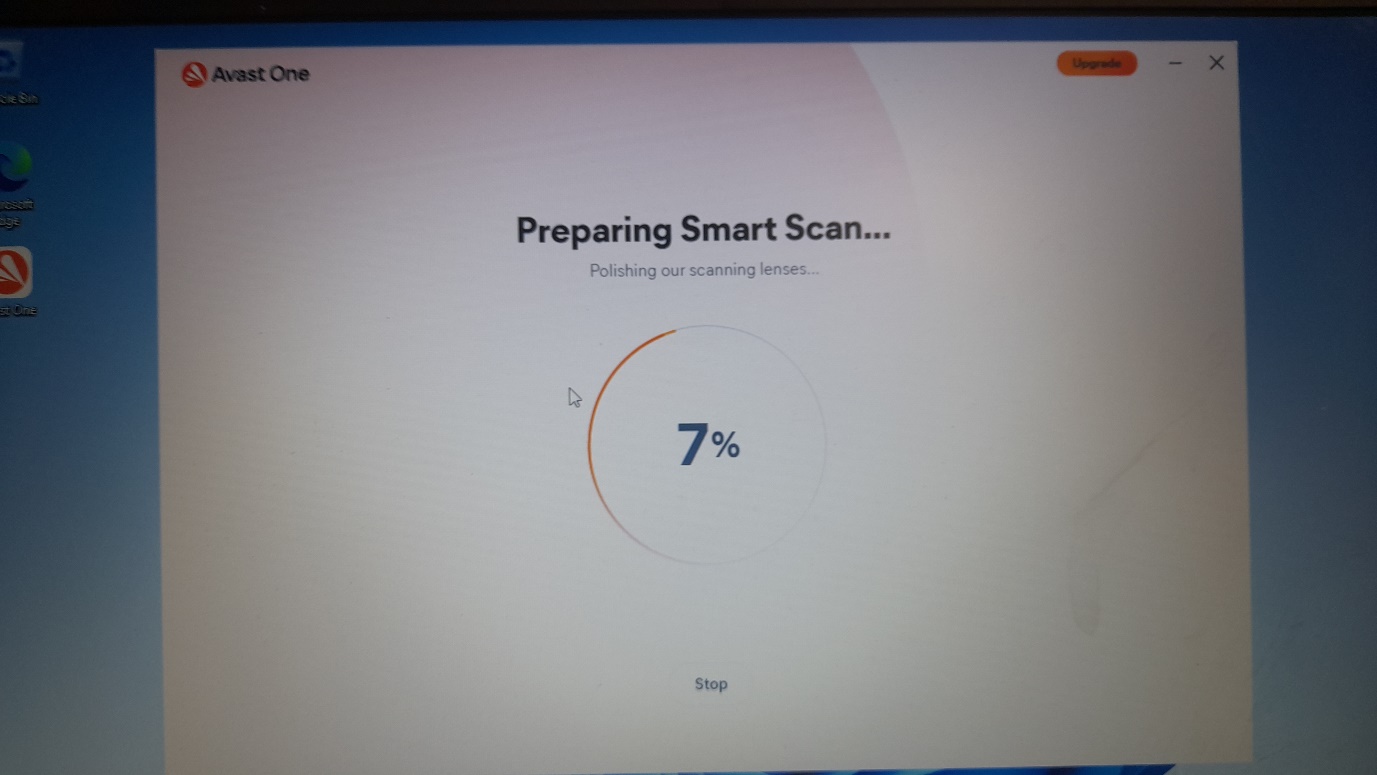
Scaning the device

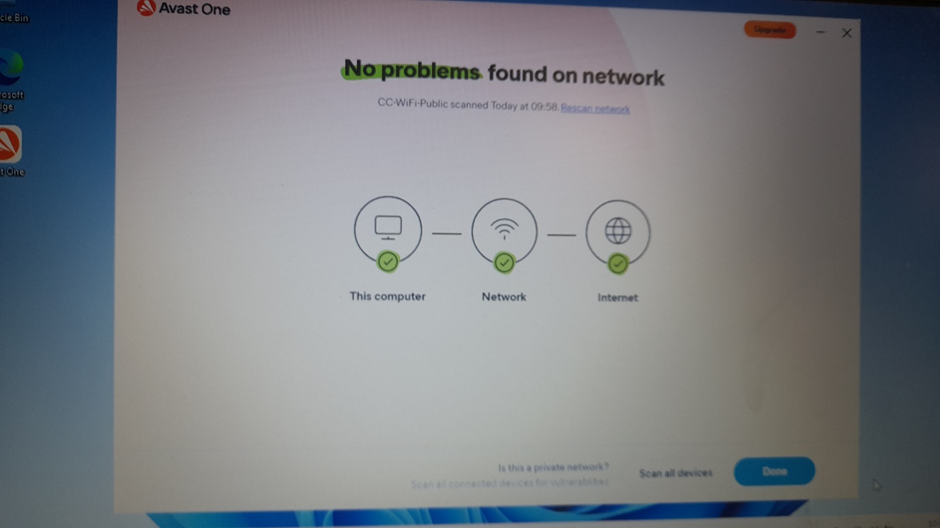
I click on smart scan because

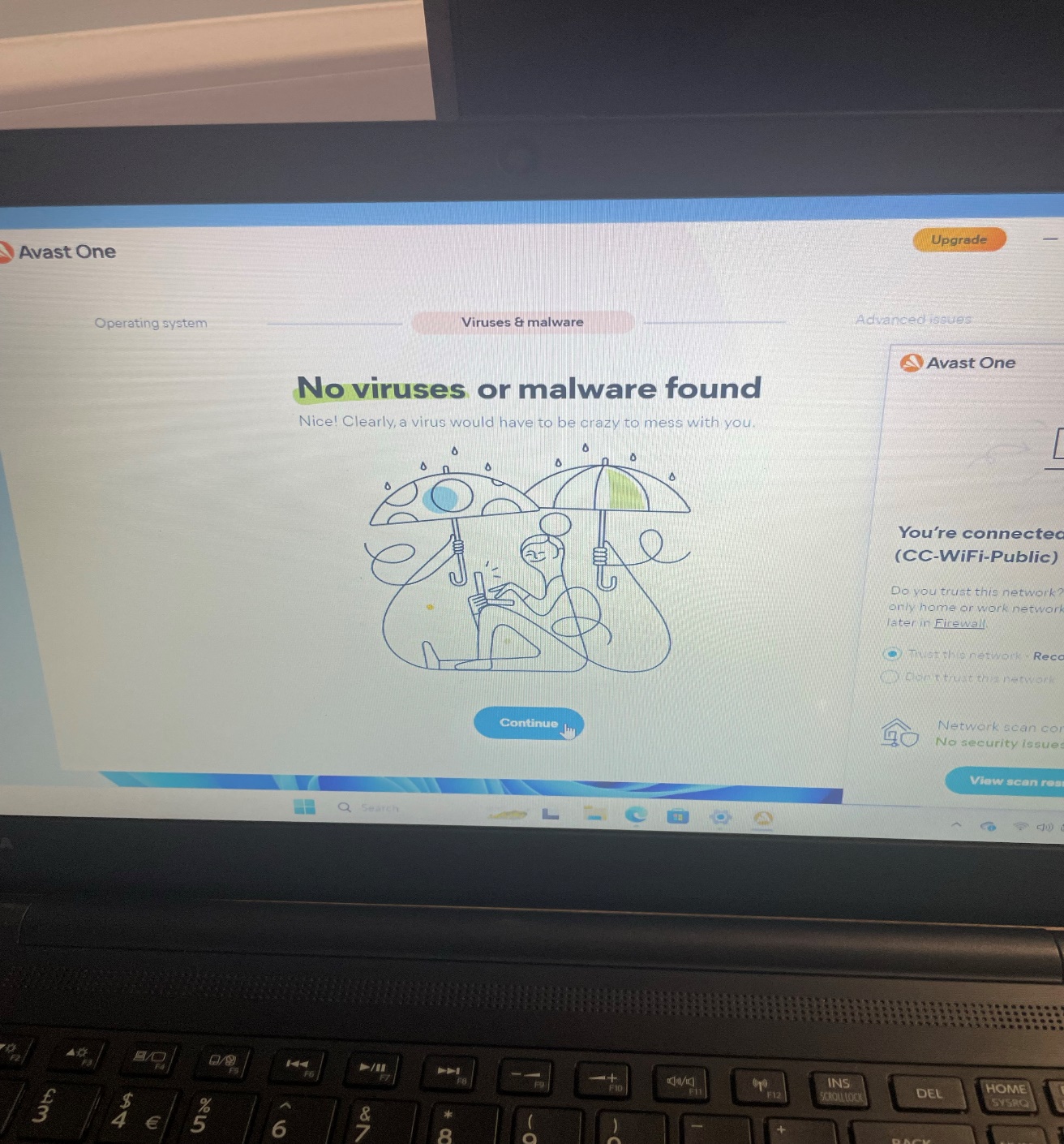


Smart Scan — A comprehensive scan that detects malware, out-of-date software, browser add-ons with poor reputations, network threats, and performance issues. Full Virus Scan — An in-depth scan of your system that checks all hard drives, rootkits, and auto-start programs.

What is Smart Scan? Smart Scan is a new technology from Trend Micro that utilizes a central scan server on your network take the burden of scanning off your clients and reduce the amount of network traffic. Enable Smart Scan to let the Smart Scan Server download all the necessary scan components and scan clients.

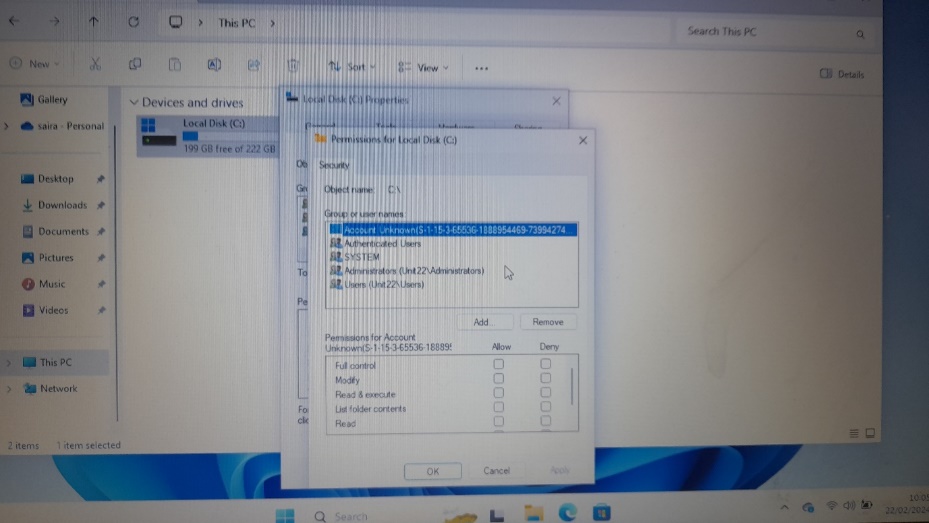


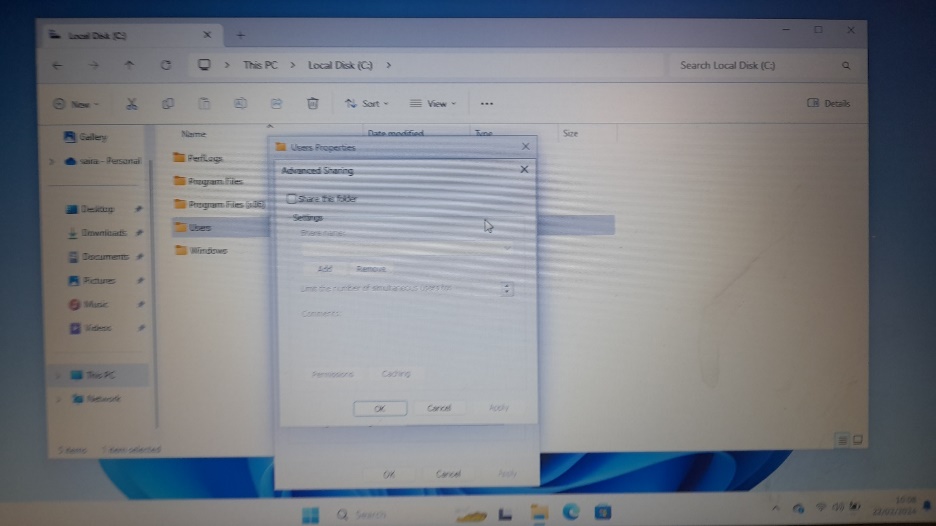




After it finished searching for problems is says that there were no problems finds

Restricting user acces





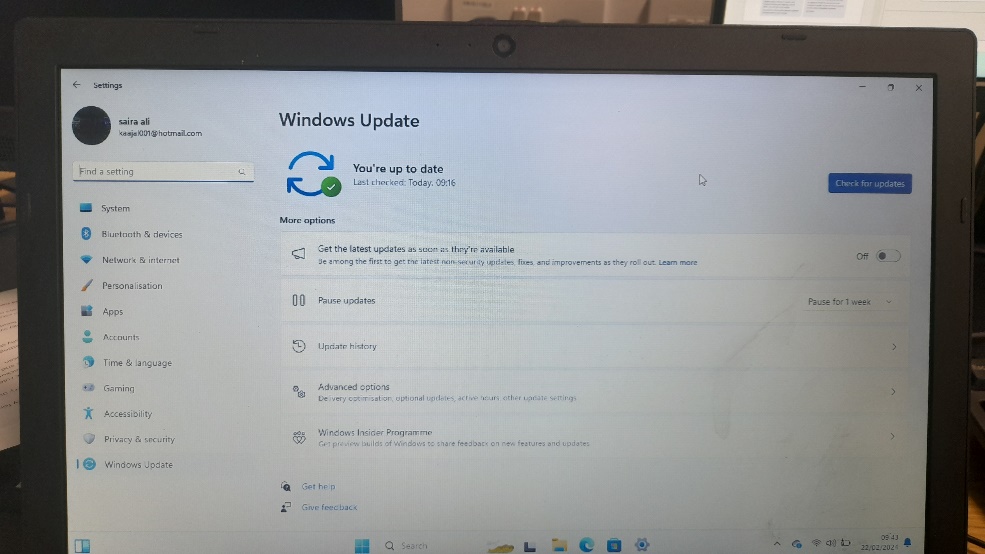
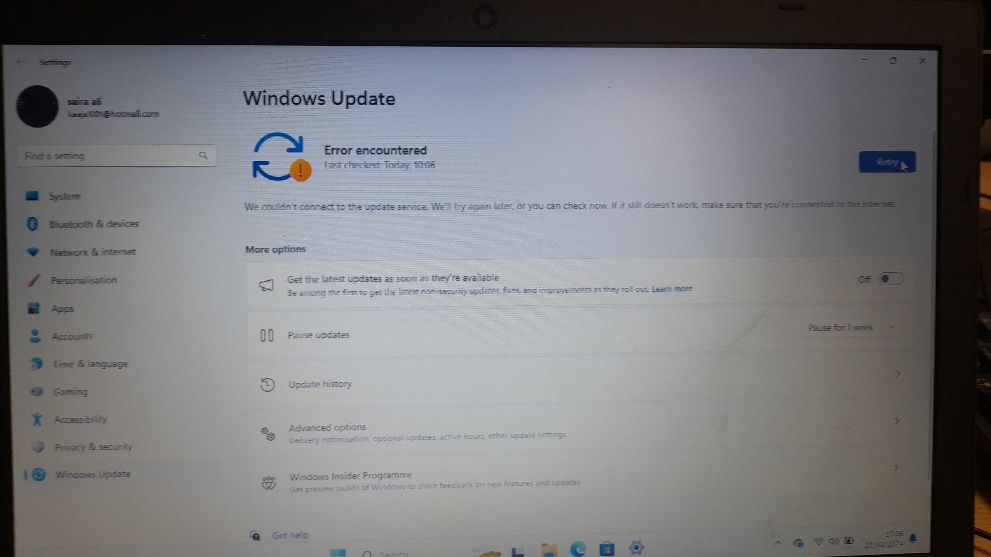
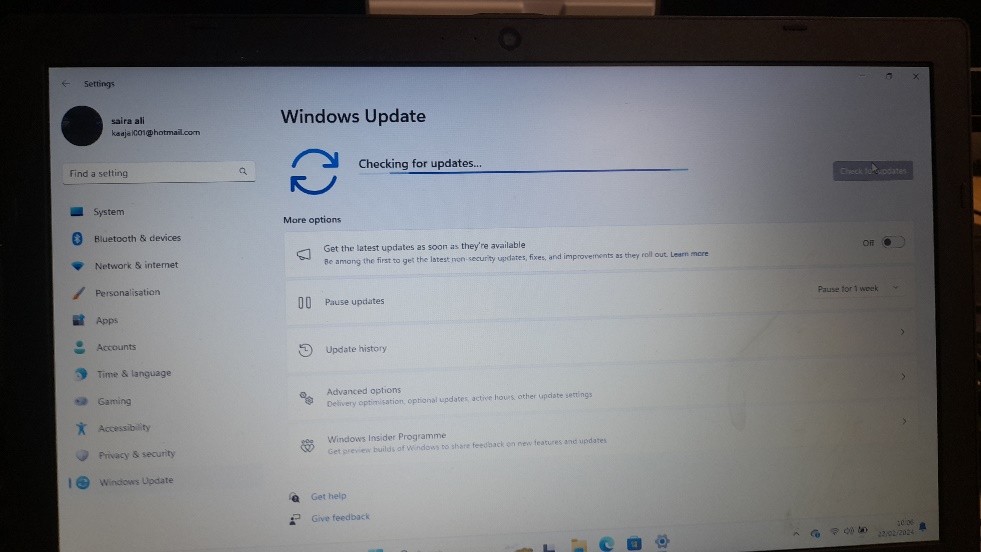
First I went on file maneger and click on local C click on properties then permission and restrict users access. And then add permision on computer such as full acces to folders,restrict users to make or delete files,delete files and read and write resctriction.

The reason why I am doing user access:

User access restrictions control access to functionality on various levels: They determine which functions users may access. This covers the access of UI pages and menus. In addition, the restrictions indicate which protected data may be accessed from the functions.

By limiting user access, you narrow the amount of data employees have access to — and incidentally can compromise — without having to go through any of your network's other defenses. This is a smart practice that we always recommend to every client to increase their organization's network and device security.

System update/software update



First I went on settings and click on windows update, and started the update.But error occure so I restart the system and doit again and it work and it sait that the system is uptodate

What is system update:

Software updates provide new and improved functionality while addressing existing issues, such as bugs and crashes. And with antivirus updates, the developers often continue to improve their products to keep you safe from new viruses and malware.

What is software update:

Software updates provide new and improved functionality while addressing existing issues, such as bugs and crashes.

why you should keep the system up to date:

It's important to keep your software up to date because updates enhance existing features, patch security flaws, add new security features, fix bug issues and improve performance for devices. Continue reading to learn more about software updates and how you can check if your software is up to date

1. Better overall PC performance

Updates are one of the most important parts of sustaining performance. Out-of-date software and hardware aren’t always prepared to handle complex tasks, particularly newer tasks related to products and services introduced after their initial release.

With that in mind, it’s important to incorporate updates as part of your regular PC maintenance. Most of the points we’ll cover tie back to upkeep and preventative measures, which are designed to help avoid problems. That leads to better performance and a smoother user experience day to day with less downtime.

2. More robust passive and active security

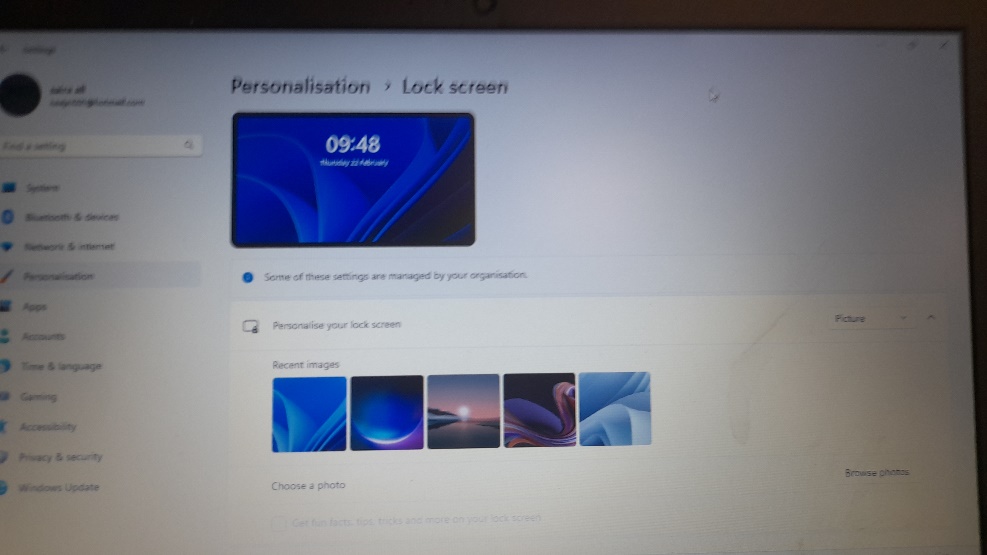
When you think about keeping your PC’s security features up to date, you may be considering any antivirus and spyware protection software on your device. However, the same benefits of updates apply to other software and hardware, because they’re often related to maintaining protection through the life of a device or component. When kept current, your software and hardware are much less vulnerable to tampering and hacks.

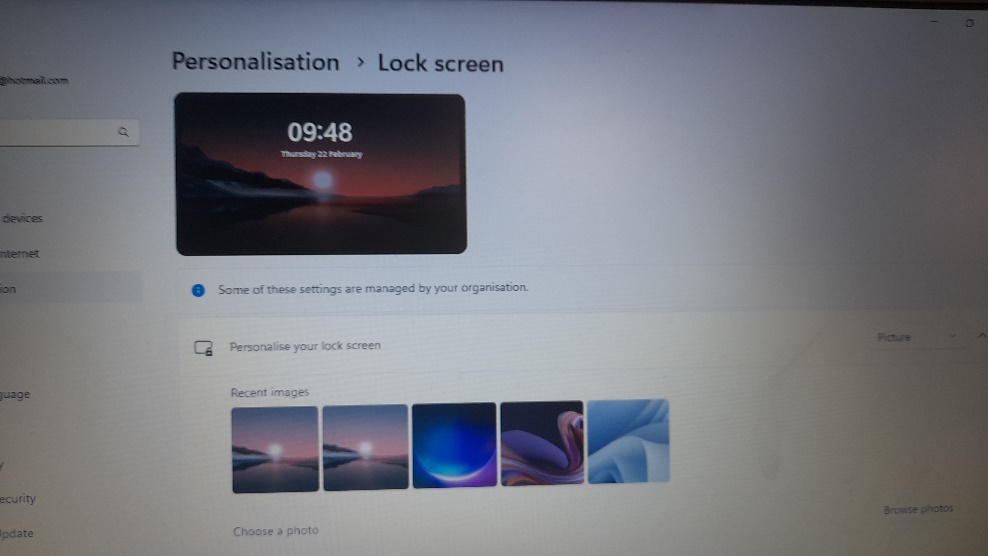
3. Optimised workflow for staff

For business users, including regular updates as part of your fleet management or office maintenance routine is a great way to boost efficiency. When you and your employees aren’t being interrupted by security or performance issues, everyone can stay focused on the task at hand.

There are similar benefits for family computers and household devices with multiple users. Staying on top of updates helps avoid issues for everyone involved, whether it’s a heavily used family computer or a fleet of networked devices.

Changing the system





First, I went on settings and clicked on personalisation and customise the look of windows/system for example change the picture, change the taskbar, and turn on dark mode. I did it by clicking :  
  
Open Settings > Personalization and select one of the default themes to change the background image, sounds, cursor, accent color, and color theme all at once. Open Themes to edit current themes, add new themes from the Microsoft Store, or create your own.

purpose of personalisation?

Personalisation means recognising people as individuals who have strengths and preferences and putting them at the centre of their own care and support. The traditional service-led approach has often meant that people have not been able to shape the kind of support they need, or received the right help.

Why is personalization important?

Personalization is important for a few reasons: It's the standard across several industries. Today, personalization is everywhere, and if you aren't offering it, customers may feel underwhelmed by your organization. It impacts customer sentiment.

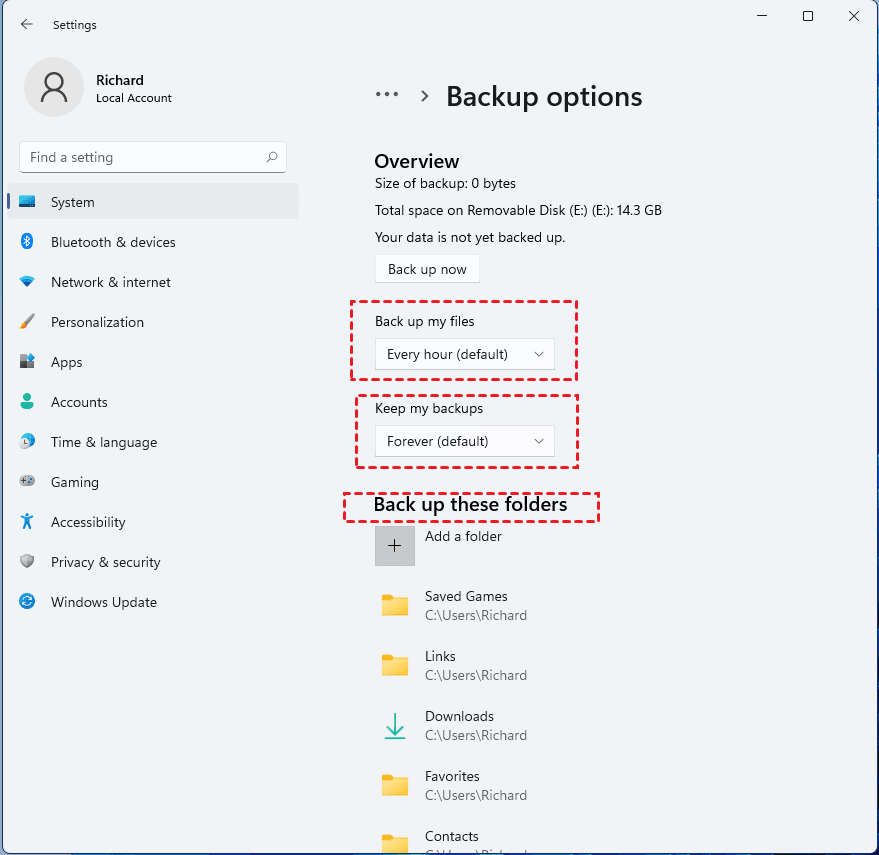
what is the purpose of Changing the system?

Applying systems change as an approach to complex challenges can help decision-makers pinpoint critical actions on which to focus, identify more effective solutions, and better understand the cascading impacts of various interventions.

what is Changing the system important

By changing systems, we can create large-scale, widespread change that has the potential to transform society as a whole. Another reason why system change is important is that it builds resilience. System change can create more resilient societies that are better equipped to deal with future challenges.

**Data Backup**



First, I went on settings and clicked on accounts and then on manage sync settings also I went on system setting and clicked on backup opinions. I choose to backup my folders every hour and to keep my backup forever basically (default settings)

The Importance of Backups

Making backups of collected data is critically important in data management. Backups protect against human errors, hardware failure, virus attacks, power failure, and natural disasters. Backups can help save time and money if these failures occur.

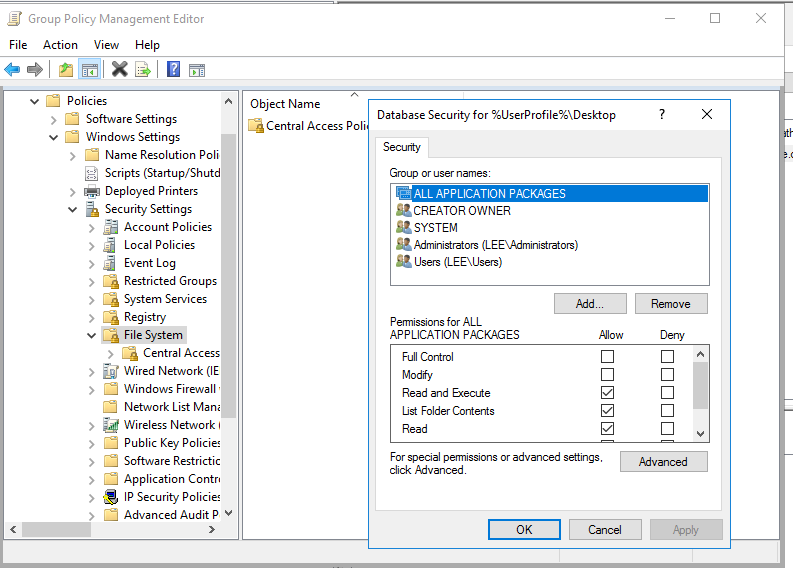
The purpose of the backup

is to create a copy of data that can be recovered in the event of a primary data failure. Primary data failures can be the result of hardware or software failure, data corruption, or a human-caused event, such as a malicious attack (virus or malware), or accidental deletion of data.

why to do daily backups

By backing up every day, you can be sure you aren't missing anything important, even if something goes wrong overnight. Daily backups are especially easy if you take advantage of an IT company's data backup solutions.

**Preventing External Access to Local Storage**



First, I went to file manager then I clicked on properties and then click on security and restrict users

why to Preventing External Access to Local Storage

Underlying storage mechanisms may vary from one user agent to the next. In other words, any authentication your application requires can be bypassed by a user with local privileges to the machine on which the data is stored. Therefore, it's recommended not to store any sensitive information in local storage.

What are the advantages and disadvantages of local storage?

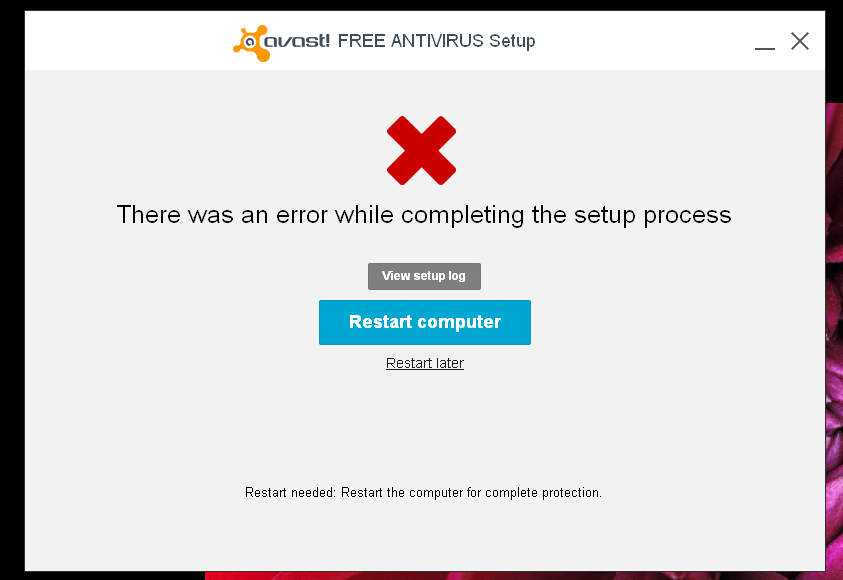
Limited Scalability: Local storage has finite capacity, which can be a limitation as your data needs grow. You may need to invest in additional hardware as your storage requirements increase. Data Redundancy: Local storage does not inherently offer data redundancy or disaster recovery capabilities.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test number | Task | Expected result | Actual result | Adjustment & solution (if any) |
| 1 | Setting up firewall | Confirm proper firewall set up and rule changes, verify firewall is enabled | I have successfully managed to check the activation of the firewall and system is protected. |  |
| 2 | Data backup | Ensure data integrity and availability through backups. Initiate manual backup | Verify backup completion and integrity. Schedule and validate an automated backup. Test data restore from the backup |  |
| 3 | Installing anti-virus/malware protection | I would expect an ant-virus/Mawere software work successfully also that it isn’t bloat ware | When I was installing the antivirus/malware software on the system, encountered installation error | To fix this I went on control panel to remove the anti-virus/malware software then I rebooted the system and install it again |
| 4 | Restricting user acces | Limited an Invidia’s access to specific authority premises. | Restricting guest and user from accessing sensitive or confidential information  From being accessed by unauthorized users |  |
| 5 | System update/software | Update the system, drivers and software.  Also, to make the system faster and debug the OS. | There was an error when was is checking for update it said we couldn’t check for update | I restarted the system and everything work as expected |
| 6 | Changing the system | be able to customize the OS look and feel | users can only customize the colors of task bar and wallpaper |  |

Test the additional functionality, repairing any faults

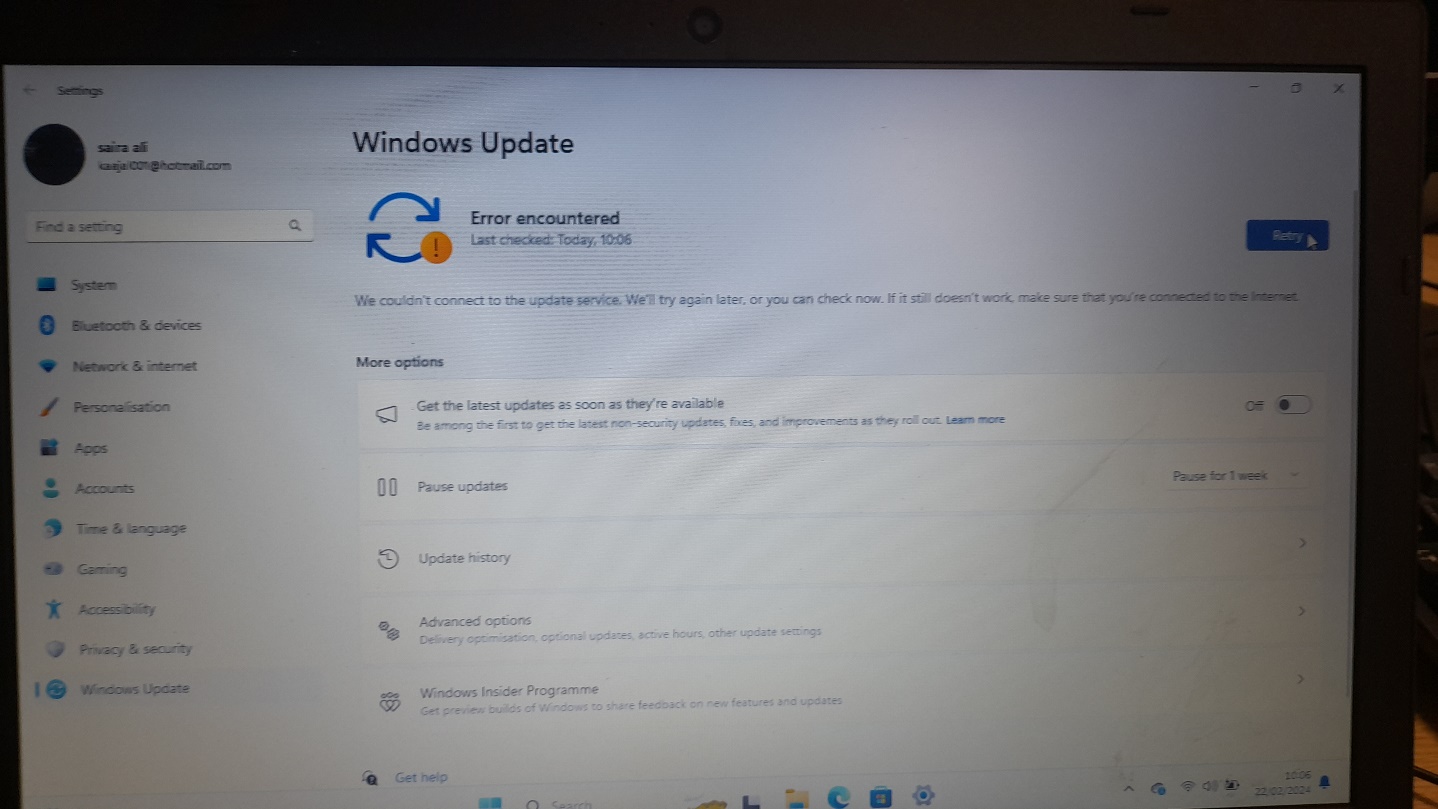
When crating my test plan, I had one error and that was the anti-virus that I installed originally, I have included a screen shot that shows this anti-virus installation as failed and to resolve this issue I deleted it from system restart the system and then I went to reinstall the software. this screenshot shows that I had an issue with Avast to resolve this I went into the control panel to uninstall and then reinstall the files. when testing all of my security tasks and I have tested the additional functionality of each of tasks and this has been successful.

As shown above I have only had one fault with the security software and it was easy because I just had to uninstall and reinstall the software



Also, when crating my test plan, I had another error and that was the updating the system, I have included a screen shot that shows this system update installation as failed and to resolve this issue restart the system. this screenshot shows that I had an issue with windows update to resolve this I went into the start and click on power button and chose restart. when testing all of my updating system tasks and I have tested the additional functionality of each of tasks and this has been successful.

As shown above I have only had one fault with the update manager and it was easy because I just had to restart the system



Employee policy

IT services are made available to a wide range of users on a conditional basis. All users of the zdisoft services must comply with this Acceptable Use Policy, which additionally incorporated the JANET Acceptable Use Policy. This policy applies to all zdisoft and personal devices, regardless of who owns the device, Breaches of this policy constitute a breach of the zdisoft Regulations and shall be subject to investigation.

All zdisoft employee have access to the following:

• Reasonable access to computers and printers.

• A personal user account stored on zdisoft systems with at least 10GB of storage space.

• An Email account which you can access from within company building or any internet connected computer system, powered through Microsoft Office365.

• Filtered access to the internet which you can use for work or other activities. (Review section ‘Web Filtering Policy’)

• Free wireless access for personal devices. In return, students are required to act in a responsible, ethical and legal manner.

In return, employees and staff are required to act in a responsible, ethical and legal manner.

* 1. **Acceptable Use**

• Registered users are encouraged to use the zdisoft IT services to further the goals and objectives of their work, study and research.

• ‘Personal use’ of the zdisoft IT services is permitted but only on a conditional basis providing it does not cause unwarranted expense, risk or liability, or reputational damage to the zdisoft company to be incurred by the zdisoft or otherwise impact upon the delivery of services to others through its scale or nature.

Use of Personal devices through the CC-ZDISOFT-USER Wireless system, which requires a registered user log in.

* 1. **Unacceptable use**

Unacceptable use includes, but is not limited to, the following activities (Other than for properly supervised and lawful research purposes), some of which may be unlawful in certain circumstances.

• Take part in any illegal activity. The Police will be informed where there is evidence of illegal activity

• Store, e-mail or publish comments which are defamatory to others, or which could constitute bullying or harassment in any form.

• Attempt to gain unauthorized access to zdisoft systems or external networks (Hacking).

• Attempt to install your own software on zdisoft Systems.

• Using Hacking/Proxy Avoidance Systems

• Disclose private information about other people. Please be careful about giving other people personal information about yourself – they may not be who they say they are.

* 1. **Web Content Filtering Policy**

zdisoft uses Firewalls to control its web filtering. The Firewall automatically blocks websites under common filters that relate to content considered offensive, obscene, indecent, defamatory or which advocate violent, illegal or discriminatory activities, as stated above. The zdisoft reserved the right to filter content to sites manually alongside this. zdisoft staff and employees have access to computer control software, allowing them to filter access to specific websites, or full internet access, on a class-by-class basis. Should an End User believe that a site has been incorrectly blocked, they can discuss this with their tutor, who can send through a request to the ITSU helpdesk unblock a site. at the discretion of the ITSU and the safeguarding team, the site may be unblocked.

* 1. **UK Legislation**

Users must comply with all UK legislation relating to the use of information, computers and networks. Applicable laws include: a. PREVENT Strategy. Government’s counter terrorist strategy b. Data Protection Act 1998. This act makes provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. For more information, please contact the Head of MIS. c. Computer Misuse Act 1990. The act provides safeguards for computer material against unauthorised access or modification. d. Fraud Act 2006. The Act prohibits ‘phishing’ whereby official-looking emails guide unsuspecting users to fake websites (e.g., fake bank websites) in order to steal their login details. Creating or possessing software to enable this activity is also an offence.

**Employee Policy for Cybersecurity**

This cyber security policy is for our employees, suppliers, and customers to refer to when they need advice and guidelines related to cyber law and cybercrime. Having this cyber security policy, we are trying to protect Blackwood Plant Hire Ltd.’s (BPH) data and technology infrastructure. This policy applies to all of BPH employees, suppliers, and anyone else who may have any type of access to BPH systems, software and hardware.

Examples of Confidential Data

Some of the common examples of confidential data include:

• Classified financial information.

• Customer data.

• Data about suppliers.

• Technology and technical data.

Device Security- Using personal devices.

Logging in to any of company's accounts from personal devices such as mobile phones, tablets or laptops, can put our company's data at risk. BPH prohibits accessing any restricted company's data from personal devices unless authorised by BPH Managing Director. If authorised, staff are obligated to keep their devices in a safe place, not exposed to anyone else.

All employees must follow best practices as below:

• Keep all electronic devices' password secured and

protected.

• Logging into company's accounts should be done only through safe networks.

• Install security updates on a regular basis.

• Upgrade antivirus software on a regular basis.

• Do not leave your devices unprotected and exposed.

• Lock your computers when leaving the desk.

Email Security

Email Security Emails can carry scams or malevolent software. In order to avoid virus infection or data theft, all employees must:

• Abstain from opening attachments or clicking any links in the situations when its content is not well explained.

• Make sure to always check email addresses and names of senders.

• Search for inconsistencies

• Be careful with clickbait titles (for example offering prizes, advice, etc.)

In case that an employee is not sure if the email received, or any type of data is safe, they can always contact our IT specialist.

To ensure avoiding that your company account password gets hacked, use these best practices for setting up passwords:

Managing Passwords

• At least 8 characters (must contain capital and lower-case letters, numbers and symbols)

• Do not write down password and leave it unprotected

• Do not exchange credentials when not requested or approved by supervisor

• Change passwords every [x] month

Transferring Data

Data transfer is one of the most common ways cybercrimes happen. Follow these best practices when transferring data:

• Avoid transferring personal data such as customer and employee confidential data

• Adhere to personal data protection law

• Data can only be shared over company's network

Working Remotely

Even when working remotely, all the cybersecurity policies and procedures must be followed.

Disciplinary Action

When best practices and company's policy are not followed, disciplinary actions may take place. Some of the examples of disciplinary actions include:

• In case of breaches that are intentional or repeated, and are harmful to the Company, or its clients. BPH will take serious action which could result in termination of employment.

• Depending on how serious the breach is, verbal/formal written warnings will be issued in line with current HR policies.

• Each case and incidence will be assessed on a case-by-case basis.

**M4 Test the additional functionality, repairing any faults, and gather feedback from others**

Feedback from client about my system and what went wrong

Reviewer name: Mohamed Haaris

Date 02/05/2024

I have successfully tested the system which Haaris has done and it works but there were a few errors such as the windows system wasn’t updating and encountering an error. To fix this error I had to try again by restarting the system after that the windows update work as expected

(CHANGE THIS)

**D3: Refine the modified technology system in order to improve protection against security threats, taking account of feedback from testing.**

1. Identify Security Vulnerabilities: The first step in refining the modified technology system is to identify any security vulnerabilities that may compromise the system's integrity. This can be achieved by conducting a thorough assessment, including vulnerability scans and penetration testing.
   1. security instead of windows use Linux or FreeBSD, OpenBSD or any free OS instead of free antivirus use a premium or Foss/FOSS alternatives
2. Analyse Feedback from Testing: Testing is a critical component of any technology system's development, as it allows for the identification of weaknesses and areas for improvement. Feedback from testing, such as bug reports, system logs, and user feedback, should be analysed to identify specific security threats and vulnerabilities.
3. Implement Security Measures: Based on the analysis conducted in the previous step, appropriate security measures should be implemented to strengthen the modified technology system. This may include implementing robust authentication mechanisms, encryption techniques, and regular updates to software and security patches. Additionally, access controls and privilege management should be implemented to limit access to sensitive data and resources.
4. Communicate Security Updates: Finally, it is important to communicate any security updates made to the modified technology system to all relevant stakeholders. This includes employees, customers, and partners, to ensure that everyone is aware of the enhanced security measures and knows how to adhere to them responsibly.
5. Monitor and Maintain Security: To ensure continuous protection against security threats, it is crucial to monitor and maintain the modified technology system. Regular security audits, intrusion detection systems, and intrusion prevention systems can be employed to detect and respond to potential attacks. Additionally, implementing an incident response plan can help mitigate the impact of security breaches and speed up the recovery process.
6. Conclusion: Refining the modified technology system to protect from security threats is an ongoing process that requires continuous evaluation and improvement. By identifying vulnerabilities, analysing feedback from testing, implementing appropriate security measures, monitoring and maintaining the system, and communicating updates, organizations can safeguard their digital assets and mitigate the risks posed by cyber threats.