Essential cyber security awareness training topics

Passwords and passphrases

Note: according to the Verizon data breach investigations report, compromised passwords are responsible for 81% of hacking-related breaches. A key part of overall information security is securing your passwords.

Characteristics of strong passwords

- At least 15 characters, the more characters, the better
- A mixture of both uppercase and lowercase letters
- A mixture of letters and numbers

Note: do not use < or > in your password, as both can cause problems in web browsers

A strong password is hard to guess, but it should be easy for you to remember—a password that must be written down is not strong, no matter how many of the above characteristics are employed.

Examples of weak passwords

- Any word that can be found in a dictionary, in any language (e.g., Airplane or aeroplano).
- A dictionary word with some letters simply replaced by numbers (e.g., A1rplan3 or aeroplan0).
- A repeated character or a series of characters (e.g., AAAAA or 12345).
- A keyboard series of characters (e.g., Qwerty or poiuy).
- Personal information (e.g., Birthdays, partner name, kids name, names of pets or friends, social security number, addresses).

Tips for keeping your password secure

- Change it regularly—once every three to six months.
- Change it if you have the slightest suspicion that the password has become known by a human or a machine or unusual activity.
- Avoid typing it on computers that you do not trust, for example, in an internet café.

- Never save it for a web form on a computer that you do not control or that is used by more than one person.
- Never tell it to anyone, and never write it down.
- Use a different password for every online account you have

Tips for creating a strong password/passphrase

Long passwords are strong passwords. A straightforward way to create a good password is to make a passphrase, which is four or more random words. Not only are passphrases easier to remember, but they are also as strong as a password that uses a long mix of numbers, letters, and symbols.

You can try making a passphrase that is a sentence or fun phrase unique to you.

- For example, popcornwithbutterisbest or catseatpotatochips
- Another idea is to look around you and pick four random items, for example coffeelemoncupflowers
- Or use a web link like- https://bitwarden.Com/password-generator/ choose type – passphrase and generate a random phrase you like. Example- boogieman-oil-unrelated-rascal

Password manager

How safe are password managers?

Like anything else online, password managers are not fool proof. But they do make it much more difficult for anyone to get access to your personal information.

Even if someone got access to your password manager, they would not get access to the information you store in it without your master password. Password managers encrypt your data. This means that you are the only person who can see it.

If you want to add an extra layer of security to your password manager, you can turn on two-factor authentication (2FA). That way an attacker would need your password and an additional thing, like a one-time code, to get into your password manager.

Using a password manager is an easy way to protect yourself online — and you will only need to remember one password for all your online accounts.

Why do you need a password manager?

Passwords need to be unique, long, and strong. There are so many accounts that need a password that it is hard to remember them all. That is where password managers are useful. You do not have to try to remember lots of different passwords, or risk re-using a version of the same one.

What is a password manager?

A password manager is software that saves all your passwords. Using a password manager is like putting your passwords in a safe that only you have the key to.

- Store and protect all your passwords
    - The password manager encrypts your passwords so no-one else can access them.
- Create and store unique passwords
    - A password manager can choose and remember long complicated passwords for you so they can all be different.
- Store valuable information
    - They also let you store answers to your security questions or two-factor authentication backup codes.

There are a lot of password managers available, look at reviews online to see which is best for you and feel free to contact us for advice and help.

Options:

1. Jumpcloud - https://jumpcloud.Com/platform/password-manager
2. 1password - https://1password.Com/business/
3. Bitwarden - https://bitwarden.Com/products/business

Multifactor authentication – MFA/2FA

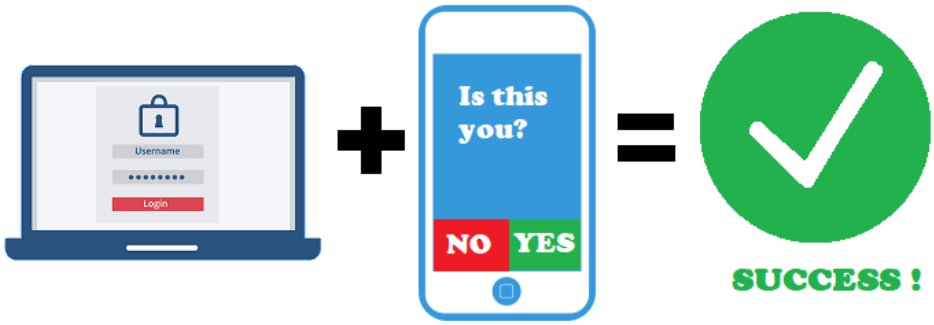
Use two-factor authentication to protect your accounts

When you log in to your accounts online, you mostly use a simple 'username and password' combination to do so. Adding two-factor authentication (2FA) to your login process is a straightforward way of adding an extra layer of security to your accounts.

The problem with relying on a username and password style of login is that you cannot always keep your password safe. Your password could be stolen:

- Through a scam, like phishing
- From a business you have an account with if they have a data breach.

Adding another level of security with 2FA makes it harder for an attacker to access your online accounts — just knowing your password is not enough.



How 2FA works

When you log into an online account with a username and password, you are using what is called single factor authentication. You only need one thing — your password — to verify that you are who you say you are.
With 2FA, you need to provide two things — your password and something else — before you can access an account.

You can authenticate (prove you are you) based on:

- Something you know
- Something you have, and
- Something you are.

Something you know could be your:

- Password
- Passphrase
- Security questions, or
- PIN (personal identification numbers) number.

Something you have could be:

- A physical device, for example:
    - Security tokens and fobs assigned to a specific person that generates a temporary access code, or
    - Your phone, where you get a call back to press certain phone keys to grant access to an account
- Software, such as an application like google authenticator, that:
    - Sends a notification to your smartphone, or
    - Provides you with a temporary access code.

Something you are includes things like:

- Fingerprint scans, and
- Voice recognition.

For example: with 2FA, if you want to log into one of your social media accounts, you might need both your password and a temporary access code from an app on your phone. That means that even if someone finds out what your password is, they cannot get into your account with that alone. They would also need to have physical access to your phone so they can get the code, which is not likely.

Ransomware

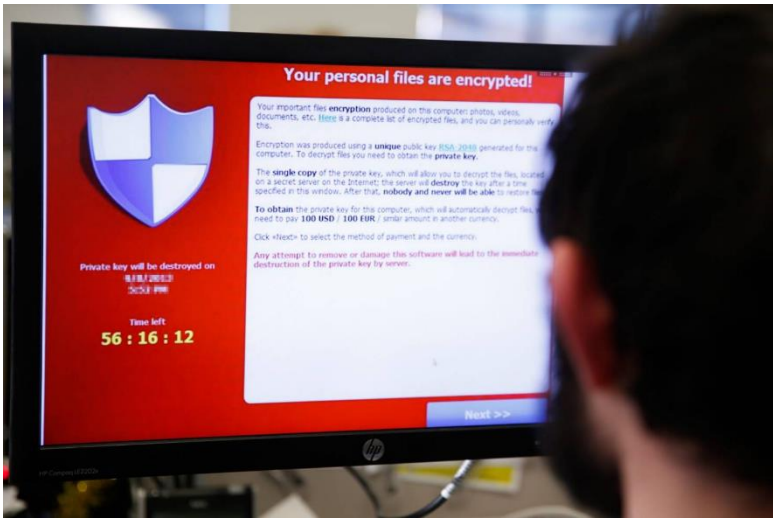
Ransomware is a type of malicious software that denies someone access to their files or computer system unless they pay a ransom. This type of attack can target anyone, from individuals and small businesses to large organisations.

The first sign of a ransomware attack is often a text file pop up or a background, or that you are suddenly unable to access or open any files. The attacker will then demand that you pay money ‘a 'ransom' to get your files back.

Ransomware can get into your computer in the same way that malware or a virus does for example, through a phishing campaign, which is a type of email scam.

There are steps you can take to recover from a ransomware attack but the best thing you can do is understand how to prevent an attack in the first place:

- Always update your operating system and your apps when new versions are available. You can set this up to happen automatically with windows and a lot of other applications like office.
- Make sure you back up your files regularly. This includes the files on your computers, phones, and any other devices you have. You can:
    - Do an 'offline' or 'cold' backup. Back up the data to an external hard drive and then remove the hard drive from your device.
    - Do a cloud backup to dropbox or a similar online hosting service.
- Install antivirus and anti-ransomware software on your computer and update it regularly.
- Do not enable macros in Microsoft office.



If you are affected by ransomware

- Unplug your machine from the network or disconnect from the wireless.
- Call us immediately – let your colleague's and managers know.
- We will:
    - Check to see if you have 'real' ransomware on your computer. Scammers sometimes only claim to have installed ransomware as a tactic to get you to pay them.
    - Restore your computer to its factory settings and rebuild it for you if we cannot remove the malicious software, this may also erase all your files.
    - Advise you on security to protect yourself in the future.
    - Install security protection for you.

We do not recommend that anyone pay ransoms because there is no guarantee you will get your data back. Paying a ransom could also put you at risk of further attacks because if an attacker sees that you are willing to pay them, they could simply target you again.

Report it to CERT NZ, either via their online reporting tool at www.Cert.Govt.Nz/report, or their contact centre 0800 CERT NZ.

Phishing/spear phishing and whaling

Phishing

Phishing scams are one of the most common, prolific, and successful attacks we see. It is important to know how to protect your business against them.

Scammers run phishing campaigns a lot because they are effective and do not cost much to run. It is easy for them to send phishing emails to 10,000 people, for example. Even if only 5% of people respond by clicking a link in the email, they will still have had success with 500 people.

One of the challenges with phishing is that it exploits people's everyday behaviour. Businesses often send emails to customers asking them to:

- Click on links to the business's website
- Log into their account when they get there.

Phishing scams mimic this behaviour to appear legitimate. And, whether it is a legitimate request or a phishing attack, customers are likely to expect to do this. They will follow the instructions they are given, assuming the request is legitimate. But if it is not, the scammers can:

- Trick them into giving up their information or account login details, or
- Install malicious software — like ransomware — on their computers.

Targeted email scams to your business are harder to spot so you are more likely to trust them.

Spear phishing and whaling

Most people have heard of — or have experienced — phishing. It is a common type of email scam. The sender pretends to be a trustworthy organisation in an attempt to get you to provide them with personal information. It affects many people at once and targets them at random.

Spear phishing and whaling scams are much more targeted in their approach. Their goal is to get information about a company or organisation from someone who works there. It is important to note that spear phishing and whaling attacks can be a precursor to another, more serious attack.

In a spear phishing attack, people within a company receive an email asking them to provide the sender with confidential company information. The emails will look like they have come from a particular department or person in the company.

Whaling specifically targets the management or executives in a company — the 'big fish.' These are usually the people who have the most authority and the most access to sensitive business information.

Like phishing, spear phishing and whaling are email scams, but they are much harder to spot. The emails look like they have come from someone within the company, so you are much more likely to trust them. The attacker's aim is to get information about your business, for example:

- Staff credentials
- Financial information
- Personally identifiable information (PII) about your customers
- Trade secrets or intellectual property (IP).

Attackers take time to plan and set up spear phishing and whaling attacks. Successful attacks are very profitable, so the amount of time spent crafting an attack is often worth it for the gain.

Before an attack is launched, the attacker will gather as much information about their target as possible. This can be from social media, like LinkedIn or Facebook, search engines or through the company's website. There is often a lot of useful information available, such as:

- Company information — like details of staff and business partners — on the company website
- Personal information — like people's names, their date of birth, and their hobbies — on social media.

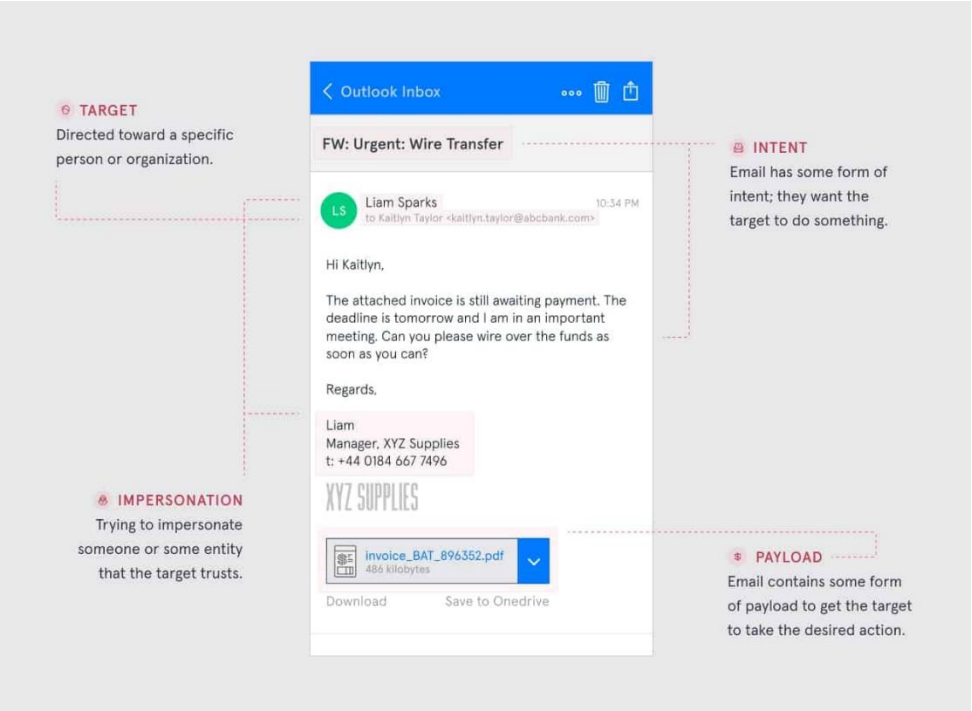
This information can be used to tailor an attack to specific people. The more personal and customised an attack, the more likely it is to work.

Spear phishing and whaling emails will often refer to their subject by name and job title. They might request that you:

- Send them information by return email
- Open an attachment
- Pay an invoice
- Visit a fake website to enter personal information, like login details.

These requests seem urgent and sound legitimate. For example:

- A staff member may get an email that looks like it has come from the CEO. It could ask them to pay an invoice on their behalf, or send them private staff details
- A CEO may receive an email asking them to click on a link to confirm their login details on the company website
- An email may go out to staff that looks like it is from HR, asking them to login and change their password on the HR system.



Reduce your risk

As spear phishing and whaling attacks are difficult to recognise, you might not know you have been targeted until it is too late. Although you cannot prevent an attack, there are things you can do to reduce the risk for your business. A mix of staff education, technology, and validation of the processes you use to prevent these attacks is key to reducing your risk. Talk to your IT support person or a local computer services company if you need help implementing any of these steps.

- Train your staff to know what to look out for. Make sure they understand what to do in certain circumstances — for example, when they get an unexpected email asking them to pay an invoice.

- Confirm any email requests that you are not expecting, or that seem strange, by another means. Call the sender to confirm the request if you can. If a request looks like it has come from within the business, check it with the sender by phone or in person if you can.
- Do not click on web links sent by someone you do not know, or that seem out of character for someone you do know. If you are not sure about something, contact the person you think might have sent it to check first.
- Do not give out personal or business information by email.
- Put privacy settings on your social media accounts to limit who can see them and keep details about you or business to a bare minimum.
- Think about implementing a social media policy for your business. This can help guide staff on what they can or cannot post about their work.
- Ensure that proper security measures are in place for your organisation. Think about:
    - Antivirus/EDR/XDR
    - Firewalls
    - Email filtering
    - Antispam/mail security
    - Limiting access to external websites within your network
    - Segmenting highly privileged accounts (like administrator and root accounts)
    - Documenting and testing processes for dealing with security incidents
    - How you monitor and react to security events.
- Keep your support contracts (with your antivirus provider or your firewall provider, for example) up to date.
- Make sure that you have an incident response plan in place for dealing with security events.
- Regularly validate the security processes you have in place to ensure that they work as expected and update them if they do not.
- Report any phishing attempts

Public wi-fi

Public wi-fi is not secure

When you are at home, you can take steps to keep your home wireless network secure — like using a strong router password, limiting what devices can get onto your network, and turning on encryption, which scrambles the information you send over the internet into a code that cannot be read by others. But when you are using your favourite coffee shops or airport wi-fi, there is not a lot you can do to control its network security.

Why does it matter? If the network is not secure, and you log into an unencrypted site — or a site that uses encryption only on the sign-in page — other users on the network can see what you see and send. They could hijack your session and log in as you. New hacking tools — available for free online — make this easy, even for users with limited technical knowledge. Your personal information, private documents, contacts, family photos, and even your login credentials could be up for grabs.

A scammer also could use your account to impersonate you and scam people on your contact lists or test your usernames and passwords on other websites — including sites that store your financial information. If a scammer gets your personal or financial information, they could steal your identity.

When you sign on to public wi-fi, you may also be sharing your data with the companies providing the wi-fi. Many public wi-fi networks such as in airports and hotels will also prompt you to install a “digital certificate” to use their internet. They may do this to scan your traffic for malware — but this also allows them to read your traffic, even if it is to a site using https (which encrypts information).

There are steps you can take to protect your information, even in public.

Ways to encrypt your information

While there is not much you can do to make a public wi-fi network more secure, you can do some things to help keep your data secure on public wi-fi:

- Connect to websites securely. If you see https in the web address, you have a secure connection to the website. But using https does not mean a website is legit. Scammers know how to encrypt sites, too. They know that people assume https means a website is safe — so they have started adding it to their websites, as well. So, your data is encrypted on its way to the site, but it will not be safe from scammers operating that site.
- Consider using a VPN app. Some virtual private networks, known as vpns, offer encryption.
- Use your mobile data. Your mobile data is usually encrypted. If you are on the go, do not have the option of using a secure website, and have no VPN encryption, consider using your mobile data instead of wi-fi. This is a good option when you are putting personal information into apps, since it can be hard to know if they are encrypted.

Mobile security

Mobile security best practices

When it comes to mobile device security, there is a lot to understand. Not only will management need to be aware of the risks and threats, but users are increasingly targets for malicious attacks —making ongoing education and training essential!
Below are some of the best practices you can implement to keep mobile devices safe and data secure.

User authentication

Since lost phones and theft are a big issue when it comes to securing mobile devices and data, implementing policies towards authentication is important. Make sure that user authentication is one of the top priorities in your organization. Authentication comes in the form of:

- Passwords
- Biometrics (fingerprint and facial recognition)
- Personal identification numbers (pins)

Implementing enterprise authentication policies is more than just passwords and pins; it also means educating end-users about best practices for authentication. 65% of users will admit to using the same password, even though 91% of users responding to a survey by LastPass claimed they understood the risks of password reuse.

It is best to implement password policies as well as two-factor authentication (2FA) methods when available. You want to ensure that users understand not only the importance of authentication but also the risks.

Upgrading regularly

Outdated mobile operating systems pose a significant risk. With almost 90% of android phones running outdated software, this is not a small issue. Keeping your team and data safe means developing policies that will ensure devices are always up to date.

Both google and android will frequently update through software updates and security patches. These updates help resolve known security issues and vulnerabilities. Keeping users safe is a bit more complicated than just updating software, though.

Updating can pose a risk in and of itself. From a security perspective, the update process can trigger a re-vetting of a devices' security clearance. This means that updates might impact the performance of the device — in turn decreasing user productivity. Nevertheless, security updates are essential to meeting the evolving threat landscape.

Backups

Keeping data secure also means keeping data intact. Since a lot of variables are out of an organization's control, like user behaviour, it is critical to have a backup policy. Backing up data will help fill the gaps if an event occurs, like the loss or theft of a device.

While backups can happen regularly, it should be noted that they can cause some downtime. Transfer speed will help you understand what this downtime might look like, but even with fast transfer speeds, other security features and measures like vpns or firewalls can slow down the process.

Remote backups are the obvious choice for mobile devices but present some challenges as well. Unfortunately, this alone gives no guarantee that data will stay secure. To mitigate this risk, proper encryption is necessary.

Encryption practices

Always use encryption. Through the encryption process, data is securely protected, and only authorized users have access. Encryption should be a part of local data stored on the mobile device itself, as well as be a part of transferring data across a network.

Nevertheless, encryption is essential to keeping data secure and safe. But, even with encryption policies, end-user training is necessary to mitigate certain risks. With a public wi-fi network, for example, users can connect to an authentic-seeming network and become victims to a man-in-the-middle-style attack. Keeping data secure means training employees on authentication best practices and using extra security measures like virtual private networks (vpns)

Disabling features when not in use

Communication radios, like Bluetooth and wi-fi, play an integral role in the operation of the mobile device but also create a large attack surface for malicious actors. Bluetooth can be victim to all kinds of attacks, including:

- Bluesmacking
- Bluejacking
- Bluesnarfing

Users should disable these features when they are not in use to minimize these risks. Turning off Bluetooth and wi-fi reduces the exposure and limits the time for vulnerabilities to become exploits. Turning off these features will require intentional action from the user, meaning they will have to keep up with it themselves.

You can find tools that help with this process, but at the end of the day, proper training and education helps keep workers on the same page regarding these specific security policies and practices.

IoT (internet of things)

What is IoT and IoT security?

The internet of things is a network of smart devices that connect to each other in order to exchange data via the internet without any human intervention.

The architecture of IOT systems usually consists of wireless networks, cloud databases for communication, sensors, data processing programs, and smart devices that interact closely with each other. IoT systems use the following components to exchange and process data:

- Smart devices that collect, store, and share data about the environment and other devices and components
- Embedded systems used by smart devices — which can include various processors, sensors, and communication hardware — whose goal is to collect, send, and act on data they acquire from environments
- IoT gateways, hubs, or other edge devices that route data between IoT devices and the cloud
- Cloud or on-premises data centres with remote servers that exchange data through wireless connections

IOT technologies are used within various industries: manufacturing, automotive, healthcare, logistics, energy, agriculture, and more. Smart devices can range from simple sensors to DNA analysis hardware depending on a particular IOT system's goals.

The most popular IOT use cases and devices are:

Why does IOT security matter?

Such a wide application of IOT systems requires organizations to pay special attention to system security.

Any vulnerability can lead to a system failure or a hacking attack, which, in turn, can affect hundreds or thousands of people. For instance, traffic lights could stop working, causing road accidents; or a home security system could be turned off by burglars. Since some IOT devices are used for healthcare or human protection, their security can be crucial for people's lives.

Another important reason to prioritize security when developing IOT systems is to keep their data safe. Smart devices gather tons of sensitive data, including personally identifiable information, which is required to be protected by various cybersecurity laws, standards, and regulations. The compromise of such information can result in lawsuits and fines. It can also lead to reputational damage and the loss of customer trust.

Why do we remove local admins rights

The danger of local administrative privileges

Convenience vs. Security

Users enjoy the freedom of having local administrative rights on their workstations. They can add/remove programs, install printers, etc. Without requiring assistance from the IT department. In a small organization with limited IT resources, granting users local admin rights allows IT to focus on more important projects. However, convenience often comes at a cost.

Abusing local admin privileges

If an attacker compromises a user account with local admin privileges, it could spell disaster for an organization. Would you want to give hackers the ability to do any of these things?

- Disable endpoint antivirus
- Install malicious software
- Encrypt data with ransomware
- Move laterally within a network
- Generally, weaponise the system against the organization

Benefits of removing local admin rights

Removing local admin access might not be well received by users. However, doing so provides many benefits to an organization's security posture:

- Lowers risk of malware infections
- Ensures antivirus and other protections remain active
- Reduces an attacker's ability to exploit vulnerabilities

Special circumstances

Most employees do not need local admin access to perform their daily job duties. However, some users may occasionally require higher privileges to complete a task. For these situations, it is recommended to create a separate account with admin-level access. The employee should only use the privileged account when necessary to complete their work.

This has still risk associated and should be handled with serious thought.

Lock it down

Granting users local admin access was a common practice in the past. However, modern security threats require IT professionals to move beyond the mindset of "*this is how we've always done it.*" The risks associated with local admin access far outweigh the benefit of convenience. Local admin access should be removed from users before hackers take advantage of this unsafe, outdated practice.

Default settings on routers and wireless

Secure your home network

You need to make sure your home wireless network is secure, to protect it against unauthorised access or attack. The best place to start is with your router.

When we talk about routers, we are talking about more than one thing. Your home wireless network is made up of three distinct parts — the modem, the router, and the access points.

- The modem is the bridge between your home network and the internet.
- The router is what connects all the devices on your home network and sends traffic in and out. It shields the devices on your home network from view, acting like a single source of traffic for your home.
- The access points allow your devices to connect to the home network wirelessly.

The devices that your internet service provider (ISP) provides to you are all these things in one. Your ISP calls them modems, but most of us refer to them simply as routers. You need to secure your router so people cannot access your home wireless network without your knowledge — or use your wi-fi for free. Here is what you need to do.

Change the default login details for your router

Everything that comes in and goes out of your home wireless network goes through your router. The best place to start when you want to protect it is with the default login details, or 'default credentials'. You use these to log in to the router, to manage how both it and your devices access the internet. These login details give you 'admin access' to the router, and let you define:

- What data can pass through it, and
- What devices have permission to send and receive that data.

When you buy a router, it will come with default login details that are set by the manufacturer. Often, all devices of the same model will have the same default username and password. The username might be something like 'admin', and the password might be 'password'. The router should come with details of what the default login details are. If it does not, or you do not know what they are, you can find a list of default passwords for most routers on the internet.