Glossary of IT Terms

Word/Term:	Definition:	See also:
2FA	Two-Factor Authentication (2FA) is a security process that requires users to provide two different forms of identification to verify their identity before accessing an account or system. This adds an extra layer of security beyond just a password, making it more difficult for unauthorised users to gain access. How 2FA Works: First Factor: Typically, this is something you know, like a password or PIN. Second Factor: This is something you have or are, such as a one-time code sent to your phone, a fingerprint, or facial recognition. Common Methods of 2FA: **SMS Codes**: A code sent to your mobile phone via text message. **Authenticator Apps**: Apps like Microsoft Authenticator or Duo generate time-based codes. **Biometrics**: Fingerprint or facial recognition. **Hardware Tokens**: Physical devices that generate codes. Using 2FA significantly enhances your account security by ensuring that even if your password is compromised, an attacker would still need the second factor to gain access	
Access point	An access point is a networking device that allows wireless devices to connect to a wired network. It acts as a bridge between your devices (like smartphones, laptops, and tablets) and the network, providing a wireless connection for your devices to access network resources Key Functions of an Access Point: **Wireless Connectivity**: Enables wireless devices to connect to a wired network. **Network Extension**: Can extend the range of your wireless network, eliminating dead spots. **Security**: Modern access points come with built-in encryption to secure the wireless network	Network Wi-Fi
BCDR	Business Continuity and Disaster Recovery (BCDR) is a comprehensive approach that combines two critical strategies to ensure an organisation can continue operating during and after a disaster. Here's a breakdown: **Business Continuity (BC)** Focus: Ensures that essential business functions can continue during and after a disaster. Scope: Involves planning for maintaining operations, including processes, resources, and personnel. Proactive: Aims to prevent interruptions and maintain business operations seamlessly. **Disaster Recovery (DR)** Focus: Deals with the recovery of IT systems, data, and infrastructure after a disaster. Scope: Involves restoring critical technology and data to minimise downtime and data loss. Reactive: Focuses on responding to and recovering from incidents. **Key Components of BCDR:**	

	Risk Assessment: Identifying potential threats and their impact on business operations. Business Impact Analysis (BIA): Determining the criticality of business functions and the resources required to support them. Recovery Strategies: Developing plans to recover and restore business operations and IT systems. Testing and Maintenance: Regularly testing and updating the BCDR plans to ensure their effectiveness.	
Broadband	The terms Wi-Fi, broadband, and internet are often used interchangeably, but they refer to different aspects of how we connect and use the web. Broadband refers to high-speed internet access that is always on and faster than traditional dial-up access. It can be delivered through various technologies, including DSL, cable, fibre-optic, and satellite. Broadband is the connection that brings the internet to your home or office. How They Work Together: Broadband provides the high-speed connection to the internet. Internet is the vast network you access through your broadband connection, using Wi-Fi or wired connections Wi-Fi allows you to connect your devices wirelessly to the broadband connection.	Internet Public Wi-Fi Wi-Fi
(The) Cloud	The cloud refers to a network of remote servers hosted on the internet that store, manage, and process data, rather than using a local server or personal computer. This allows users to access their data and applications from any device with an internet connection, providing flexibility and convenience. Key Features of the Cloud: Scalability: Easily adjust resources and storage based on demand. Accessibility: Access data and applications from anywhere with an internet connection. Cost Efficiency: Reduce costs by eliminating the need for physical hardware and maintenance. Reliability: Cloud providers often offer high availability and disaster recovery options. Types of Cloud Services: **Public Cloud**: Services offered over the public internet and shared across multiple users. **Private Cloud:** Dedicated services for a single organisation, often hosted on-premises. **Hybrid Cloud**: A combination of public and private clouds, allowing data and applications to be shared between them.	Internet Network Servers
DNS	DNS stands for Domain Name System. It's essentially the phonebook of the internet. DNS translates human-friendly domain names (like www.calderit.com) into IP addresses (like 192.168.1.1) that computers use to identify each other on the network. This system allows users to access websites using easy-to-remember names instead of having to memorise complex numerical addresses.	Internet IP
Domain	In computing, a **domain** can refer to a couple of different concepts:	Internet IP

	Network Domain: This is a group of computers and devices on a network that are managed as a unit with common rules and procedures. Domains are often used in large organisations to manage resources and security policies centrally. For example, a domain controller manages user accounts, permissions, and security settings for all devices within the domain **Internet Domain**: This refers to a domain name, which is a human-readable address used to access websites on the internet. For example, "calderit.com" is a domain name that points to Calder IT's IP address. Domain names make it easier to remember and access websites without needing to remember numerical IP addresses	Network
DoS attack	A **Denial-of-Service (DoS) attack** is a type of cyberattack where the attacker aims to make a machine or network resource unavailable to its intended users. This is typically done by overwhelming the target with a flood of internet traffic, causing it to slow down or crash. There are different types of DoS attacks, including: **Buffer Overflow Attacks**: These exploit vulnerabilities in software to consume all available memory or CPU time, causing the system to become unresponsive. **Flood Attacks**: These involve sending an overwhelming amount of traffic to the target. A more advanced version is the **Distributed Denial-of-Service (DDoS) attack**, where the traffic comes from multiple sources, making it harder to defend against. Protecting against DoS attacks involves a combination of proactive measures and real-time defences. Increase your Network Security by: Firewalls and Intrusion Detection Systems (IDS) Rate Limiting Redundancy and Load Balancing Load Balancers Anycast Network Regular Updates and Patching DDoS Protection Services Network Segmentation IP Blocking	Firewall IP Network
Firewall	A firewall is a network security device designed to monitor, filter, and control incoming and outgoing network traffic based on predetermined security rules. Its primary purpose is to establish a barrier between a trusted internal network and untrusted external networks, such as the internet. Firewalls can be either hardware or software-based and work by inspecting data packets to determine whether to allow or block them based on a set of rules. These rules can be configured to permit or deny traffic based on various criteria, such as source and destination IP addresses, port numbers, and protocol types There are different types of firewalls, including:	DoS Attack Internet IP Network Phishing Port

	Proxy Firewalls: Act as a gateway from one network to another for a specific application. **Stateful Inspection Firewalls**: Monitor all activity from the opening of a connection until it is closed. **Unified Threat Management (UTM) Firewalls**: Combine stateful inspection with intrusion prevention and antivirus. **Next-Generation Firewalls (NGFW)**: Include advanced features like application awareness and control, integrated intrusion prevention, and cloud-delivered threat intelligence. Firewalls are essential for protecting networks from external threats like viruses, phishing attacks, and denial-of-service (DoS) attacks, as well as internal threats from malicious insiders.	
HTTP/HTTPS	HTTP stands for Hypertext Transfer Protocol. It is the foundation of data communication on the World Wide Web. HTTP defines how messages are formatted and transmitted, and how web servers and browsers should respond to various commands HTTPS stands for Hypertext Transfer Protocol Secure. It is an extension of HTTP and adds a layer of security by using SSL/TLS (Secure Sockets Layer/Transport Layer Security) to encrypt data transferred between the client (e.g., a web browser) and the server. Key Differences Between HTTP and HTTPS **Security**: - HTTP: Transmits data in plain text, making it vulnerable to interception by attacker. - HTTPS: Encrypts data, ensuring that it cannot be easily read by anyone who intercepts it. **Authentication**: - HTTP: Does not provide any authentication of the server, which means users cannot be sure they are communicating with the intended website. - HTTPS: Uses SSL/TLS certificates to authenticate the server, ensuring that users are connecting to the legitimate website. **Data Integrity**: -HTTP: Data can be altered or corrupted during transmission without detection. - HTTPS: Ensures data integrity by detecting any tampering or corruption during transmission. **SEO Benefits:** -HTTP: Websites using HTTP may be flagged as "Not Secure" by browsers, potentially affecting user trust and SEO rankings. - HTTPS: Preferred by search engines like Google, which can improve SEO rankings and user trust. **How HTTPS Works:** SSL/TLS Handshake: When a user connects to an HTTPS site, the browser and server perform a handshake to establish a secure connection. Encryption: Data exchanged between the browser and server is encrypted using cryptographic keys.	Server SSL/TLS

	Certificate Verification: The server presents an SSL/TLS certificate to the browser, which verifies its authenticity. *Using HTTPS is essential for protecting sensitive information, such as login credentials, payment details, and personal data, ensuring a secure and trustworthy browsing experience.*	
IaaS	Infrastructure as a Service (IaaS) is a type of cloud computing service that provides essential computing resources such as servers, storage, and networking on a pay-as-you-go basis. This model allows businesses to rent these resources from a cloud provider instead of maintaining their own physical infrastructure. **Key Features of IaaS:** Scalability: Easily scale resources up or down based on demand. Cost-Efficiency: Pay only for the resources you use, reducing capital expenditures. Flexibility: Quickly provision new applications and environments. Reliability: Benefit from the cloud provider's robust infrastructure and redundancy. **Common Use Cases:** Development and Testing: Quickly set up and dismantle environments. Web Hosting: Host websites and web applications. Storage, Backup, and Recovery: Manage data storage and recovery efficiently. High-Performance Computing: Handle complex computations and large-scale simulations.	Cloud Network Servers
Internet	The terms Wi-Fi, broadband, and internet are often used interchangeably, but they refer to different aspects of how we connect and use the web. The internet is a global network of interconnected computers that communicate with each other using standardised protocols. It allows users to access information, communicate, and share resources worldwide. The internet is what you connect to using broadband and Wi-Fi. **How They Work Together** **Broadband** provides the high-speed connection to the internet. **Wi-Fi** allows you to connect your devices wirelessly to the broadband connection. **Internet** is the vast network you access through your broadband connection, using Wi-Fi or wired connections	Broadband Public Wi-Fi Wi-Fi
ISP	An Internet Service Provider (ISP) is a company that provides individuals and businesses with access to the internet. ISPs offer various types of internet connections, including: **Dial-up** **DSL** (Digital Subscriber Line) **Cable**	Domain Internet

	Fibre-optic **Wireless** In addition to internet access, ISPs may also provide other services such as domain registration and web hosting.	
Malware	Malware, short for "malicious software," refers to any software intentionally designed to cause harm to a computer, server, client, or network. This can include disrupting operations, stealing sensitive information, gaining unauthorised access, or causing other types of damage. Common types of malware include: **Viruses**: Programs that attach themselves to legitimate software and spread when the software is executed. **Worms**: Standalone programs that replicate themselves to spread to other computers. **Trojan Horses**: Malicious software disguised as legitimate software. **Ransomware**: Malware that locks or encrypts data and demands a ransom for its release. **Spyware**: Software that secretly monitors and collects user information. **Adware**: Software that automatically displays or downloads advertising material.	Virus
Network	In computing, a **network** refers to a collection of computers and other devices connected to share resources and information. Here are some key points: **Types of Networks**: The main difference between a Local Area Network (LAN) and a Wide Area Network (WAN) lies in their geographic coverage and network characteristics: **Local Area Network (LAN)** **Coverage**: Covers a small geographic area, such as a single building, office, or campus **Speed**: Typically offers high data transfer speeds (e.g., 1000 Mbps) **Ownership**: Usually owned, controlled, and managed by a single organisation **Components**: Uses devices like switches, bridges, and Ethernet cables **Fault Tolerance**: Generally has fewer issues due to the smaller number of connected devices **Wide Area Network (WAN)** **Coverage**: Spans large geographic areas, such as cities, countries, or even continents **Speed**: Generally has lower data transfer speeds compared to LANs (e.g., 150 Mbps) **Ownership**: Often involves multiple organisations and may use public or leased lines **Components**: Utilises routers, multi-layer switches, and technologies like MPLS, ATM, and satellite links **Fault Tolerance**: More prone to issues due to the larger number of connected systems In summary, LANs are ideal for localised networking with high speeds and easy management, while WANs are designed for broader connectivity over long distances, often involving more complex infrastructure and management **Components**: Networks typically include devices like computers, servers, routers, switches, and other networking hardware. These devices communicate using common protocols, such as the Internet Protocol (IP)	IP Routers Servers Switches

	Benefits: Networks allow for resource sharing, such as printers and files, and enable communication through email, instant messaging, and other applications The largest and most well-known network is the internet, which connects millions of private, public, academic, business, and government networks worldwide	
Password manager	A password manager is a tool designed to help you store, manage, and secure your passwords. Here's how it works: **Storage**: It securely stores all your passwords in an encrypted database. **Generation**: It can generate strong, unique passwords for each of your accounts. **Auto-fill**: It automatically fills in your login details on websites and apps. **Synchronisation**: It syncs your passwords across all your devices, so you can access them anywhere. **Security**: It often includes features like two-factor authentication (2FA) and alerts for compromised passwords. Using a password manager can greatly enhance your online security by ensuring you use strong, unique passwords for each of your accounts without having to remember them all. Using a password manager can significantly enhance your online security, but there are some risks to be aware of: **Single Point of Failure**: If someone gains access to your master password, they could potentially access all your stored passwords. **Data Breaches**: Although rare, password managers can be targeted by hackers. A breach could expose your encrypted data. **Software Vulnerabilities**: Like any software, password managers can have bugs or vulnerabilities that might be exploited. **Trust Issues**: You need to trust the password manager provider with your sensitive information. **Device Security**: If your device is compromised (e.g., through malware), it could affect the security of your password manager. To mitigate these risks, it's important to: Use a strong, unique master password. Enable two-factor authentication (2FA) for your password manager. Keep your software up to date. Choose a reputable password manager with a strong security track record.	2FA
Phishing	Phishing is a type of cybercrime where attackers deceive individuals into revealing sensitive information, such as passwords, credit card numbers, or other personal details. This is typically done through fraudulent emails, messages, or websites that appear to be from legitimate sources **Phishing via email examples**:	Malware 2FA

Tech Support Scams: These emails claim there's an issue with your computer and urge you to download a "fix" that is actually malware[1].
Tax Refund Scams: Posing as tax authorities, these emails promise a refund but aim to steal your financial details
Suspicious Activity Notices: These emails warn of suspicious activity on your account and prompt you to verify your identity by clicking a link[2]
Payment Confirmation Scams: Fake receipts, invoices or charges that prompt you to click on a link to dispute the charge, or make a payment.
Social Media Phishing: Emails that appear to be from social media platforms asking you to verify your account or reset your password.
Always be cautious of unsolicited emails, especially those that create a sense of urgency or ask for personal information. If you're unsure about an email, it's best to contact the organisation directly using a known, trusted method, (do not ply to the email) or contact Calder IT to check the origin of the email.
Phishing via text message, often called **smishing** (a combination of "SMS" and "phishing"), involves cybercriminals sending harmful links or requests for personal information through text messages.
Here are some common signs of smishing:
Unknown Sender: The message comes from a number you don't recognise.
Urgent Language: The message creates a sense of urgency, such as claiming your account will be locked if you don't respond immediately.
Suspicious Links: The message includes a link that looks unusual or doesn't match the supposed sender's website.
Requests for Personal Information: The message asks for sensitive information like passwords, credit card numbers, or account details
If you receive a suspicious text, it's best not to click any links or provide any information. Instead, you can report the message to your mobile provider by forwarding it to 7726 (which spells "SPAM" on a phone keypad) in the UK.

phishing via WhatsApp
Phishing via WhatsApp, often referred to as WhatsApp phishing, involves scammers using the platform to deceive users into revealing sensitive information or installing malware. Here are some common types of WhatsApp phishing scams:
Account Hijacking: Scammers pose as a friend and ask for your WhatsApp verification code, which they use to hijack your account. Once they have control, they can impersonate you to scam your contacts.
Fake Tech Support: Scammers pretend to be WhatsApp support and ask for personal information or direct you to malicious websites.

	Gift Card Scams: Messages claim you've won a gift card and ask you to click a link to claim it. The link often leads to a phishing site designed to steal your information. **Emergency Scams**: Scammers impersonate a friend or family member in distress, asking for money or personal information. *To protect yourself from these scams:* *Verify Contacts: Always verify the identity of the person contacting you, especially if they ask for sensitive information.* *Avoid Clicking Links: Be cautious of unsolicited links and attachments.* *Enable Two-Step Verification: Add an extra layer of security to your account.* *Report Suspicious Messages: Use WhatsApp's reporting feature to flag suspicious messages.*	
Port	In the context of computer networking, a port is a virtual point where network connections start and end. Ports are used to differentiate between different types of network traffic, allowing multiple services to run on a single device. Each port is associated with a specific process or service, identified by a port number. Ports are identified by numbers ranging from 0 to 65535. Common examples include port 80 for HTTP and port 443 for HTTPS. Well-Known Ports: Range from 0 to 1023 and are reserved for common services (e.g., HTTP). Registered Ports Range from 1024 to 49151 and are used by less common applications. Dynamic/Private Ports: Range from 49152 to 65535 and are used for temporary or private connections. **How Ports Work**: When data is sent over the internet, it is directed to a specific port on the receiving device. This helps the device understand which application or service should handle the incoming data.	Internet Network HTTP/HTTPS
Public Wi-Fi	Public Wi-Fi refers to wireless internet access available in public places like cafes, airports, libraries, hotels, and more. While it's convenient, it also comes with several security risks: **Man-in-the-Middle Attacks**: Attackers can intercept the communication between your device and the Wi-Fi network, potentially capturing sensitive information. **Unencrypted Network**: Many public Wi-Fi networks lack encryption, making it easier for attackers to access your data. **Malware Distribution**: Hackers can exploit vulnerabilities to distribute malware to devices connected to the network. **Wi-Fi Snooping and Sniffing**: Attackers can use special software to eavesdrop on Wi-Fi signals, capturing data being transmitted over the network. ***Tips for Staying Safe on Public Wi-Fi:*** *Use a VPN: Encrypts your internet connection, making it harder for attackers to intercept your data.* *Avoid Sensitive Transactions: Refrain from accessing banking sites or entering personal information while on public Wi-Fi.*	Broadband HTTPS Internet Malware VPN WI-FI

	Keep Software Updated: Ensure your device's operating system and applications are up to date to protect against vulnerabilities. *Disable File Sharing: Turn off file sharing and other network services when connected to public Wi-Fi.* *Use HTTPS: Look for websites that use HTTPS, which encrypts data between your browser and the website.*	
Router	A router is a networking device that forwards data packets between computer networks. It connects multiple devices to the internet or to other networks, directing data traffic efficiently to ensure that information reaches its intended destination. Key Functions of a Router: **Data Routing**: Determines the best path for data packets to travel across networks. **Network Management:** Manages traffic within a local network (LAN) and between different networks (WAN). **Security**: Often includes features like firewalls and content filtering to protect the network from unauthorised access Types of Routers: **Home Routers**: Used in residential settings to connect home devices to the internet. **Enterprise Routers**: Used in business environments to manage large volumes of data and connect multiple networks. **Core Routers**: Used by internet service providers to manage data traffic across the internet backbone.	Firewall Network
SaaS	**Software as a Service (SaaS)** is a cloud computing model where software applications (apps) are delivered over the internet. Instead of installing and maintaining software on individual computers, users access the software through a web browser or mobile app Here are some key points about SaaS: **Accessibility**: SaaS applications can be accessed from any device with an internet connection, making it convenient for remote and hybrid work environments **Cost-Effective**: Typically, SaaS operates on a subscription model, reducing the need for large upfront investments in software and hardware **Maintenance-Free**: The SaaS provider handles all updates, maintenance, and infrastructure management, allowing users to focus on using the software **Scalability**: SaaS solutions can easily scale to accommodate growing business needs without requiring significant changes to the underlying infrastructure Common examples of SaaS applications include email services, customer relationship management (CRM) systems, and office productivity tools like Microsoft Office 365	Cloud internet
server	A server is a specialised computer or software system designed to provide services, data, or resources to other computers, known as clients, over a network. Servers can perform a wide range of tasks, such as: Data Storage and Retrieval: Storing and managing data, making it accessible to authorised users. Website Hosting: Hosting websites and delivering web pages to users' browsers.	Network Spam

	Email Services: Managing the flow of electronic messages, including spam filtering and user authentication. Application Hosting: Running applications and software services for users. File Sharing: Providing a centralised location for storing and sharing files within a network. Servers are essential for the functioning of the internet and many organisational networks, ensuring that resources are available, reliable, and secure for users.	
Spam	**Internet Spam:** Unsolicited and often irrelevant messages sent over the internet, typically to many users. These messages are usually for advertising, phishing, spreading malware, etc. For example, unwanted emails or messages on social media **Email Spam**: Unsolicited emails often containing advertisements, phishing attempts, or malware. Examples include offers for products, fake lottery wins, and phishing emails that mimic legitimate companies. **Phishing Scams**: Emails or messages designed to trick recipients into revealing personal information, such as passwords or credit card numbers, by pretending to be from a trusted source2. **Spoofing:** Emails that appear to come from a known contact or legitimate organization but are actually from spammers trying to deceive the recipient. **Chain Letters:** Messages that encourage recipients to forward them to others, often with threats of bad luck or promises of good fortune. **Hoaxes**: False information or promises, such as miracle cures or get-rich-quick schemes, intended to mislead recipients. **Money Scams:** Requests for money, often involving stories of hardship or promises of large rewards in return for a small upfront payment. **Malspam**: Spam emails that contain malware or malicious links, aiming to infect the recipient's device. **Social Media Spam**: Unwanted messages or comments on social media platforms, often promoting products or containing malicious links	Phishing Malware Spoofing
SPF DKIM and DMARC	SPF, DKIM, and DMARC are three key technologies used to enhance email security and prevent email spoofing and phishing attacks. Here's a brief overview of each: **SPF** (Sender Policy Framework)SPF is an email authentication method that allows domain owners to specify which mail servers are permitted to send emails on behalf of their domain. It works by adding a DNS record that lists the IP addresses authorized to send emails. When an email is received, the recipient's mail server checks the SPF record to verify if the email came from an authorized server. **DKIM** (DomainKeys Identified Mail) DKIM adds a digital signature to the email headers, which can be verified by the recipient's mail server to ensure the email has not been altered in transit. This signature is created using a private key, and the corresponding public key is published in the domain's DNS records. If the signature matches, it confirms that the email is legitimate and has not been tampered with.	DNS IP Phishing spoofing

	DMARC (Domain-based Message Authentication, Reporting, and Conformance) DMARC builds on SPF and DKIM by providing a way for domain owners to specify how to handle emails that fail SPF or DKIM checks. It also offers reporting capabilities, allowing domain owners to receive feedback on how their emails are being processed and whether any unauthorised emails are being sent from their domain. DMARC policies can instruct receiving mail servers to quarantine, reject, or accept emails based on the results of SPF and DKIM checks. Together, these technologies help ensure that emails are authenticated and reduce the risk of email-based attacks.	
Spoofing	Spoofing is a type of cyber attack where a malicious actor disguises their identity as a trusted source to deceive victims. This can involve various forms of communication, such as: **Email Spoofing:** Forging the sender's address to make an email appear as if it's from a legitimate source. **Caller ID Spoofing**: Falsifying the caller ID to make it look like the call is coming from a trusted number. **Website Spoofing**: Creating a fake website that mimics a legitimate one to steal sensitive information. **IP Spoofing**: Altering the source IP address in network packets to impersonate another device. **Text Message Spoofing**: Sending SMS messages that appear to come from a trusted contact or organisation. Spoofing attacks often involve social engineering tactics to manipulate victims into taking actions that benefit the attacker, such as revealing personal information or transferring money.	IP
SSL/TLS	SSL(Secure Sockets Layer) and TLS (Transport Layer Security) are cryptographic protocols designed to provide secure communication over a computer network. Key Points about SSL/TLS: **Encryption**: SSL/TLS encrypts data transmitted between a client (e.g., a web browser) and a server, ensuring that the data remains private and secure. **Authentication**: These protocols use certificates to authenticate the identity of the server, ensuring that users are communicating with the intended website. **Data Integrity**: SSL/TLS ensures that data is not tampered with during transmission. Evolution from SSL to TLS: -SSL: The original protocol, with versions SSL 2.0 and SSL 3.0, both of which have known security vulnerabilities and are now deprecated[1]. TLS: The successor to SSL, with improved security features. The most current version is TLS 1.3, which addresses many of the vulnerabilities found in SSL[1]. **How SSL/TLS Works:** Handshake Process: When a client connects to a server, they perform a handshake to establish a secure connection. This involves exchanging cryptographic keys and verifying the server's certificate.	Network Server

	Data Encryption: Once the connection is established, all data transmitted between the client and server is encrypted using the agreed-upon keys. Using SSL/TLS is essential for protecting sensitive information, such as login credentials, payment details, and personal data, ensuring a secure and trustworthy browsing experience. You will know that a website has SSL/TLS certificate-when you see the padlock icon	
Tenant	In computing, a tenant refers to a group of users who share common access and privileges within a software application (app). This concept is often used in multi-tenant architectures, where a single instance of a software application serves multiple clients or organisations, known as tenants Each tenant has isolated access to their data, configurations, and other resources, making it seem as if they are using their own instance of the application, even though they share the same underlying infrastructure. This is particularly common in Software as a Service (SaaS**)** applications, where the service provider can efficiently manage and maintain a single application while serving multiple customers	SaaS
Virus	A computer virus is a type of malicious software (malware) designed to replicate itself by modifying other computer programs and inserting its own code into those programs. When the infected program runs, the virus code is executed, which can lead to various harmful effects such as data corruption, system crashes, or unauthorised access to sensitive information	Malware
VoIP	VoIP, or Voice over Internet Protocol, is a technology that allows you to make voice calls using an internet connection instead of traditional phone lines. How it works: VoIP converts your voice into digital signals that travel over the internet. When you make a call, these signals are sent to the VoIP service provider, which then routes them to the receiver, converting them back into voice signals. Devices used: You can use VoIP on various devices, including computers, smartphones, tablets, and specialised VoIP phones. Features: Modern VoIP services offer more than just voice calls. They can include video calls, file transfers, group calls, and more. VoIP is popular for its cost-effectiveness and versatility, making it a great option for both personal and business communication.	internet
VPN	A VPN (Virtual Private Network) is a service that creates a secure, encrypted connection between your device and the internet. This connection, often referred to as a “tunnel,” routes your internet traffic through a server operated by the VPN provider, masking your IP address and encrypting your data.	IP ISP

	Using a VPN (Virtual Private Network) when working from home offers several important benefits: Enhanced Security: A VPN encrypts your internet connection, protecting your data from cybercriminals, especially when using public or unsecured Wi-Fi networks. Privacy Protection: It hides your IP address and online activities from your Internet Service Provider (ISP) and other potential snoopers Access to Company Resources: Many companies use VPNs to allow remote workers secure access to internal networks and resources, ensuring that sensitive information remains protected. Bypass Geo-Restrictions: A VPN can help you access websites and services that may be restricted in your region, which can be useful for both work and personal use. Prevent ISP Throttling: Some ISPs throttle your internet speed based on your activities. A VPN can help prevent this by masking your online activities. Using a VPN is a simple yet effective way to enhance your online security and privacy while working from home	
Wi-Fi	The terms Wi-Fi, broadband, and internet are often used interchangeably, but they refer to different aspects of how we connect and use the web: Wi-Fi is a wireless networking technology that allows devices like smartphones, laptops, and tablets to connect to the internet without using cables. It uses radio waves to transmit data between your device and a router, which then connects to the internet. How They Work Together Broadband provides the high-speed connection to the internet. Wi-Fi allows you to connect your devices wirelessly to the broadband connection. Internet is the vast network you access through your broadband connection, using Wi-Fi or wired connections	Broadband Internet Public Wi-Fi router