THE CYBER SECURITY WORKSHOP

Artifact

By,
Hacker Zone Club,

LOYALiST COLLEGE

APRIL 22, 2023

LOYALIST COLLEGE
376 Walbridge Loyalist Rd, Belleville, ON, K8N 5B9

Activity and Document Details

Document Version Control:

Document Title	The Cyber Security Workshop
Document ID	
Document Version	1.2
Prepared by	Hacker Zone Club
Classification	Controlled and Public

Document Submission Details:

Date	22nd April 2023
Classification	Controlled and Public
Document Type	Artifact
Submitted To	
Address	
Email	

Document Distribution List:

Sr. No.	Name	Organization	Purpose
01	Harkirat Mann	Loyalist College – Hacker Zone Club	Author
02	Mohamed Sufiyan Shaikh	Loyalist College – Hacker Zone Club	Author
03	Saurabh Alate	Loyalist College – Hacker Zone Club	Author
04	Umar Khan	Loyalist College – Hacker Zone Club	Author
05	PathikKumar Patel	Loyalist College – Hacker Zone Club	Author
06	David Peterkin	Loyalist College – Hacker Zone Club	Author
07	Terry Boyd	Loyalist College – Prof./Coordinator	Reviewer
08	Ken Brooks	Loyalist College - SCWI	Approver

Abstract

The home network security workshop is a comprehensive training program designed to equip individuals with the necessary knowledge and skills to secure their home networks and devices. Over the course of six hours, participants will learn the basics of network security, Wi-Fi security, securing their devices, identifying, and avoiding malware and phishing attacks, and setting up network monitoring and parental controls. Practical demonstrations will be used to enhance learning and to provide participants with hands-on experience in accessing router settings, testing the strength of Wi-Fi passwords, setting up antivirus programs, and configuring parental controls on a router. The workshop will conclude with a Q&A session to address any specific concerns and provide additional resources for continued learning and support. By the end of the workshop, participants will have gained a comprehensive understanding of home network security and the necessary skills to protect their home networks and devices from potential threats.

Contents

INTRODUCTION

Our objective for the workshop is to provide you with the knowledge and tools you need to secure your home network and protect your devices from potential threats.

Why does home network security matter, you might ask? Well, our homes have become increasingly connected, and we rely on our home networks for everything from streaming movies to online shopping to working remotely. However, with this convenience comes the potential risk of cyber-attacks that can compromise our personal information and disrupt our daily lives.

To start, we will go over some basic terminology and concepts of network security. This will include routers, firewalls, encryption, and more. We will then have a practical demonstration on how to access your router's settings and configure basic security features.

In the second module, we will focus on Wi-Fi security. We will discuss Wi-Fi encryption, such as WEP, WPA, and WPA2, and why it is important to change your Wi-Fi network's name and password regularly. We will also have a practical demonstration on how to test the strength of a Wi-Fi password and change it on a phone or laptop.

Followed by securing your devices, including phones, laptops, and IoT devices. We will discuss the importance of basic security settings, such as passwords, updates, and antivirus software, and we will have a practical demonstration on how to set up and use an antivirus program on a laptop.

The fourth module will focus on malware and phishing, which are types of cyber-attacks that can harm your network and devices. We will discuss how to recognize and avoid common types of malware and phishing attacks, and we will have a practical demonstration on how to spot and avoid phishing emails and links on a phone or laptop.

Once we are done with malware and phishing, we will cover network monitoring and parental controls. We will discuss how to monitor your network traffic and identify potential security issues, as well as the benefits of parental controls in protecting your family from online dangers. We will have a practical demonstration on how to set up network monitoring and parental controls on a router.

Finally, we will have a Q&A session to answer any remaining questions and address specific concerns. We will also recap the workshop's key concepts and takeaways and provide you with resources for further learning and support.

we hope that you find this workshop informative and useful in securing your home network. Let us get started!

DOMAIN 1: INTRODUCTION TO HOME SECURITY

DEFINITION:

Home network security refers to the protection of a network that connects devices—such as routers, computers, smartphones, and Wi-Fi-enabled baby monitors and cameras—to each other and to the internet within a home.

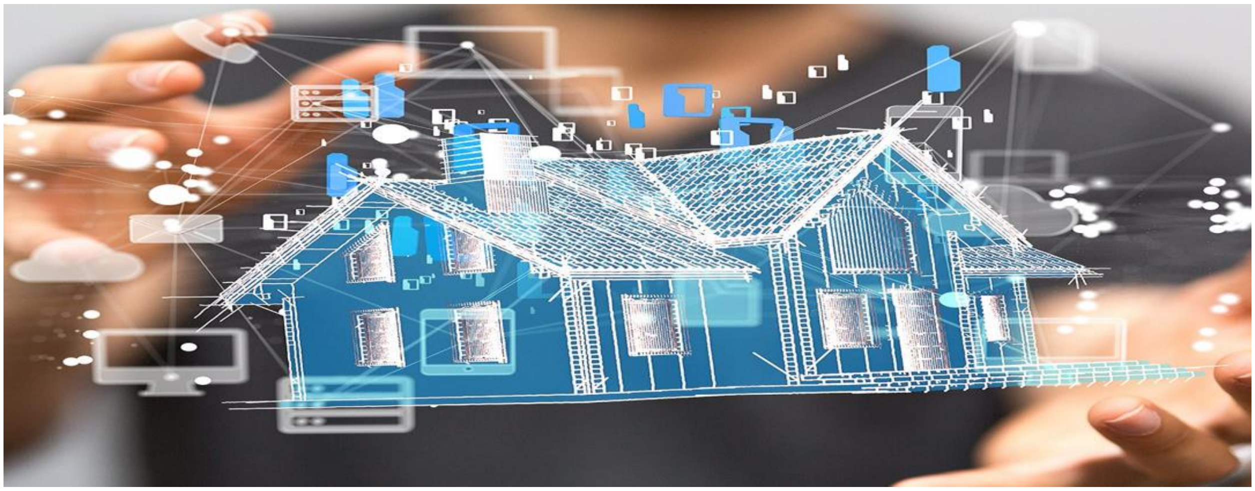


Figure 1: Picture of Home Security

WHY HOME NETWORK SECURITY MATTERS AND THE RISKS OF NOT SECURING YOUR NETWORK?

HOME NETWORK SECURITY THREATS:

Home network security threats refer to the various methods that cybercriminals use to access and steal personal information from your devices. Some of the common home network security threats include:

1. **Malware and viruses:** Malware refer to malicious software that cybercriminals use to gain access to your devices or network. Malware can take the form of viruses, worms, Trojan horses, or ransomware.
2. **Phishing attacks:** Phishing is a type of social engineering attack that aims to trick users into giving away their personal information, such as passwords or credit card details.
3. **Identity theft:** Identity theft involves stealing someone's personal information to access their financial accounts or open new ones in their name.
4. **Unauthorized access to personal information:** This refers to someone gaining access to your personal data without your consent.

IMPACT OF HOME SECURITY BREACHES:

Home network security breaches can have severe consequences, including:

1. **Financial loss:** A cyber-attack can result in the loss of money from your bank accounts or unauthorized purchases on your credit card.
2. **Loss of privacy:** Cybercriminals can use your personal information to access your online accounts, monitor your online activities, and steal sensitive information.
3. **Legal consequences:** If a cyber-attack results in the theft of confidential data, you may be liable for legal action or face penalties.

Figure 2: Impact of Home Security Breaches

BASIC TERMINOLOGIES AND NETWORKING DEVICES:

UNDERSTANDING NETWORK DEVICES:

1. **Routers:** Routers are network devices that connect multiple devices to the internet and facilitate communication between them.
2. **Switches:** Switches are devices that connect devices within a network, allowing them to communicate with each other.
3. **Access points:** Access points are devices that provide wireless connectivity to devices within a network.

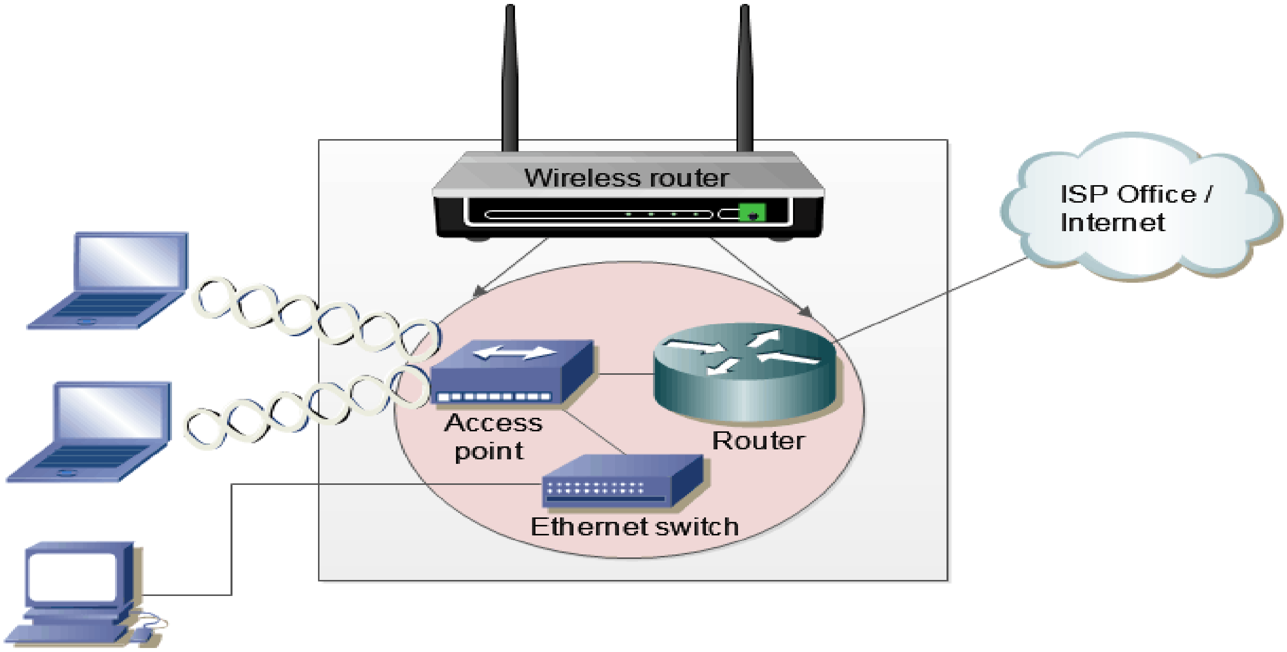


Figure 3: Networking Devices

UNDERSTANDING HOME NETWORK SECURITY:

1. **Encryption:** Encryption involves encoding data in a way that only authorized parties can access it.
2. **Firewalls:** Firewalls are software or hardware devices that monitor incoming and outgoing network traffic to block unauthorized access.
3. **Virtual private networks (VPNs):** VPNs provide secure, encrypted connections to the internet by routing traffic through a private server.

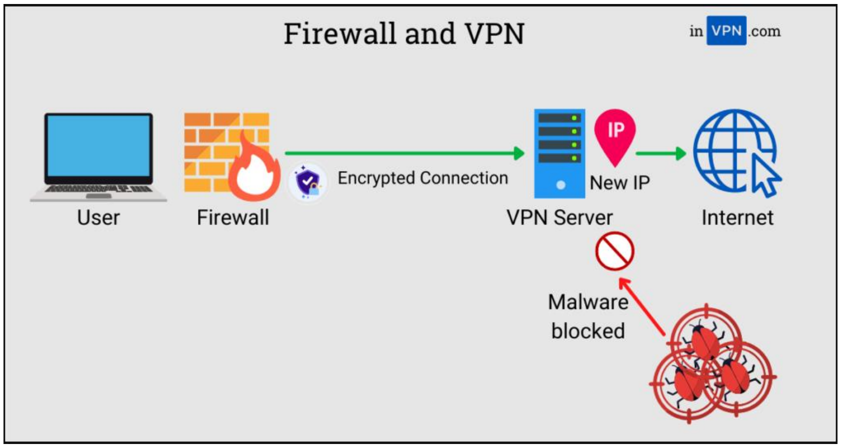


Figure 4: Use of Firewall and VPN

BEST PRACTICES FOR HOME NETWORK SECURITY:

Implementing the following best practices can help enhance home network security:

1. **Strong passwords:** Use strong, unique passwords and two-factor authentication to protect your accounts.
2. **Regular software updates:** Keep your devices and software up to date to patch any security vulnerabilities.
3. **Disable remote access:** Disable remote access to your devices unless necessary.
4. **Limit access to devices:** Restrict access to devices by using guest networks or by setting up access controls.
5. **Disable unused services:** Disable unused services, such as file-sharing or remote printing, to reduce the risk of unauthorized access.

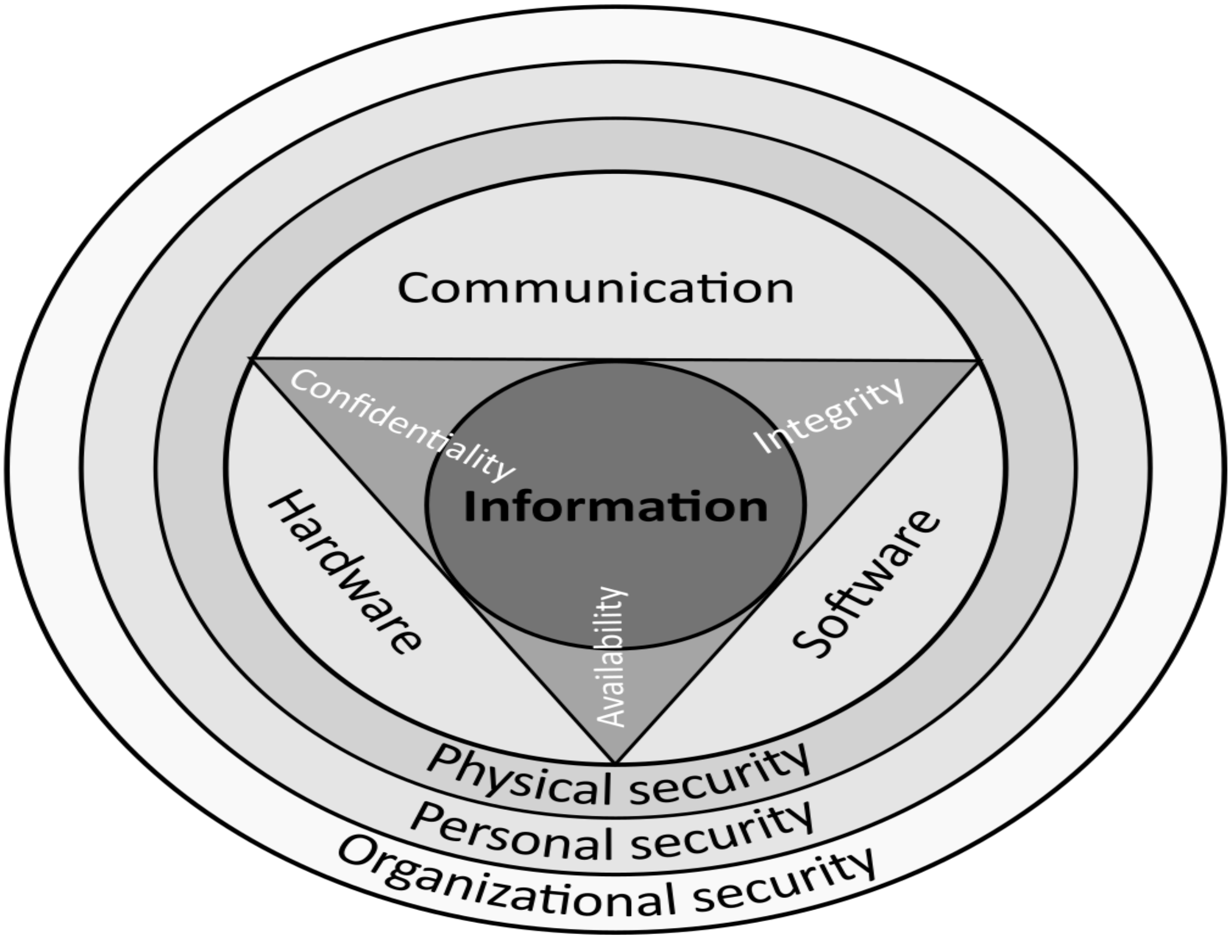


Figure 5:Best Practices to enhance home network security.

CONCLUSION:

RECAP OF HOME NETWORK SECURITY THREATS AND CONSEQUENCES:

Securing your home network is crucial in protecting your personal information from cyber-attacks. Understanding the various home network security threats and implementing best practices, such as using strong passwords and regular software updates, can help mitigate the risks of a security breach. By following these basic concepts and practices, you can ensure that your home network remains secure.

KEY TAKEAWAYS FOR HOME NETWORK SECURITY

1. Understand network devices and security protocols.
2. Follow best practices for home network security.
3. Regularly update software and change passwords.

DOMAIN 2: WIFI-SECURITY

WHAT IS WI-FI SECURITY AND WHY IT IS IMPORTANT?

In essence, Wi-Fi security refers to the steps taken to protect wireless networks from unauthorized access or malicious activities. This involves implementing measures such as setting up strong passwords and encryption protocols to prevent hackers from accessing personal information. Without proper Wi-Fi security, hackers can easily gain access to the network and potentially use it for illegal activities. This can lead to serious problems for the network owner. Therefore, it is crucial to prioritize Wi-Fi security to ensure the safety and protection of personal and sensitive information.

WI-FI ENCRYPTION:

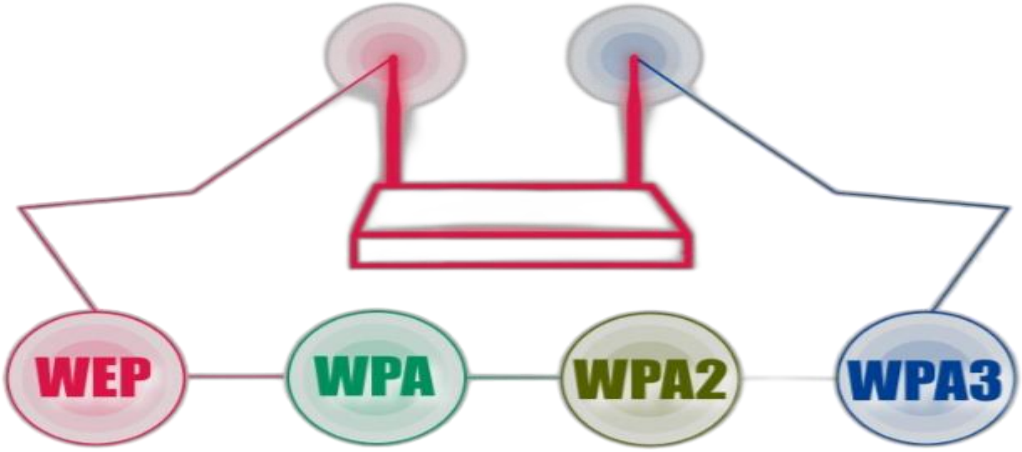


Figure 6:Wi-Fi Encryption Protocols

Wi-Fi security encryption is a technique used to protect wireless networks and data by encrypting the data transmitted over the network, which makes it unreadable to unauthorized users. The encryption process involves scrambling data, making it unreadable until it is decrypted with the proper encryption key. When a device connects to a Wi-Fi network, a handshake process occurs between the device and the router, which establishes an encryption method and generates a shared key for encrypting and decrypting data. The level of security provided by Wi-Fi encryption protocols depends on the encryption algorithm used.

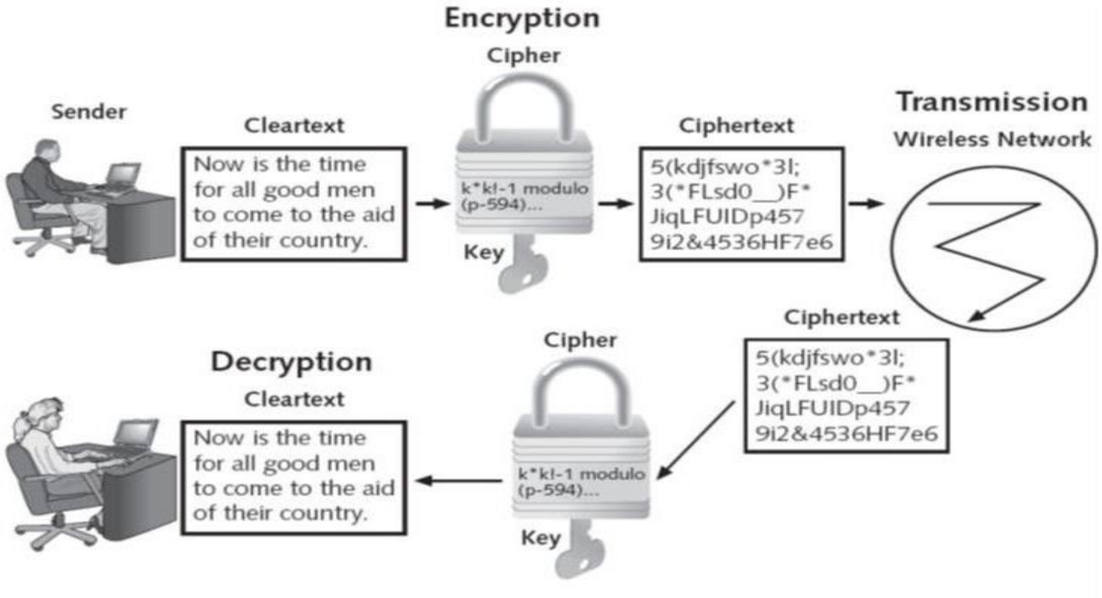
Mainly there are four different encryptions:

1. WEP
2. WPA
3. WPA2
4. WPA3

Among these, WEP is the least secure, while WPA2 and WPA3 are considered the strongest. WPA2 is currently the most used encryption method in wireless networks.

WEP

WHAT IS IT?



Encryption
Cipher
Sender
Cleartext
Now is the time for all good men to come to the aid of their country.
k*k!-1 modulo (p-594)...
Key
Ciphertext
5(kdjfswo*3l; 3(*FLsd0__)F* JiqLFUIDp457 9i2&4536HF7e6
Transmission
Wireless Network
Ciphertext
5(kdjfswo*3l; 3(*FLsd0__)F* JiqLFUIDp457 9i2&4536HF7e6
Decryption
Cleartext
Now is the time for all good men to come to the aid of their country.
Cipher
k*k!-1 modulo (p-594)...
Key

Figure 7: Working of WEP

- The oldest wireless security protocol is called WEP or Wired Equivalent Privacy.
- Wireless networks are generally less secure than wired networks because the signal is broadcasted through the air and can be intercepted if encryption technologies are not in place.
- WEP was created to provide the same level of privacy as a wired network by encrypting data transmitted over a wireless network using a shared secret key.
- The key is used to encrypt and decrypt data, ensuring that only authorized users with the key can access the network.

PROBLEMS:

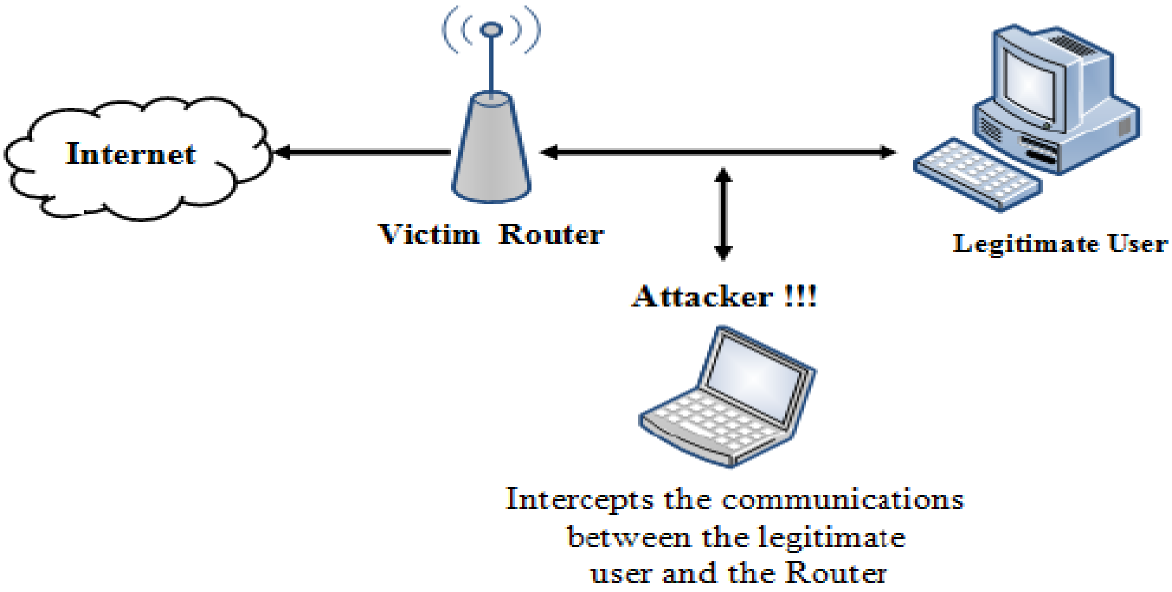

Internet
Victim Router
Legitimate User
Attacker !!!
Intercepts the communications between the legitimate user and the Router

Figure 8:Vulnerability of WEP

- WEP is an old and unreliable protocol for wireless networks because it uses a fixed encryption key that can be easily guessed by attackers.
- This makes WEP vulnerable to attacks, which can allow hackers to access confidential messages and modify data transmission.
- As a result, WEP is no longer recommended for use in wireless networks.
- In order to address this issue, a new protocol called WPA (Wi-Fi Protected Access) was developed to provide better security for wireless networks.

WPA

WHAT IS IT?

- WPA, or Wi-Fi Protected Access, is a security protocol that was created to replace the vulnerable WEP protocol.
- WPA uses an encryption method called Temporal Key Integrity Protocol (TKIP) to secure wireless networks.
- This method changes the encryption key dynamically, making it harder for unauthorized individuals to access the network.
- WPA also employs a process called the Four-Way Handshake, which establishes a secure connection between the Wi-Fi router and devices connecting to it.

PROBLEM:

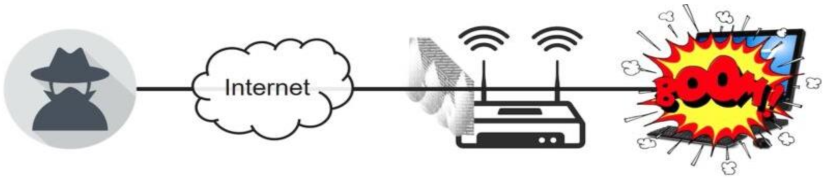


Figure 9:Brute Force Attack on WPA

- Currently, WPA is no longer considered as secure as other more robust protocols due to its vulnerabilities, including those found in TKIP.
- Additionally, WPA passwords are susceptible to brute force attacks, where attackers utilize automated tools to attempt a multitude of possible passwords until they locate the correct one.

WPA 2

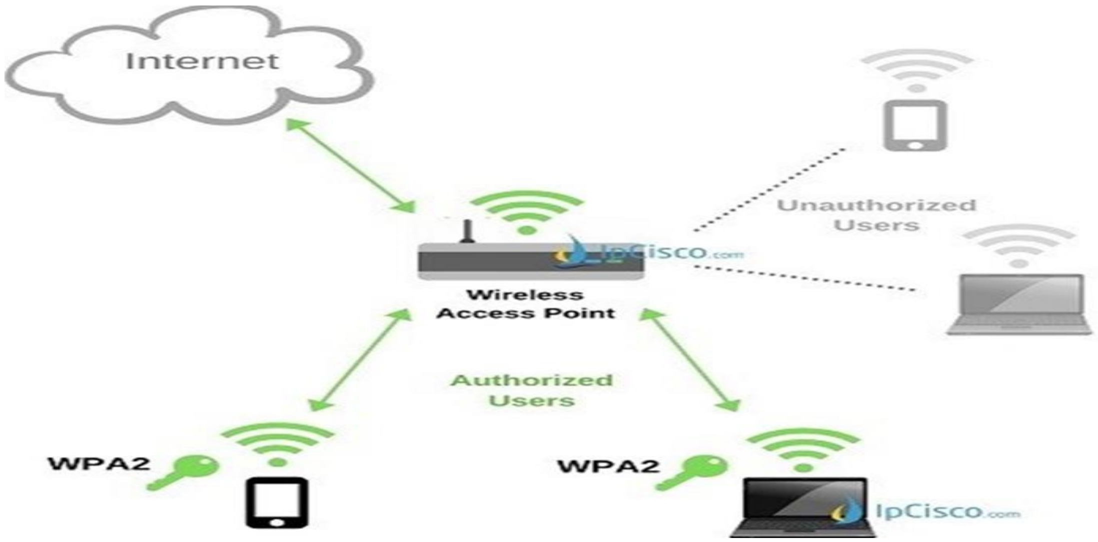


Figure 10:Working of WPA 2

WHAT IS IT?

1. The WPA2 is an easier-to-configure security protocol that offers a higher level of security compared to previous alternatives.
2. It differs from its predecessors in that it uses the Advanced Encryption Standard (AES) instead of TKIP, which is highly secure and is used by the US government to protect classified information.
3. Therefore, WPA2 is the most commonly used Wi-Fi security protocol. It encrypts data transmitted over the network, making it accessible only to authorized users who have the network password.
4. Mainly there are two types of WPA 2

    1. WPA2 Personal: Also known as WPA2-PSK (Pre-Shared Key), it is the basic level of security used by most home wireless networks. In WPA2-Personal, a passphrase is used as the pre-shared key for all users to connect to the network.

    2. WPA2 Enterprise: Also known as WPA2-RADIUS, it is a higher level of security used in enterprise-level wireless networks. In WPA2-Enterprise, each user has a unique login and password, and authentication is performed using a RADIUS server.

PROBLEMS:

- Although WPA2 is typically regarded as secure, it is not entirely fool-proof, and there are some weaknesses that malicious actors can exploit.
- For example, the KRACK (Key-reinstallation attack) vulnerability, which was identified in 2017, enabled hackers to intercept and decode Wi-Fi communications.
- For this reason, a new Wi-Fi security protocol, called WPA3, was created as an updated and more secure alternative to WPA2.

WPA 3

WHAT IS IT?

- WPA3 is a recently developed security protocol for wireless networks that supersedes WPA2.
- Its purpose is to fix security vulnerabilities and weaknesses that were found in WPA2, resulting in enhanced security and privacy protection for Wi-Fi users.
- WPA3 provides stronger security features such as Simultaneous Authentication of Equals (SAE) and more powerful encryption protocols that prevent attacks like password guessing and offline dictionary attacks.
- Furthermore, WPA3 offers better security for open/public Wi-Fi networks and makes the process of connecting IoT devices to Wi-Fi networks simpler.
- It is considered a more secure and reliable security protocol for wireless networks and is gradually being adopted by device manufacturers and Wi-Fi network operators.

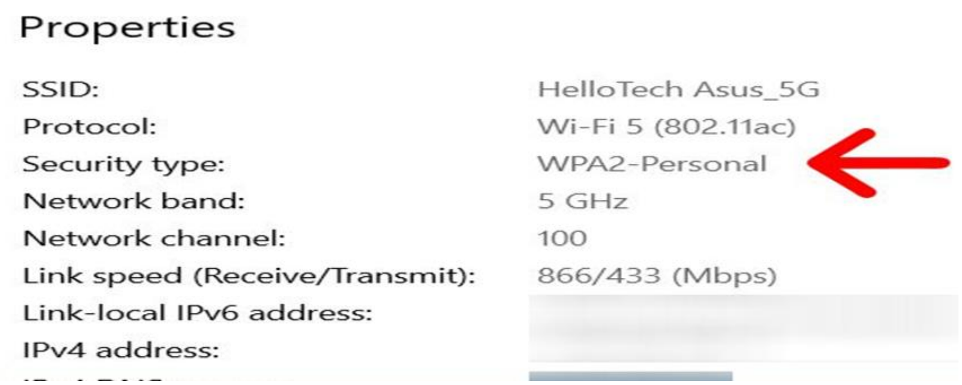
Figure 11:Wi-Fi Encryption Protocols

IDENTIFY WI-FI SECURITY TYPE IN A ROUTER:

Here are the steps to determine the security types according to your operating system. These steps are applicable for Windows, macOS, Android, and iOS. It's worth noting that you can identify the security type in most of the operating systems listed except for iOS.

WINDOWS 10:

- Find the Wi-Fi connection icon in the taskbar and click on it.
- Then click Properties underneath your current Wi-Fi connection.
- Scroll down and look for the Wi-Fi details under Properties.
- Under that, look for Security Type, which shows your Wi-Fi protocol.

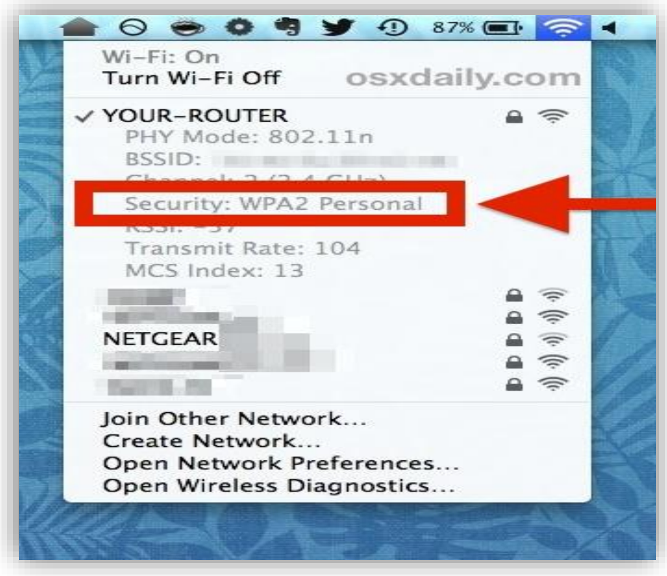


Properties

SSID:	HelloTech Asus_5G
Protocol:	Wi-Fi 5 (802.11ac)
Security type:	WPA2-Personal
Network band:	5 GHz
Network channel:	100
Link speed (Receive/Transmit):	866/433 (Mbps)
Link-local IPv6 address:	
IPv4 address:	

Figure 12:Security Type in Windows

MACOS:



PHY Mode: 802.11n
BSSID:
Security: WPA2 Personal
Transmit Rate: 104
MCS Index: 13

Figure 13: Security Type in macOS

- Hold down the Option key.
- Click on the Wi-Fi icon in the toolbar.

- This will show your network details,
    - including your Wi-Fi security type.

ANDROID:

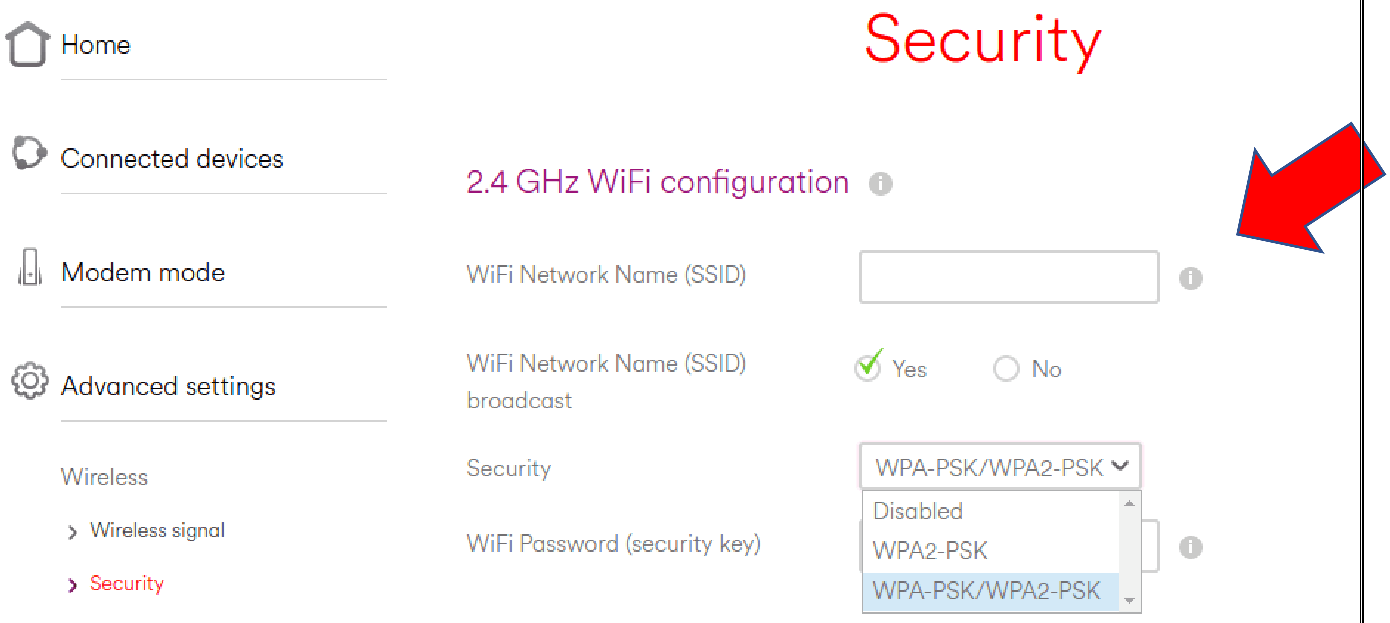
- On your Android phone, go into Settings.
- Open the Wi-Fi category.
- Select the router you are connected to and view its details.
- This will show what Wi-Fi security type your connection is.
- The path to this screen may differ depending on your device.

IOS:

- Unfortunately, there is no way within iOS to check your Wi-Fi security.

HOW TO CHANGE SECURITY TYPE ON ROUTER:

These steps are not universally applicable since various Wi-Fi router brands have their own distinct web interfaces. Therefore, the initial step involves opening a web browser and entering the router's specific IP address. Once you reach the login page, you must input your username and password. Following that, you can access advanced security settings and then different types of security protocols.



Security

2.4 GHz WiFi configuration

WiFi Network Name (SSID)

WiFi Network Name (SSID) broadcast ✓ Yes ○ No

Security WPA-PSK/WPA2-PSK

Disabled
WPA2-PSK
WPA-PSK/WPA2-PSK

WiFi Password (security key)

Figure 14:Security Type Configuration

WAYS TO CONNECT TO WI-FI ROUTER:

Mainly there are three ways you can connect to a router.

1. Using Ethernet cable
2. Password
3. WPS

USING ETHERNET CABLE:

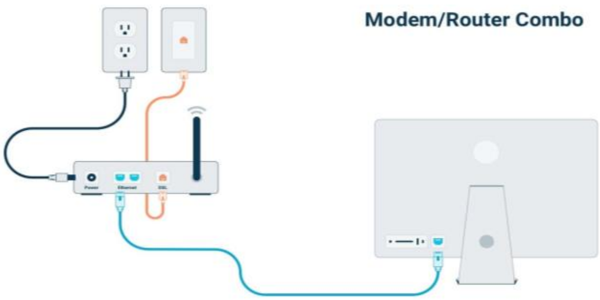
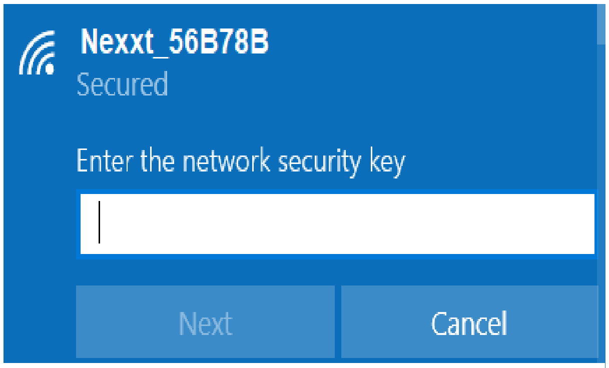


Figure 15: Ethernet

To access the internet through an ethernet cable, you need to connect one end of the cable to your device and the other end to a Wi-Fi router. However, simply plugging in the cable will not provide internet access. You need to log in to the router's interface and enable a feature called "wireless bridging" or "wireless repeater". This allows the router to receive the Wi-Fi signal and transmit it through the ethernet cable to your device, essentially converting the Wi-Fi signal into an ethernet connection.

After enabling this feature, it may take a minute or two for the connection to be established. Once the connection is established, you should see the ethernet icon appear on your laptop or computer instead of the Wi-Fi icon. It is important to note that not all routers support wireless bridging or wireless repeater modes, so it is recommended to consult your router's manual to determine if this feature is available.

USING PASSWORD:



Nexxt_56B78B
Secured

Enter the network security key

Figure 16:Password

One commonly used method for accessing a router is to use a password. When connecting to a Wi-Fi network, you will be presented with a list of available networks to choose from. Once you have chosen the network you wish to connect to, you will need to enter a password to gain access to it.

This means that to connect to a router using this method, you need to know the password for the network you want to connect to. The password is usually set by the router's owner or administrator and is intended to prevent unauthorized access to the network. It is important to keep your Wi-Fi network password secure to prevent others from accessing your network without your permission.

WPS:

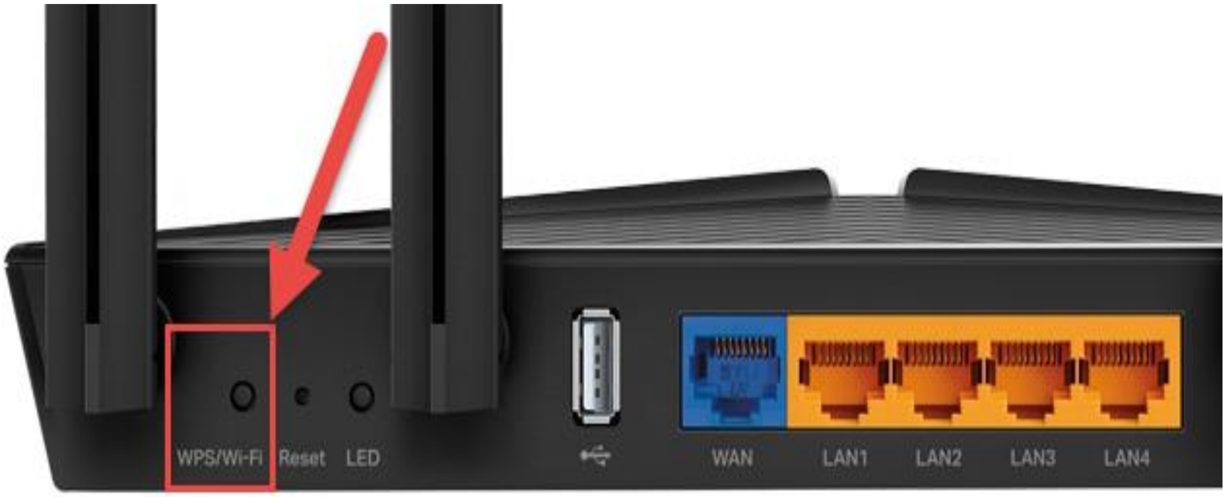


Figure 17:WPS Configuration

The last feature found on modern Wi-Fi routers is WPS, which stands for Wi-Fi Protected Setup. Its purpose is to simplify the process of connecting your devices to a Wi-Fi network without the need to type in a password. It works by either pressing a physical button on the router or entering a unique PIN code into the device that needs to connect to the Wi-Fi network. Once the device is authenticated, it is granted access to the network without having to enter the network's password.

Although WPS was designed to make connecting to Wi-Fi networks easier, it can pose a security risk if not used correctly. The WPS PIN can be vulnerable to brute-force attacks, where an attacker repeatedly guesses the PIN until they find the correct one and gain access to the network.

To keep your Wi-Fi network secure, it is recommended that you disable WPS on your router unless you have a specific need for it. Instead, use a strong password for your Wi-Fi network and make sure to keep it secure.

IMPORTANCE OF STRONG PASSWORD:

In the current era of digitalization, passwords are the first line of defence to secure our online accounts, whether it's social media, banking, or email. A strong password plays a crucial role in preventing unauthorized access and safeguarding sensitive information. To ensure a password's strength, it is recommended to use a combination of uppercase and lowercase letters, numbers, and symbols, with a minimum of eight characters. Common words, phrases, and personal information should be avoided to increase the password's security.

Using the same password for multiple accounts is a risky practice as it can lead to a chain reaction of security breaches. It is important to use different passwords for each account and regularly update them to ensure maximum security. Additionally, using a password manager is a great way to enhance password security, as it can generate and store complex passwords and provide autofill and auto-login features, eliminating the need to remember multiple passwords. However, it is important to remember not to write down passwords on paper or other easily accessible mediums as it defeats the purpose of having a strong password.

OK, let's see, sir, your FACEBOOK PASSWORD is... yep, all zeros, just like all the others

Figure 18:Importance of Password

These is the list of commonly used password. Among these, the word “password” for the password is much more popular.

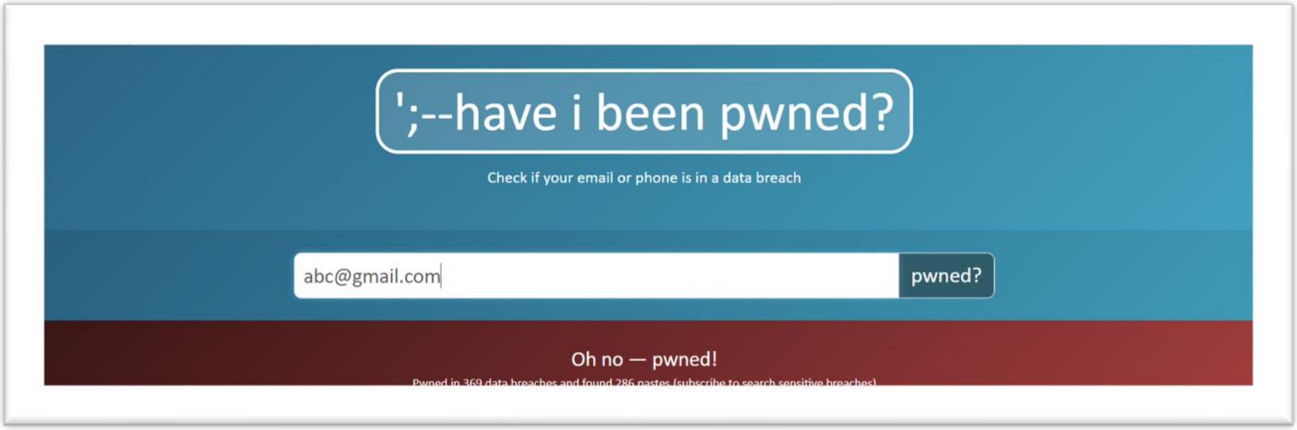
Top 30 Common Passwords		
123456	abc123	princess
password	1234	letmein
123456789	password1	654321
12345	iloveyou	monkey
qwerty	0000000	1qaz2wsx
1234567	qwerty123	123321
111111	zaq12wsx	qwertyuiop
1234567890	dragon	superman
123123	sunshine	asdfghjkl

There are several free online tools available to assess the strength of your password. These tools enable you to input any password and assess its strength, including the time it would take for an attacker or hacker to break it. By increasing the length of your password and using special characters and numbers, you can significantly increase the estimated time it would take to crack it.

Password strength checker tools

- Bit warden
- Password Monster
- Security.org

Have I Been Pwned? is a well-known website that enables users to determine if their personal data, including email addresses and passwords, has been compromised in data breaches. Users provide their email addresses to the website, which then searches its database of known breaches to see if any data associated with that email address has been compromised. If there is a match, the website notifies the user of the breached website or service and the type of information that was compromised.



Check if your email or phone is in a data breach

abc@gmail.com

Oh no — pwned!

Pwned in 369 data breaches and found 286 pastes (subscribe to search sensitive breaches)

Figure 19: Website Have I been pwned

RISKS OF USING OPEN WI-FI NETWORKS:

An open Wi-Fi network in public places does not require a password for access, which may seem convenient, but it poses cybersecurity risks. Hackers can intercept data transmitted over the network, including personal and financial information. Hackers can also create fake Wi-Fi networks to trick users into connecting, allowing them to steal data or install malware. Even if the network is secure, other users on the same network can potentially access and steal data from vulnerable devices.

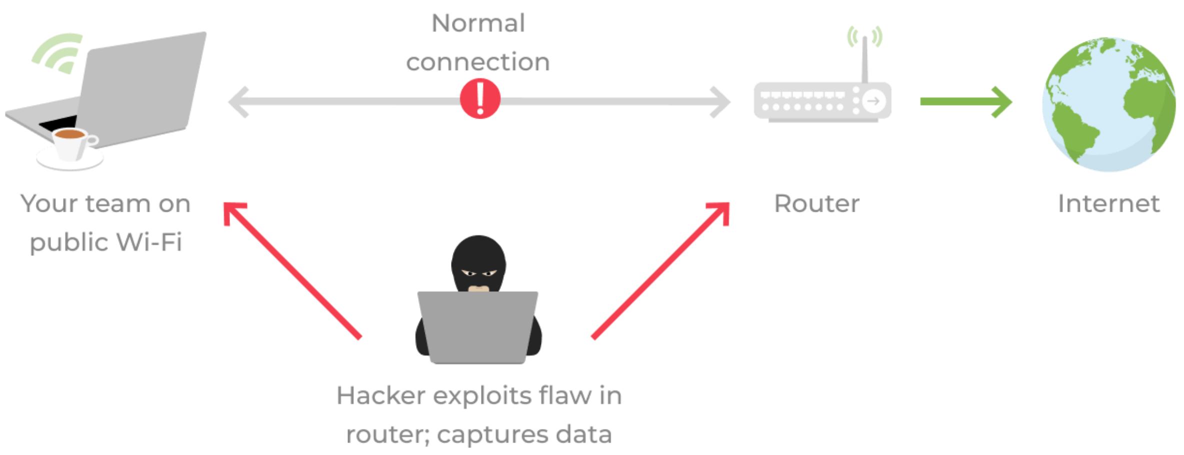

Normal connection
Your team on public Wi-Fi
Router
Internet
Hacker exploits flaw in router; captures data

Figure 20:Risks of Using Open Wi-Fi

PRECAUTIONS:

To reduce the risks of using public Wi-Fi networks, it is advisable to take the following precautions: avoid performing sensitive activities such as logging into your banking or email accounts, unless you use your secure mobile network or a secure Wi-Fi connection; keep your device's software and antivirus up to date; disable file sharing and network discovery to prevent unauthorized access to your device's files; and use a Virtual Private Network (VPN) to encrypt your online activity, which will make it more difficult for others to steal your data.

DOMAIN 3: SECURING YOUR DEVICES

We will first discuss why devices should be secured and why your devices should be up to date with the latest antivirus/device software updates.

Next, we will discuss the basic device security settings to a device, changes you're able to implement TODAY to protect you from tomorrow.

Lastly, we will demonstrate a practical demonstration of how we are able to securely download an antivirus program on Laptop.

WHY SHOULD YOU KEEP YOUR DEVICES SECURED?

Figure 21:Device Security

Devices should be secured to prevent attacks from intruders and provide peace of mind with your data. As the world is expanding and technology is growing, we are seeing a dramatic increase in the need for cybersecurity as attacks onto major corporations are becoming more prevalent.

WHAT ARE THE RISKS OF UNSECURED DEVICES?

- The risks of having an unsecured device are becoming a growing concern, data theft, identity theft, blackmailing is just some of the examples of risks for an unsecured device.
- The Dark Web and Black hat hackers will use data leaks from major companies to obtain Credit/Debit card information, and password leaks.
- Hackers can obtain user information and approach the user suggesting that if they do not pay the ransom their personal information or falsified information will be released to friends and family.

- In 2021, 20% of Americans fell victim to identity theft, as identity theft and stolen credit cards rose in popularity (Such as those TikTok videos and rap music videos showcasing Credit Card fraud), the demand for stolen credit card leaks rise.

BASIC SECURITY SETTINGS FOR YOUR DEVICES:

Acknowledging the threat of attackers and taking preventive measures is the first step in protecting yourself from a potential attack. Unfortunately, anybody can be hacked no matter what we do, but our goal is to be as difficult to hack as possible, by doing this a hacker will simply move onto somebody who is much more vulnerable.

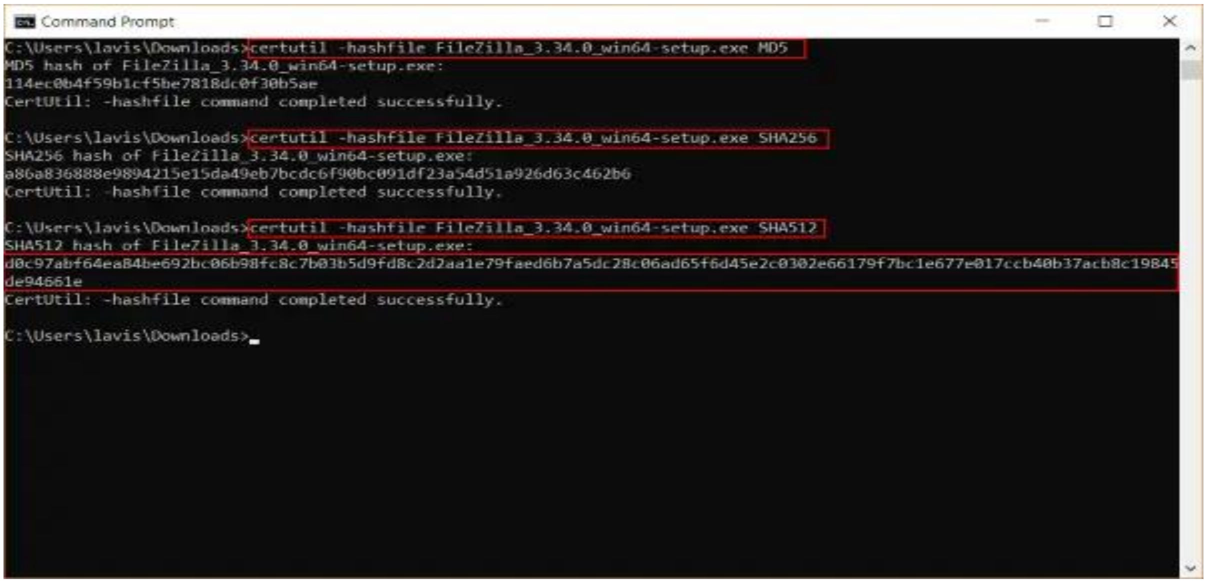
STEPS IN WHICH YOU CAN HELP PROTECT YOUR DEVICE: 2 FACTOR AUTHENTICATION

Figure 22:Multi-Factor Authentication

PASSWORD MANAGERS:

- KeePass
- BitWarden
- LastPass
- 1Password

FILE HASH:



```
C:\Users\lavis\Downloads>certutil -hashfile FileZilla_3.34.0_win64-setup.exe MD5
MD5 hash of FileZilla_3.34.0_win64-setup.exe:
114ec0b4f59b1cf5be7818dc0f30b5ae
CertUtil: -hashfile command completed successfully.

C:\Users\lavis\Downloads>certutil -hashfile FileZilla_3.34.0_win64-setup.exe SHA256
SHA256 hash of FileZilla_3.34.0_win64-setup.exe:
a86a836888e9894215e15da49eb7bcdc6f90bc091df23a54d51a926d63c462b6
CertUtil: -hashfile command completed successfully.

C:\Users\lavis\Downloads>certutil -hashfile FileZilla_3.34.0_win64-setup.exe SHA512
SHA512 hash of FileZilla_3.34.0_win64-setup.exe:
d0c97abf64ea84be692bc06b98fc8c7b03b5d9fd8c2d2aa1e79faed6b7a5dc28c06ad65f6d45e2c0302e66179f7bc1e677e017ccb40b37acb8c19845
de94661e
CertUtil: -hashfile command completed successfully.

C:\Users\lavis\Downloads>
```

Figure 23:File Hash Using Cmd

- Go to the search bar in Windows and enter ‘cmd’ this should bring up the command prompt type “Certutil -hash file Desktop\example.txt sha256”

HOW TO SECURELY BROWSE THE WEB:

PUBLIC NETWORK:

VPNs that I would use:

- Proton VPN
- Nord VPN
- Mullvad

BROWSER EXTENSIONS:

One of the most dangerous threats that are not taken seriously are extensions. These can start out legitimate, then through an update can turn malicious. These will then be removed from the webstore, but not your browser unless uninstalled.

LAPTOP/DESKTOP SECURITY:

SOFTWARE UPDATES:

Ensure you are keeping up to date with both applications and your OS, these patches will increase stability, but more importantly they will fix vulnerabilities that criminals have exploited

ADDING A FOREIGN KEYBOARD:

This is not a prevention measure, but nonetheless it’s interesting to discuss how some virus payloads will have “exceptions” that can sometime include the countries the virus was initially produced-

Dark Side for example, like a great many other malware strains, has a hard-coded do-not-install list of countries which are the principal members of the Commonwealth of Independent States (CIS)—former Soviet satellites that mostly have favourable relations with the Kremlin.

ANTIVIRUS UPDATES:

Keeping your antivirus up to date is as essential as keeping your software up to date “*More than 6000 new computer malware-viruses are created and released every month.*”, although most antivirus programs will automatically update or prompt you for an update it’s absolutely necessary to keep up to date with your antivirus as it will protect you from the most recent threats.

IOT SECURITY:

Like our smartphones and laptops, these IoT devices will be vulnerable to exploits and attacks from hackers. The biggest reason why IoT security is so important is because an IoT device can be used to gain unauthorized access into your systems. The average person might not realize that an IoT device can be hacked, but it can. And every IoT device added to your network increases the potential attack surface.

Figure 24:Securing IOT Devices

SECOND NETWORK:

Firstly, consider having an isolated network setup on your private (home) network, this will isolate the devices to their own network. If you have an IoT device connected to another network an intruder will not be able to see your other end devices connected to a network.

HOW TO WORK WITH IOT DEVICES:

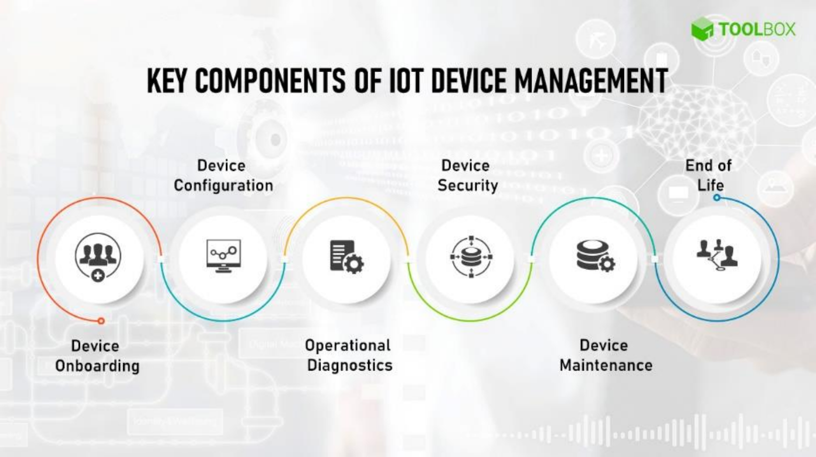


Figure 25:Components of IOT Device Management

- Pane of glass/Management tool
- Controlling access
- Use a Unique Password

ANTIVIRUS/ANTIMALWARE/ANTISPYWARE: THERE IS A DIFFERENCE!

Figure 26:Anti-Virus

COMPTIA MALWARE REMOVAL STEPS:

Figure 27: Comptia

- **Verify Symptoms** - Conduct research and verify that there is malware
- **Quarantine Infected** - Disconnect your device from the network (and remove all removable media)
- **Disable System Restore** - Malware can infect restore points
- **Remediate/Update Antivirus** - Update your antivirus (to ensure latest antivirus signatures) (Copy updated antivirus from another computer but ensure nothing plugs into the device without malware first)
- **Remediate/Scan and Remove** - Perform a full scan (Boot into safe mode preferably)
- **Schedule scans and run updates** - Always check for latest updates
- **Enable System Protection** - Enable System protection, create automated restore points

DOMAIN 4: SOCIAL ENGINEERING

DEFINITION:

Social engineering is the art of exploiting human psychology, rather than technical hacking techniques, to gain access to buildings, systems, or data.

EXAMPLE:

For example, instead of trying to find a software vulnerability, a social engineer might call an employee and pose as an IT support person, trying to trick the employee into divulging his password.

PICTORIAL REPRESENTATION:

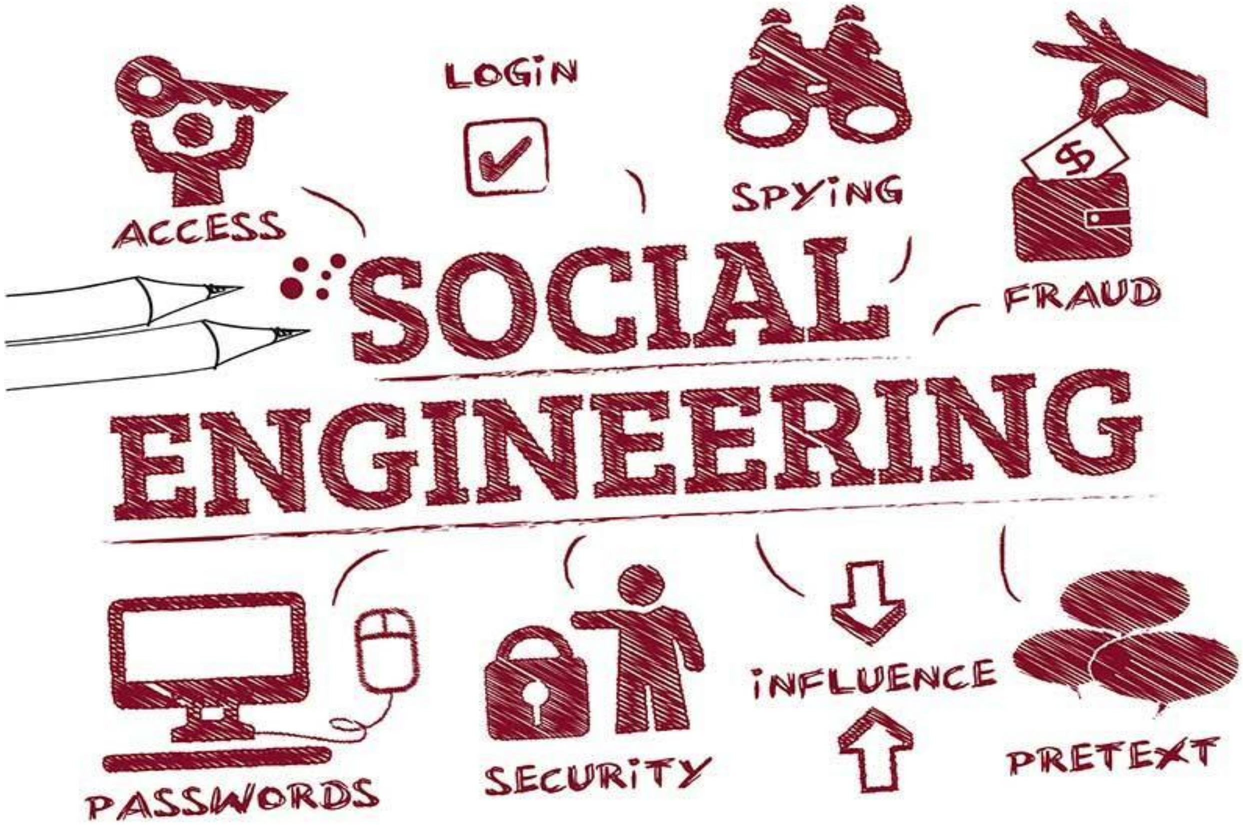


Figure 28: Types of Social Engineering

TYPES OF SOCIAL ENGINEERING ATTACK:

The following are the types of Social Engineering Attack:

- Phishing
- Tailgating
- Spam
- Dumpster Diving
- Identity Theft
- Invoice Scam

ATTACK 1: PHISHING

The fraudulent act of sending emails or other messages ostensibly from trustworthy firms to persuade people to provide personal information, including passwords and credit card numbers.

TYPES OF PHISHING:

Spear Phishing: Spear phishing is a more specialised attack tactic that seeks to steal information or install malware on the victim's device, whereas phishing is a more general attack strategy that targets several people.

Whaling: A whaling attack is a technique used by cybercriminals to impersonate a senior member of an organisation and target senior or other significant individuals directly with the intention of stealing money or sensitive information or gaining access to their computer systems for illegal activities.

Vishing: Vishing is a type of cybercrime where victims' phones are used to obtain their private information.

Smishing: Smishing, often known as SMS phishing, is a phishing cybersecurity attack carried out using mobile text messaging.

Pop-Up Phishing: Phishing that "pops up" for people as they browse the internet is known as pop-up phishing. Frequently, harmful code is added by cybercriminals to otherwise trustworthy websites, causing consumers to see these pop-up notifications when they visit them.

ATTACK 2: TAILGATING

When an unauthorized individual might follow you in through that open door without badging in themselves.

ATTACK 3: SPAM

Spam is any kind of unwanted, unsolicited digital communication that gets sent out in bulk. Often spam is sent via email, but it can also be distributed via text messages, phone calls, or social media.

ATTACK 4: DUMPSTER DIVING

This entails combing through someone else’s trash to find treasure -or in the tech world, discarded sensitive information that could be used in an illegal manner. It can be anything, including your:

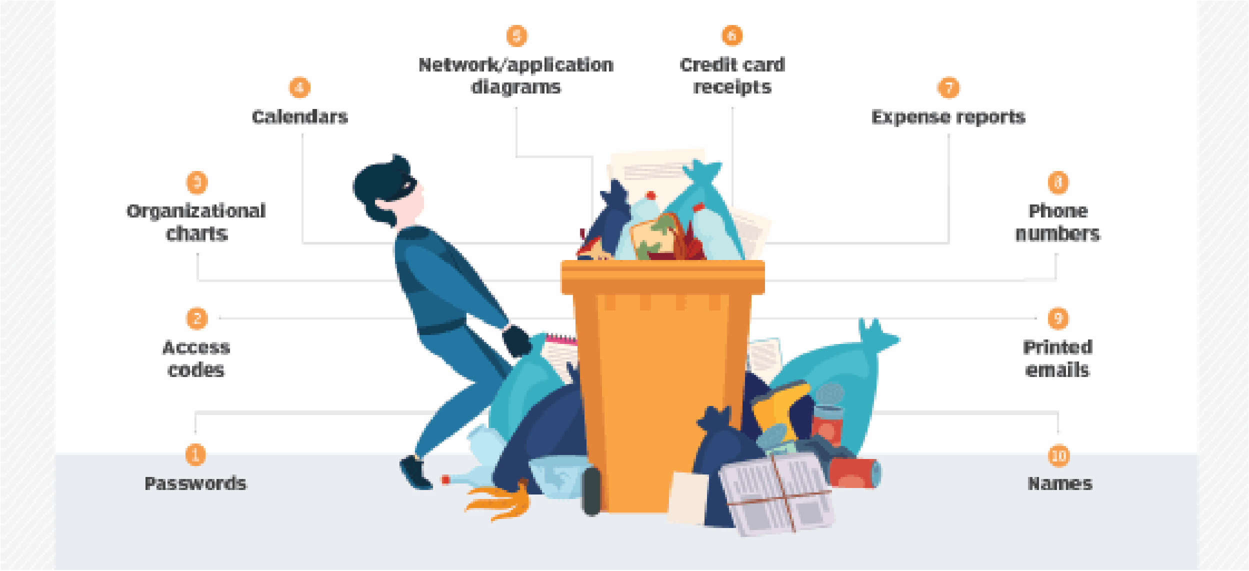


Figure 29:Dumpster Diving

ATTACK 5: IDENTITY THEFT

- Identity theft occurs when criminals steal a victim's personal information to commit criminal acts.
- Using this stolen information, a criminal takes over the victim's identity and conducts a range of fraudulent activities in their name.

ATTACK 6: MALWARE

- Anything that is purposely destructive to a computer, network, or server is known as malware, sometimes known as malicious software.

TYPES OF MALWARES:

RANSOMWARE:

- Ransomware is a type of malware from crypto virology that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid off.

Figure 30: Attacker demanding money after a ransomware attack

TROJAN HORSE:

- A Trojan Horse Virus is a form of malware that installs itself on a computer by impersonating a trustworthy application.

SPYWARE:

- Spyware is a program that gets installed without the user's permission.
- It monitors the user's activities on the internet and transmits the information to the third party.

WORM:

- Malicious program that makes copies of itself in the local network and network shares.
- They make the device slow.

ADWARE:

- Software where advertising banners are displayed while any program is running.
- It automatically downloads to your device while browsing any website.
- It is used by companies for marketing purposes.

Figure 31: Adware Attack

VIRUS:

- Software that replicates itself and spreads by damaging and deleting.
- Viruses enter in your system via attached images, greeting, audio/video, downloads etc.

PREVENTIVE MEASURES ARE:

- Conduct routine security awareness training.
- Fix and update
- Put security software and a firewall to use.
- Keep links and attachments closed.
- Activate Access Control.

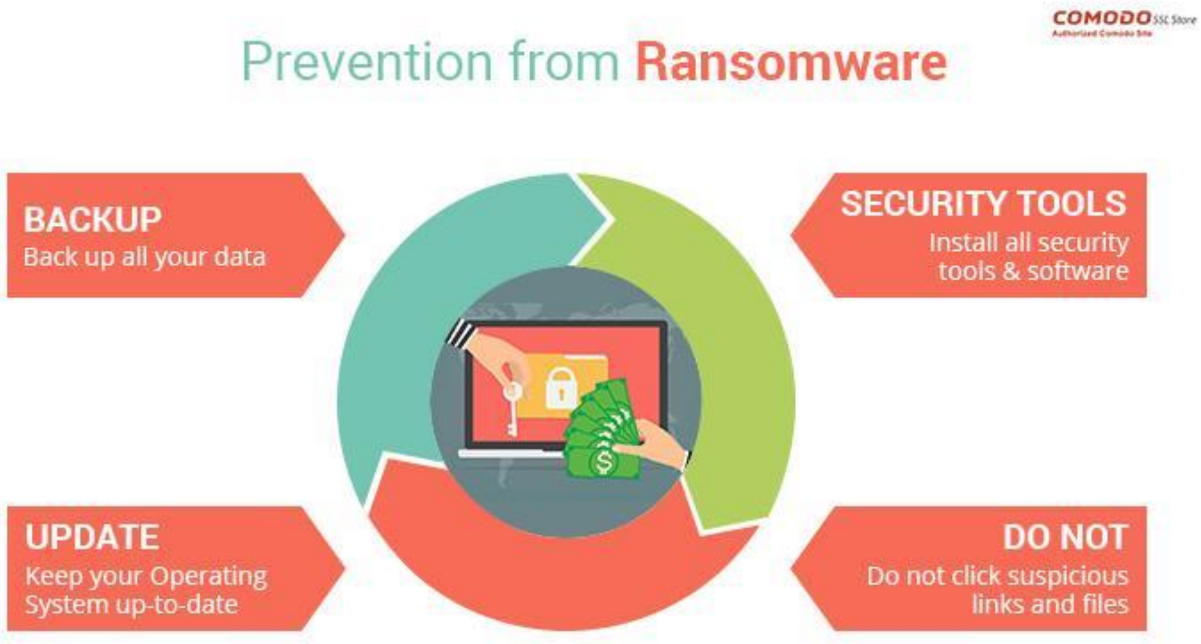

COMODO SSL Store
Authorized Comodo Site
Prevention from Ransomware
BACKUP
Back up all your data
SECURITY TOOLS
Install all security tools & software
UPDATE
Keep your Operating System up-to-date
DO NOT
Do not click suspicious links and files

Figure 32:Precautions in Ransomware Attack

- Impose multi-factor authentication requirements.
- Put the least privilege principle to use.
- Change passwords for shared resources.
- Keep an eye out for unusual or shady behaviour.
- Using a free Microsoft safety scanner.

DOMAIN 5: NETWORK MONITORING AND PARENTAL CONTROL

WHAT IS NETWORK?

A network consists of two or more devices that are linked to share resources. For instance, the image given below is showing the linked usage wires/cables or on wireless network.

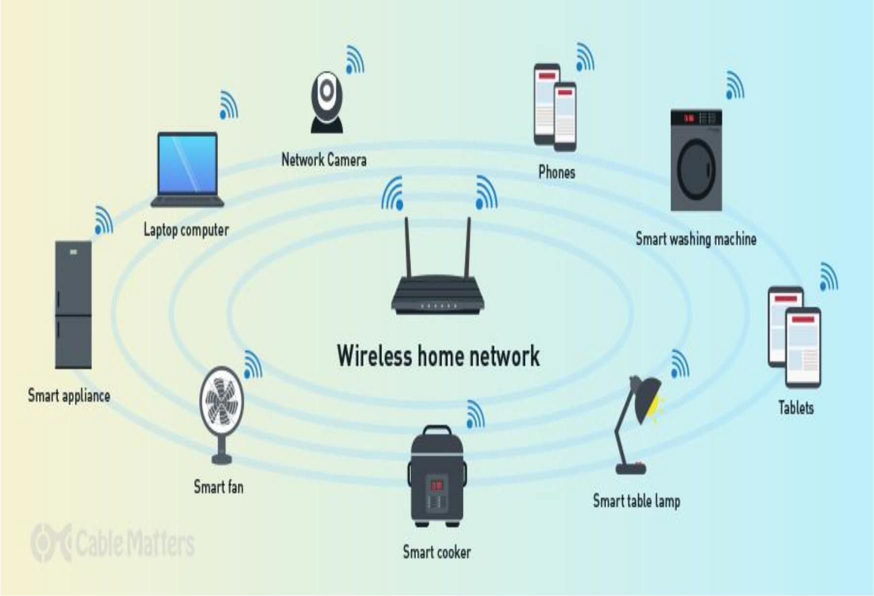


Figure 33:Wireless Home Network

WHAT IS NETWORK MONITORING?

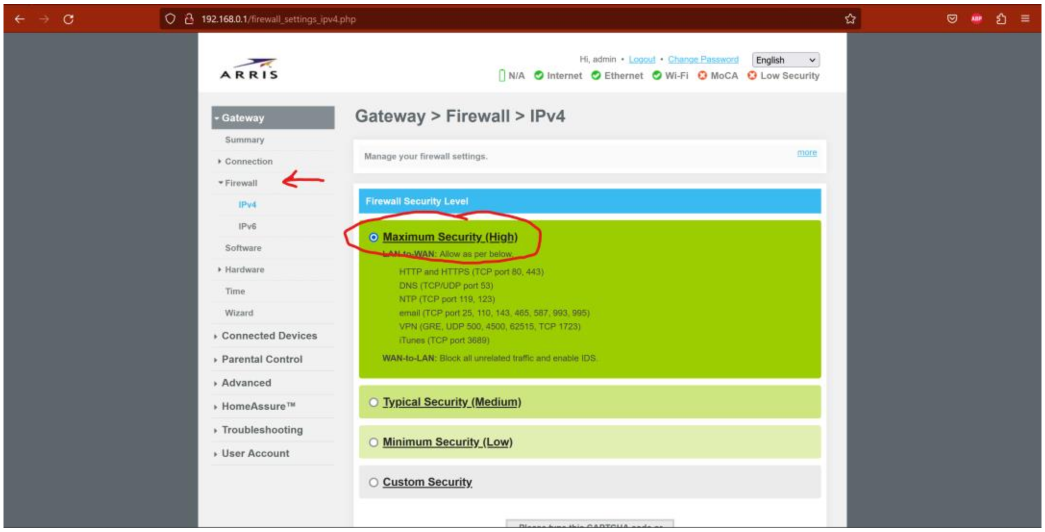
Figure 34:Network Monitoring

Network monitoring is the use of network monitoring software/ manual techniques to monitor the continuous health and reliability of a computer network.

This Includes watching over your network, for that we need to ask questions:

- What all devices are connected into your device.
- What is the function of each device in your network?
- How secure is the device in your network?
- Is your network infrastructure up to date?
- Are all the users browsing safe?
- Have you separated your network into private and guest bases?
- Is your firewall up?
- Is there any external connection into your network?
- Do you have network segmentation in your router?
- To answer all the above questions, we need to do the following setting in the router:

FIREWALL SETTINGS:



192.168.0.1/firewall_settings_ipv4.php

Gateway > Firewall > IPv4

Manage your firewall settings.

Firewall Security Level

● Maximum Security (High)

LAN-to-WAN: Allow as per below.

HTTP and HTTPS (TCP port 80, 443)
DNS (TCP/UDP port 53)
NTP (TCP port 119, 123)
email (TCP port 25, 110, 143, 465, 587, 993, 995)
VPN (GRE, UDP 500, 4500, 62515, TCP 1723)
iTunes (TCP port 3689)

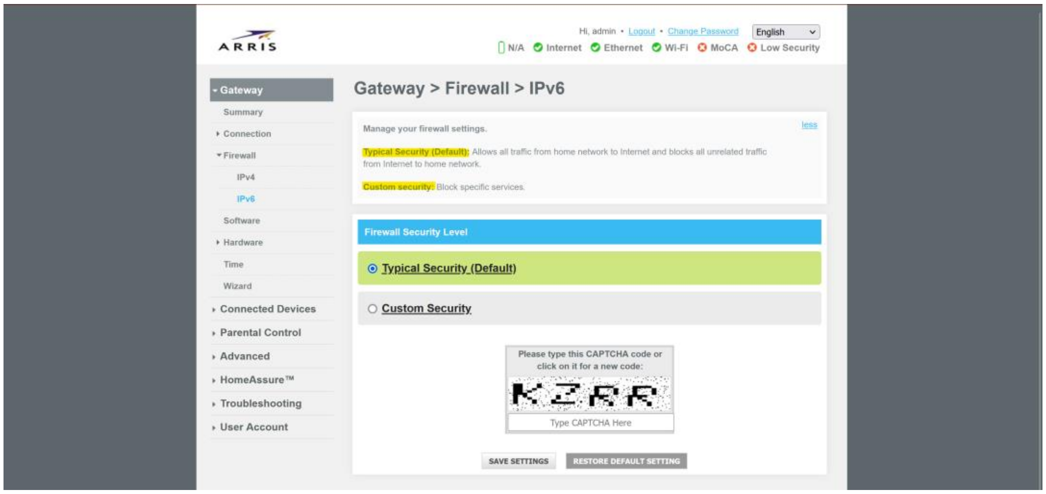
WAN-to-LAN: Block all unrelated traffic and enable IDS.

○ Typical Security (Medium)

○ Minimum Security (Low)

○ Custom Security

Figure 35:Firewall Configuration (IPv4)



Gateway > Firewall > IPv6

Manage your firewall settings.

Typical Security (Default): Allows all traffic from home network to Internet and blocks all unrelated traffic from Internet to home network.

Custom security: Block specific services.

Firewall Security Level

● Typical Security (Default)

○ Custom Security

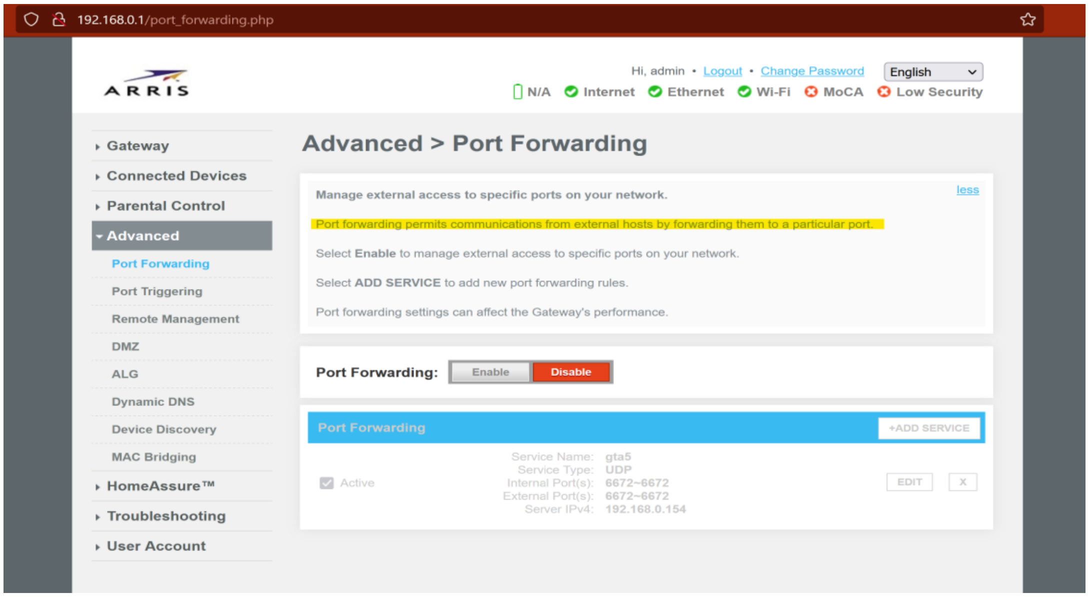
Please type this CAPTCHA code or click on it for a new code:

KZRR

Type CAPTCHA Here

Figure 36:Firewall Configuration (IPv6)

- **PORT FORWORDING:** This means your router will keep a port (i.e., network door) open for people to connect from outside of your house.



Advanced > Port Forwarding

Manage external access to specific ports on your network.

Port forwarding permits communications from external hosts by forwarding them to a particular port.

Select **Enable** to manage external access to specific ports on your network.

Select **ADD SERVICE** to add new port forwarding rules.

Port forwarding settings can affect the Gateway's performance.

Port Forwarding: Enable [✓ Disable]

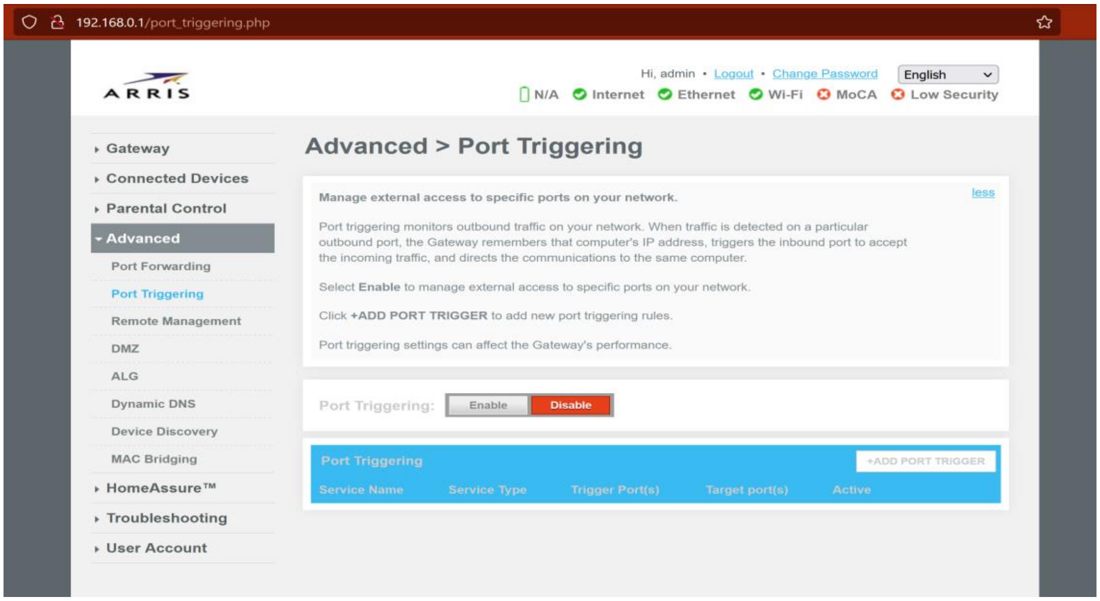
Port Forwarding

☑ Active

Service Name: gta5
Service Type: UDP
Internal Port(s): 6672~6672
External Port(s): 6672~6672
Server IPv4: 192.168.0.154

Figure 37:Port Forwarding Configuration

- **PORT TRIGGERING**: this feature monitors the outgoing traffic in your network. When the traffic is detected on a particular outbound port (i.e., is a network door which is used for exiting the network), your network will remember that computer's IP address which is trying to connect to the outside network and will return the incoming traffic to the same computer and block everything else.



Manage external access to specific ports on your network.

Port triggering monitors outbound traffic on your network. When traffic is detected on a particular outbound port, the Gateway remembers that computer's IP address, triggers the inbound port to accept the incoming traffic, and directs the communications to the same computer.

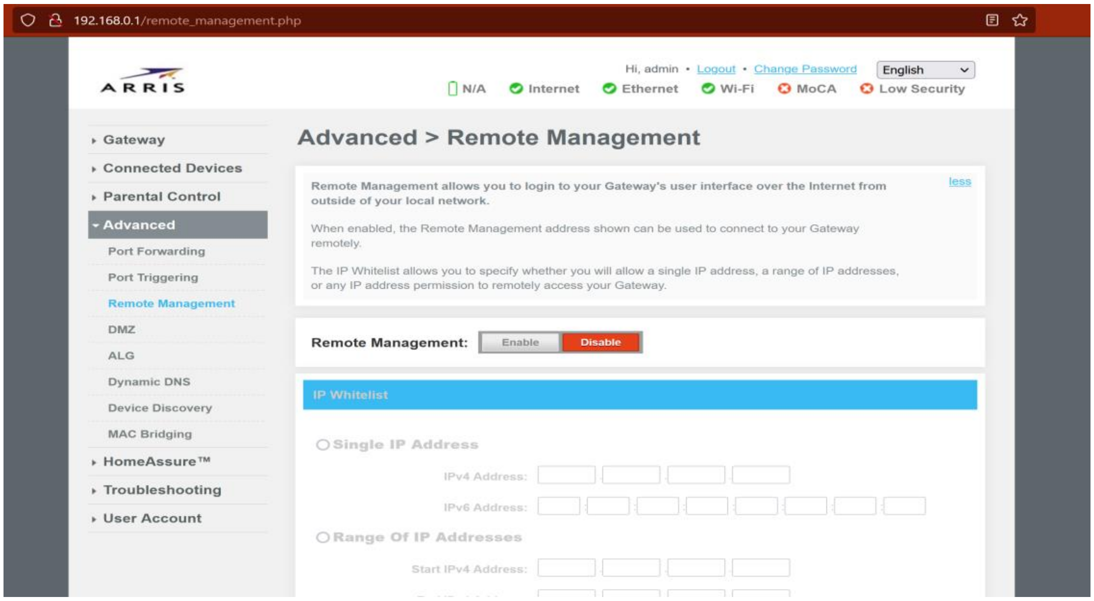
Select **Enable** to manage external access to specific ports on your network.

Click **+ADD PORT TRIGGER** to add new port triggering rules.

Port triggering settings can affect the Gateway's performance.

Figure 38:Port Triggering Configuration

- **Remote Management:** This feature allows you to connect to your router or router settings over the internet from anywhere on the earth. So, this is a very dangerous if your credentials fall into wrong hands.



192.168.0.1/remote_management.php

ARRIS

Hi, admin • Logout • Change Password English

N/A ✓ Internet ✓ Ethernet ✓ Wi-Fi ☒ MoCA ☒ Low Security

- Gateway
- Connected Devices
- Parental Control
- Advanced
  - Port Forwarding
  - Port Triggering
  - Remote Management
  - DMZ
  - ALG
  - Dynamic DNS
  - Device Discovery
  - MAC Bridging
- HomeAssure™
- Troubleshooting
- User Account

Advanced > Remote Management

Remote Management allows you to login to your Gateway's user interface over the Internet from outside of your local network. less

When enabled, the Remote Management address shown can be used to connect to your Gateway remotely.

The IP Whitelist allows you to specify whether you will allow a single IP address, a range of IP addresses, or any IP address permission to remotely access your Gateway.

Remote Management: Enable [✓ Disable]

IP Whitelist

○ Single IP Address

IPv4 Address:

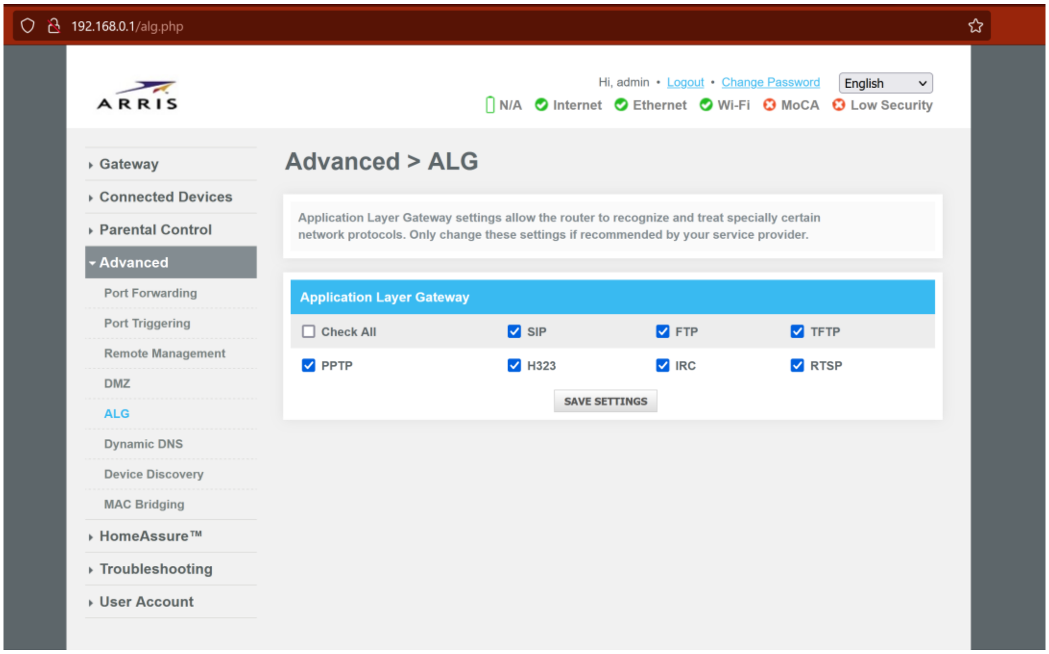
IPv6 Address:

○ Range Of IP Addresses

Start IPv4 Address:

Figure 39: Remote Management Configuration

- **Application Layer Gateway:** is a type of security software or device setting that acts on behalf of the application servers on a network, protecting the servers and the application from traffic that might be malicious.



192.168.0.1/alg.php

ARRIS

Hi, admin • Logout • Change Password English

N/A ✓ Internet ✓ Ethernet ✓ Wi-Fi ☒ MoCA ☒ Low Security

- Gateway
- Connected Devices
- Parental Control
- Advanced
  - Port Forwarding
  - Port Triggering
  - Remote Management
  - DMZ
  - ALG
  - Dynamic DNS
  - Device Discovery
  - MAC Bridging
- HomeAssure™
- Troubleshooting
- User Account

Advanced > ALG

Application Layer Gateway settings allow the router to recognize and treat specially certain network protocols. Only change these settings if recommended by your service provider.

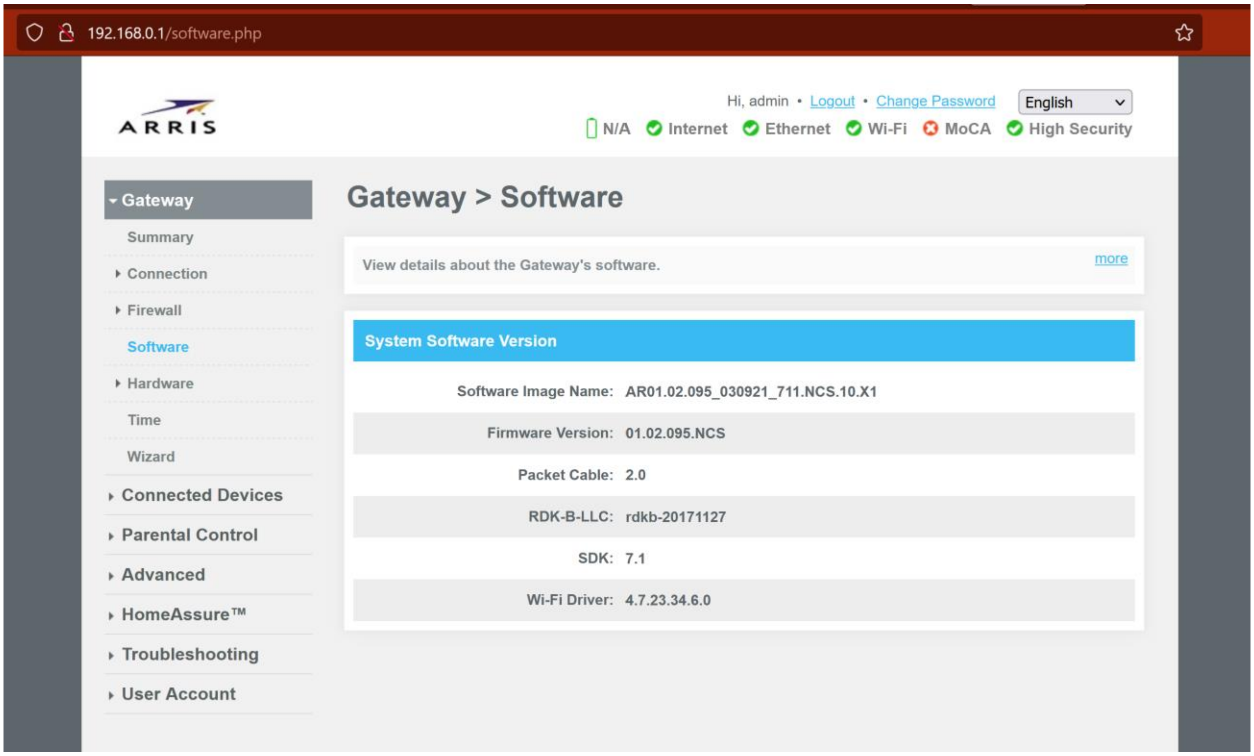
Application Layer Gateway

☐ Check All	☑ SIP	☑ FTP	☑ TFTP
☑ PPTP	☑ H323	☑ IRC	☑ RTSP

SAVE SETTINGS

Figure 40: Application Layer Gateway Configuration

- **Software/firmware Update:** Very important to keep your devices up to date, it has patches to all the vulnerabilities found till date.



Gateway > Software

View details about the Gateway's software.

System Software Version

Software Image Name: AR01.02.095_030921_711.NCS.10.X1

Firmware Version: 01.02.095.NCS

Packet Cable: 2.0

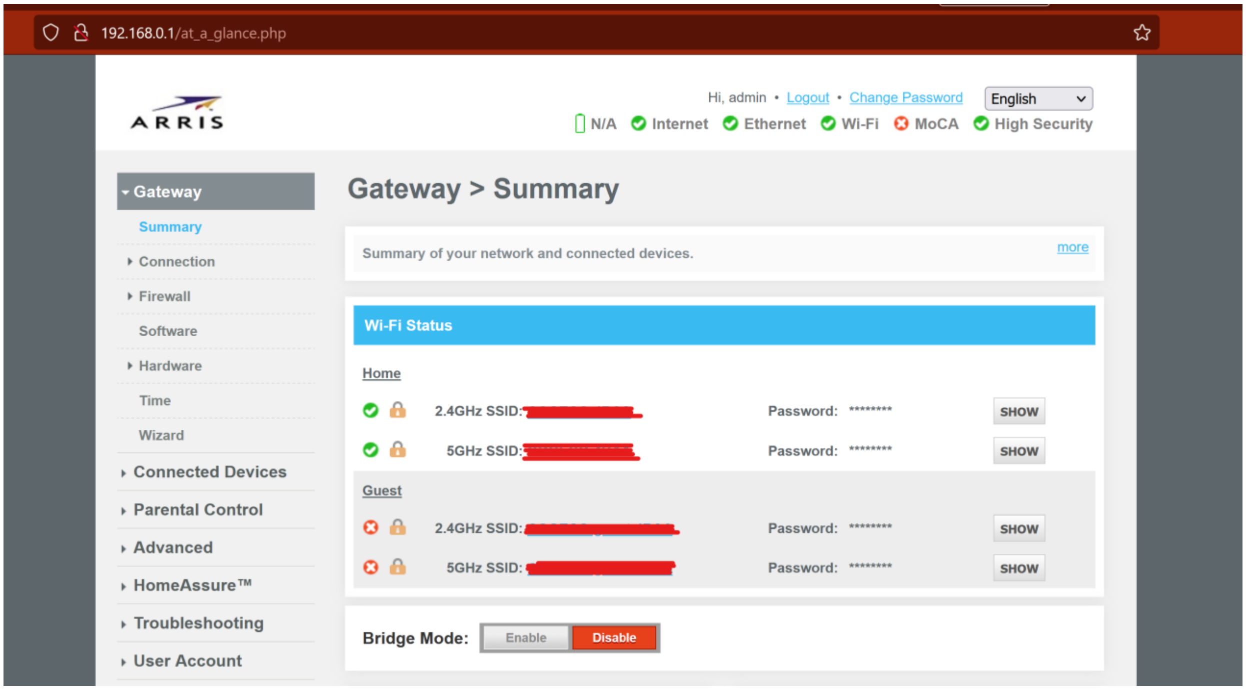
RDK-B-LLC: rdkb-20171127

SDK: 7.1

Wi-Fi Driver: 4.7.23.34.6.0

Figure 41: Firmware Update

- **Network Segmentation:** Priorities your network, this will help you to keep your devices safe from outside network interference.



Gateway > Summary

Summary of your network and connected devices.

Wi-Fi Status

Home

2.4GHz SSID: [redacted] Password: ******** SHOW

5GHz SSID: [redacted] Password: ******** SHOW

Guest

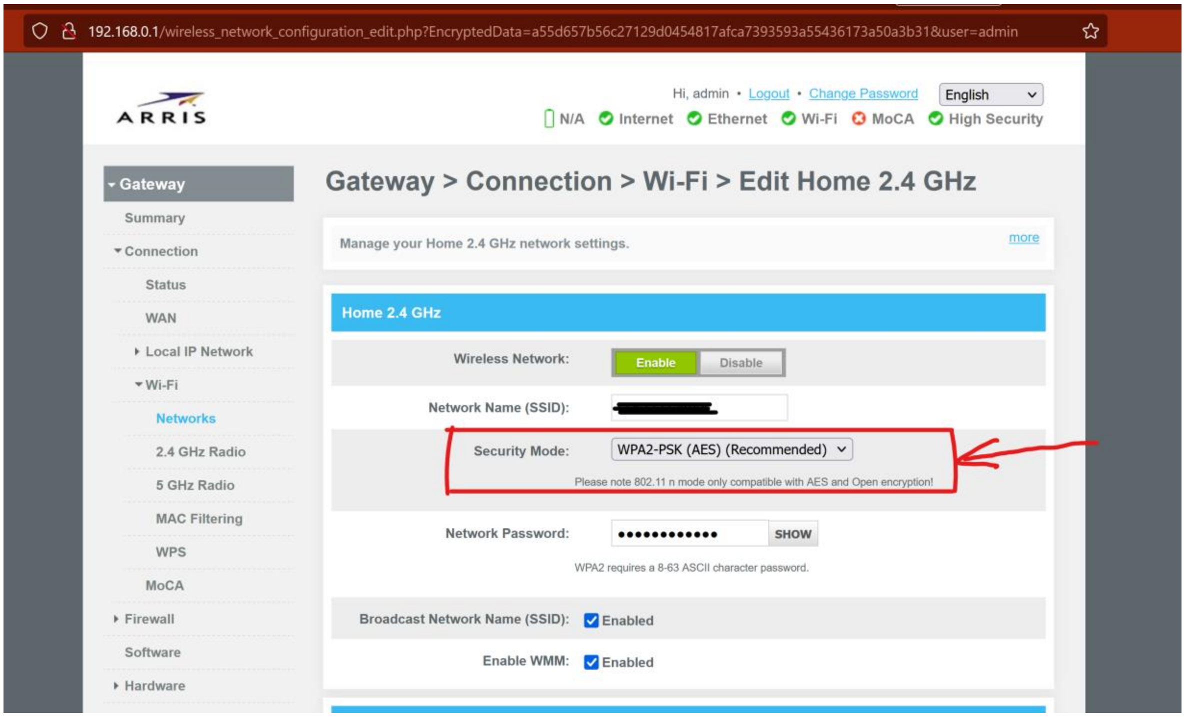
2.4GHz SSID: [redacted] Password: ******** SHOW

5GHz SSID: [redacted] Password: ******** SHOW

Bridge Mode: Enable Disable

Figure 42: Network Segmentation

- **Security Mode check:** defines the type of authentication and encryption (i.e., hiding sensitive data by scrambling data into secret code). Always keep it to the latest version. Todays it is WPA2-PSK/WPA3-PSK.



192.168.0.1/wireless_network_configuration_edit.php?EncryptedData=a55d657b56c27129d0454817afca7393593a55436173a50a3b31&user=admin

Hi, admin • Logout • Change Password English

N/A Internet Ethernet Wi-Fi MoCA High Security

Gateway > Connection > Wi-Fi > Edit Home 2.4 GHz

Manage your Home 2.4 GHz network settings. more

Home 2.4 GHz

Wireless Network: Enable Disable

Network Name (SSID): [redacted]

Security Mode: WPA2-PSK (AES) (Recommended)

Please note 802.11 n mode only compatible with AES and Open encryption!

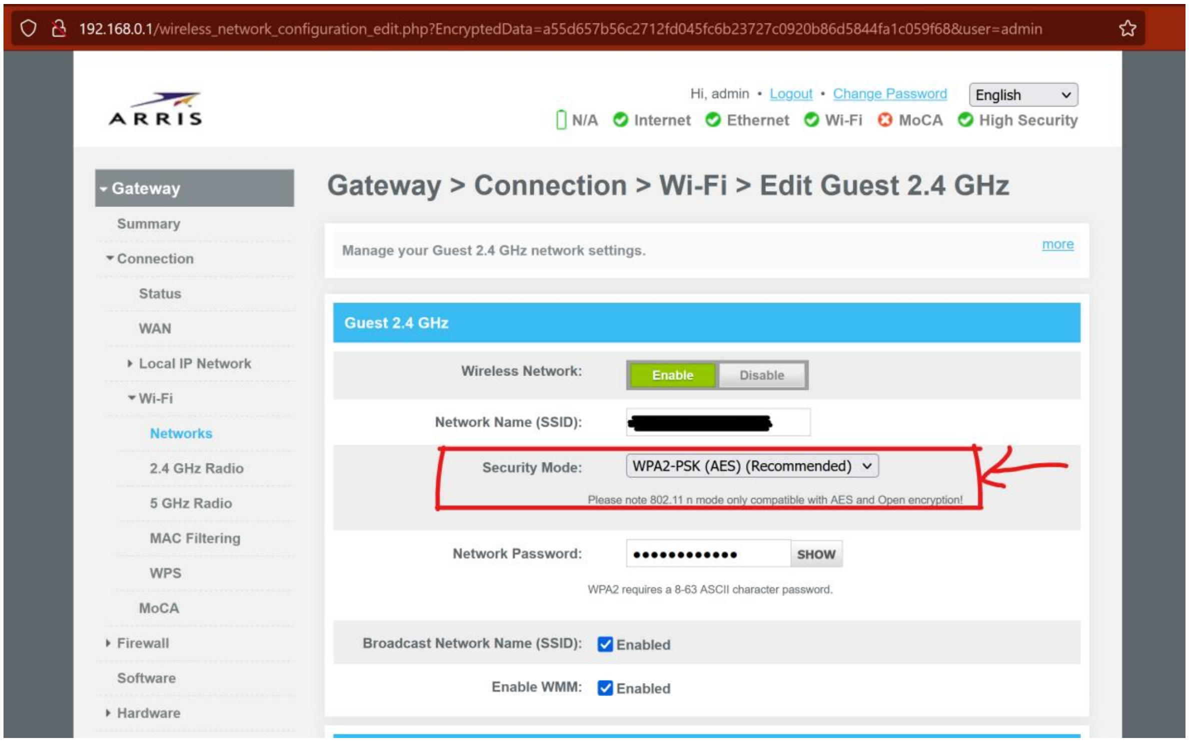
Network Password: •••••••••••• SHOW

WPA2 requires a 8-63 ASCII character password.

Broadcast Network Name (SSID): ☑ Enabled

Enable WMM: ☑ Enabled

Figure 43: Security Mode Check (Personal Network)



192.168.0.1/wireless_network_configuration_edit.php?EncryptedData=a55d657b56c2712fd045fc6b23727c0920b86d5844fa1c059f68&user=admin

Hi, admin • Logout • Change Password English

N/A Internet Ethernet Wi-Fi MoCA High Security

Gateway > Connection > Wi-Fi > Edit Guest 2.4 GHz

Manage your Guest 2.4 GHz network settings. more

Guest 2.4 GHz

Wireless Network: Enable Disable

Network Name (SSID): [redacted]

Security Mode: WPA2-PSK (AES) (Recommended)

Please note 802.11 n mode only compatible with AES and Open encryption!

Network Password: •••••••••••• SHOW

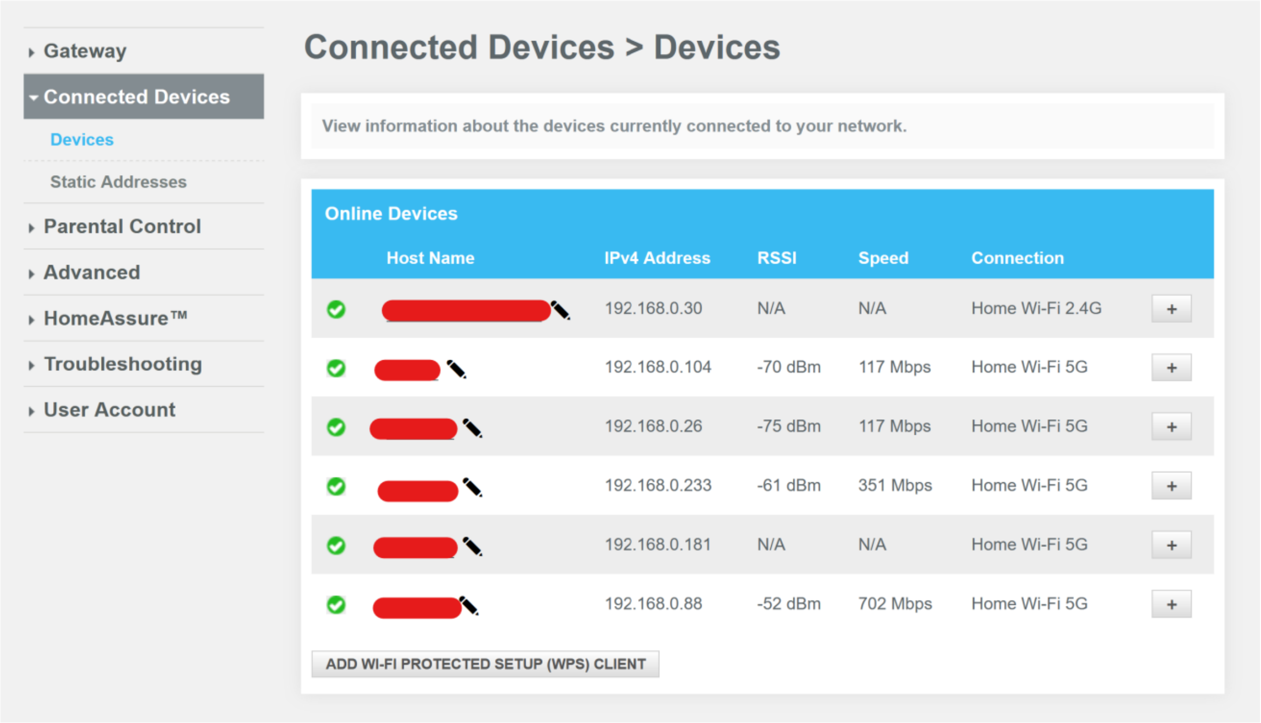
WPA2 requires a 8-63 ASCII character password.

Broadcast Network Name (SSID): ☑ Enabled

Enable WMM: ☑ Enabled

Figure 44: Security Mode Check (Guest Network)

- **Network Monitoring:** In your router settings you will see this setting of connected devices, if you find any unknown device you can kick it out of your network. Also, by clicking on each device you can monitor its bandwidth and usage. If any suspicious activity is found, you can again block any device.



Connected Devices > Devices

View information about the devices currently connected to your network.

Online Devices

	Host Name	IPv4 Address	RSSI	Speed	Connection	
✓	[redacted]	192.168.0.30	N/A	N/A	Home Wi-Fi 2.4G	+
✓	[redacted]	192.168.0.104	-70 dBm	117 Mbps	Home Wi-Fi 5G	+
✓	[redacted]	192.168.0.26	-75 dBm	117 Mbps	Home Wi-Fi 5G	+
✓	[redacted]	192.168.0.233	-61 dBm	351 Mbps	Home Wi-Fi 5G	+
✓	[redacted]	192.168.0.181	N/A	N/A	Home Wi-Fi 5G	+
✓	[redacted]	192.168.0.88	-52 dBm	702 Mbps	Home Wi-Fi 5G	+

Figure 45: List of Connected Devices to the Network

Note: To learn more advance methods of Network monitoring please check : https://www.lifewire.com/ website .

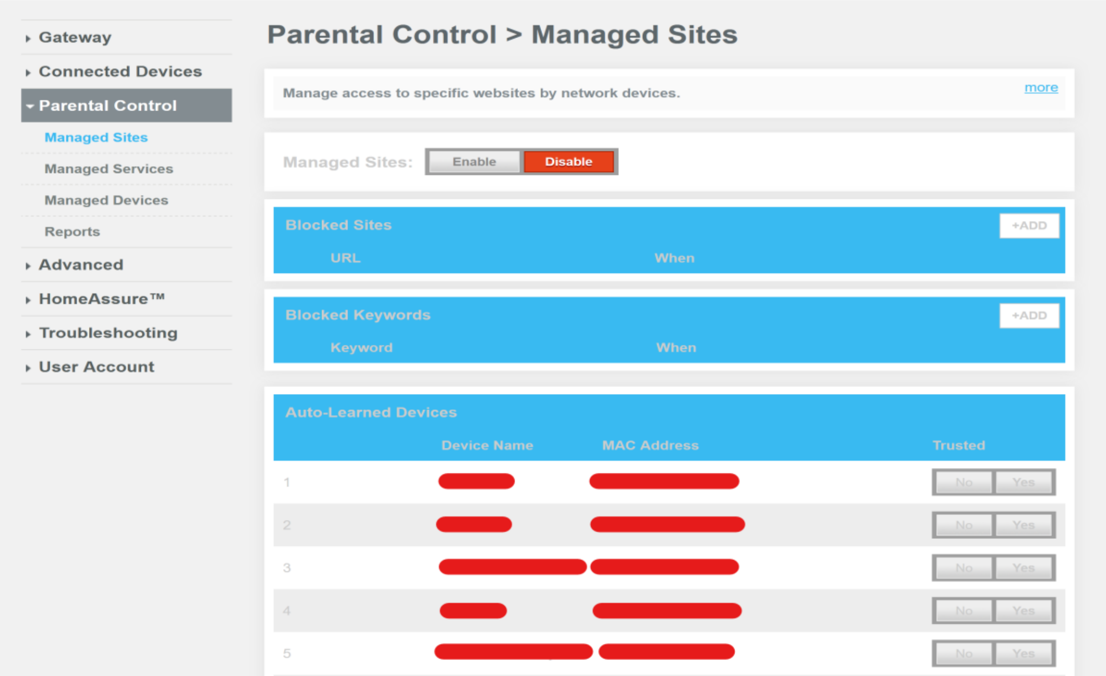
PARENTAL CONTROL:

Figure 46: Parental Control

WHAT IS PARENTAL CONTROL?

- The word "parental controls" relates to the actual use cases. Parents want to ensure that their children are accessing safe content while also setting limits. As a result, Wi-Fi routers integrate two major parental control features: content filtering and access limits.
- Content filtering prevents users from accessing specified web resources on the Internet, such as age-inappropriate content or malicious resources.
- Internet access limits restrict when a user can connect to the Internet via the Wi-Fi router. They function as an on/off switch, denying the user access to the WAN based on specific criteria.

- **Managed Sites Setting:** This setting does both content filtering and access control. Here we can specify the site and any related keyword to block it on the network. Also, we can allow the trusted devices to access the same website.



- Gateway
- Connected Devices
- Parental Control
  - Managed Sites
  - Managed Services
  - Managed Devices
  - Reports
- Advanced
- HomeAssure™
- Troubleshooting
- User Account

Parental Control > Managed Sites

Manage access to specific websites by network devices. more

Managed Sites: Enable Disable

Blocked Sites +ADD

URL	When

Blocked Keywords +ADD

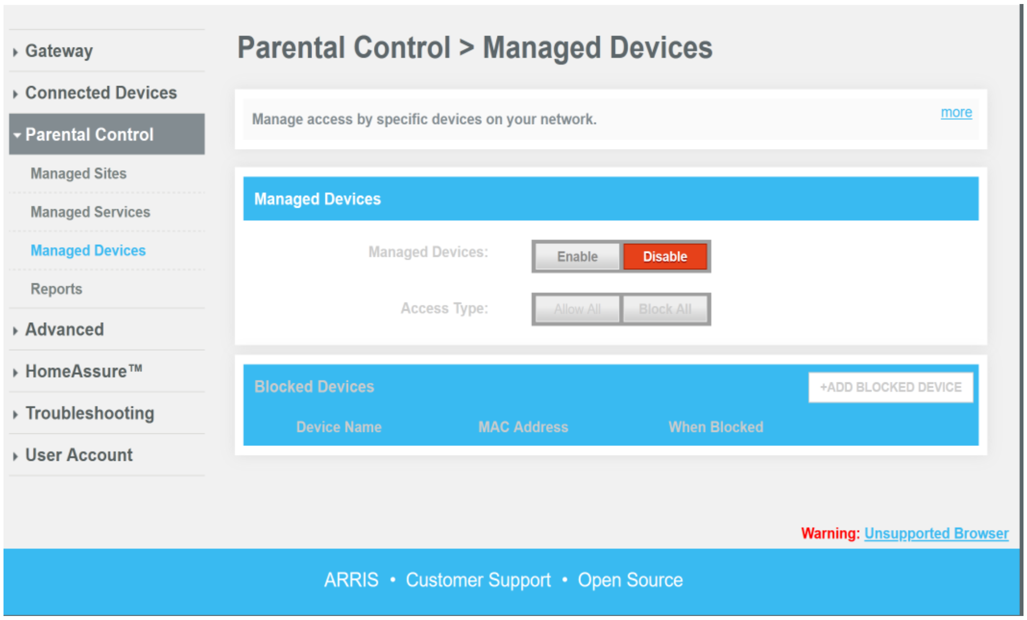
Keyword	When

Auto-Learned Devices

	Device Name	MAC Address	Trusted
1	[redacted]	[redacted]	No Yes
2	[redacted]	[redacted]	No Yes
3	[redacted]	[redacted]	No Yes
4	[redacted]	[redacted]	No Yes
5	[redacted]	[redacted]	No Yes

Figure 47: Managed Sites Control

- **Managed Device:** This is an access control device, where you can allow, what device can connect to router.



- Gateway
- Connected Devices
- Parental Control
  - Managed Sites
  - Managed Services
  - Managed Devices
  - Reports
- Advanced
- HomeAssure™
- Troubleshooting
- User Account

Parental Control > Managed Devices

Manage access by specific devices on your network. more

Managed Devices

Managed Devices: Enable Disable

Access Type: Allow All Block All

Blocked Devices +ADD BLOCKED DEVICE

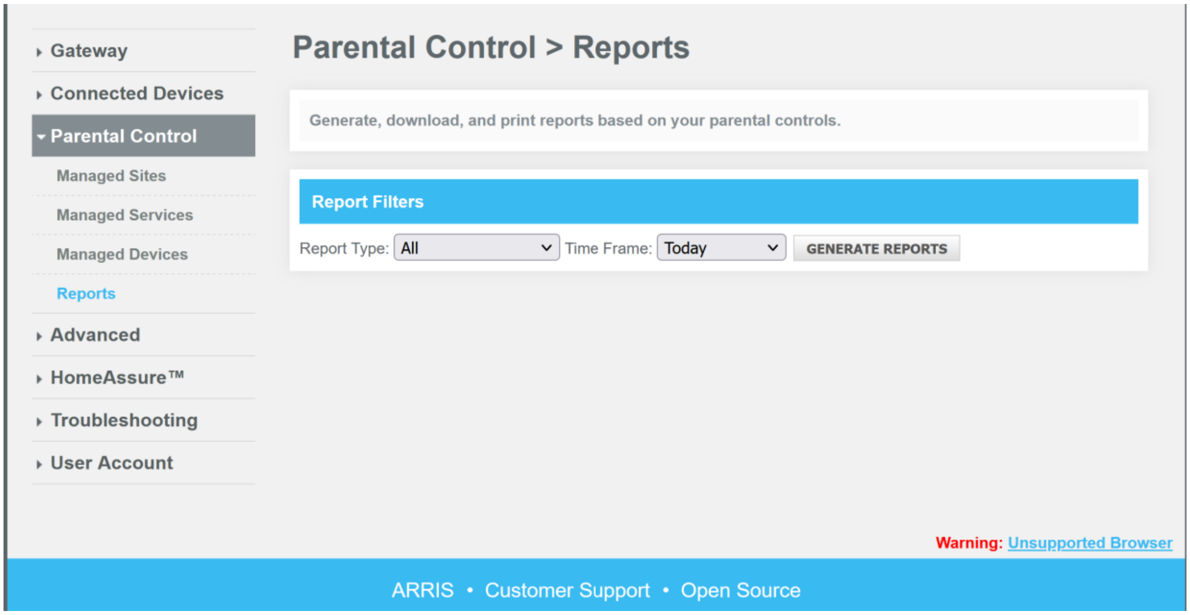
Device Name	MAC Address	When Blocked

Warning: Unsupported Browser

ARRIS • Customer Support • Open Source

Figure 48: Managed Devices Control

- **Report Generation:** This feature allows parents to have a report on their child’s browsing history. This feature allows parents to generate reports on the device connected to router and see all the browsing.



Parental Control > Reports

Generate, download, and print reports based on your parental controls.

Report Type: All

Time Frame: Today

Figure 49:Reports Generation