ZERO TRUST SOLUTIONS

The fundamentals of online safety

The fundamentals of online safety

Since the internet revolutionised the way society uses computers, there have been cyber attacks - and they are still prominent today. According to the UK Government, 39% of UK businesses have identified cyber attacks in the past year.

As a result, you must avoid being a victim of one of these attacks. Take the first step to protecting your online safety by following our tips below.

Install an antivirus on your laptop and mobile

One of the oldest forms of cyber security is antivirus (also known as AV or endpoint security) is still a worthy asset in your online safety armoury.

Most people know they should have an antivirus installed on their laptop, but did you know you should also install it on your **mobile**?

Antivirus software detects threats to your laptop and mobile as they occur and stops them immediately or just after. Often this protection happens without you needing to do anything.

All you have to do is:

1. **Choose an antivirus provider**
2. **Install**
3. **Keep it updated (or ensure it updates itself)**
4. **Make sure it's turned on**

During the last ten years, Microsoft has put a lot of effort into making Windows built-in antivirus one of the best. So, if you're running the latest Windows OS, you can skip steps 1 and 2, unless you prefer a different vendor.

Does it smell phishy? Think before you click

To strengthen your online safety, it is critical to identify phishing attacks. A phishing attack is where an attacker tries to trick you into clicking a link or opening an attachment in an email they've sent you.

Due to the complexity of cyber attacks, phishing attempts can be difficult to detect. But they are also one of the most common methods.

In addition to doing security awareness training, here are some ways to spot phishing attempts in a message:

1. **You don't recognise the sender**
2. **You don't recognise the sender's domain (always check the domain by hovering over the sender's name)**
3. **The email request is unexpected**
4. **It asks you to do something:**
    - click on a link to a domain you don't recognise
    - open an attachment
    - call someone
5. **It is poorly written**
6. **It looks out of the ordinary**
7. **It contains spelling mistakes**
8. **It asks for sensitive information**

Back up your data

If you are the victim of a cyber attack, you will lose a significant amount of crucial data if it's not backed up. According to JustGilbey IT Solutions, data loss is approximately up 400% since 2012. Avoid being part of this and back up your data so it can be recovered if necessary.

A popular way to back up data is using an external hard drive or SSD. However, as attackers can sometimes access the storage if it's connected to your computer, you should make sure your external hard drive or SSD is not permanently attached to it.

Another common way of backing up data is using a secure cloud backup, which is often more convenient than physical storage. It may seem odd that storing data using the internet is safe, but secure cloud backups store data using thousands of centres, so it is secure.

We also recommend encrypting backups locally to keep your cloud backups secure. In addition, use different keys per file for the best protection. By doing this before uploading to a secure cloud, you can prevent leaks and even compromises of the cloud provider.

There are many secure backup tools to help with this. Reach out to us if you would like help finding one.

Follow safe internet browsing practices

In addition to spotting potential phishing attacks, watch out for malicious websites. Good rules to follow are:

1. **Only visit websites by first searching for a company you know in a search engine**
2. **Only click links that start with 'HTTPS' in the URL as the information sent to you and received by the website is encrypted so that others cannot see it**
3. **Never share your personal information if you can avoid it. You can use fake names, fake date of birth, or an email account you only use for non-important matters**

Use strong passwords, means using long passwords

We've all heard that passwords should be 'hard' or 'strong', but do you know what that really means? Although you probably know what humans can predict, you likely can't say the same for computers.

Computers are good at repetitive processing. Attackers can give them lists of passwords from billions of real passwords generated by humans to try - and if a company is hacked, these passwords can be leaked.

The hackers try to predict small changes (called mutations) in the passwords. This means they can predict more passwords based on the leaked passwords. If you simply change an old password only slightly to create a new one, they can probably guess it.

To be 'unpredictable' for a computer, you should:

- **Never repeat passwords** you're using somewhere else or have used before
- Never change just a few characters to create a new password, or increment an existing password by 1
- **Don't include sensitive information** or information that is easily guessable about you – e.g., birthday dates, family names, pet names, or any other personal information that could be easily guessable, or researchable.
- **Never use common/easy-to-guess passwords** - if it's been leaked before, it's one of the first things the attacker tries. Analysis from the National Cyber Security Centre (NCSC) showed that 23.2 victim accounts used '123456' as their password.

So, those are all the do's and don'ts. But how can you make a strong password? Your password must be long and substantially different from anything you've used before.

Why is length important?

Password cracking attacks work by trying many combinations. So, it's just a chance whether they stumble upon the correct password or not. The Security Factory reports that for $25 an hour, an attacker can make **632 billion password guesses per second.** This means that if your password contains upper case, lower case, numbers and characters, they could crack a 5-character password instantly, a 6-character password in just 20 seconds, or or an 8-character password in just five days.

We recommend you use at least 16 characters. That would mean if the attacker invested $25 an hour in cracking your password, it would take them 4 quadrillion years. And, even if they spend a lot more trying to find your password, it will still likely take them thousands of years.

Never use the same password twice

Use different passwords for different websites, services, or even multiple accounts on the same website. The more passwords you have, the fewer chances the attacker has at breaking into other accounts you have if they do find a password that was breached. By using different passwords, you can limit what data they can access and lessen the severity of an attack.

So, the best password is one that is: easy for you to remember (write it down on paper somewhere safe if you can't) but hard for the attackers to guess.

Remember:

1. **Don't use personal information or information that's easily guessable**
2. **Make it at least 16 characters**
3. **Make it very different from any previous password you have used**
4. **Don't reuse it. Create a new password for every account and don't reuse the same password for different accounts and services.**

Use a password manager

Computers are good at breaking passwords but are also **good at creating passwords**. This makes them great for generating strong passwords for you that are unique every time and much longer than 16 characters.

The tool you need for this is called a password manager. The password manager is a plugin on your phone and/or browser that:

- Generates new, long passwords for you each time you sign up for a new account or service
- Stores them securely
- Automatically fills them in when you need them, so you don't need to remember them

Then, all you need to do is create one long strong password that you use to get into the password manager. For this, ZTS recommend you use a physical security key. Contact us to get one for you or your company.

Use multi-factor authentication (MFA)

Even with strong passwords that follow all the above rules, you must assume your passwords will be breached. It will happen on one or two of your services each year, and your password will be publically available to hackers.

Using multi-factor authentication will prevent an attacker from using your real password even if it is leaked. So keep MFA turned on (read more about MFA in our Insights blog here). As a result, the attacker needs more than just the password to gain access to your account. This could be something else you know or something that you have, such as a:

- Physical security key
- Employee ID card
- Mobile phone
- Your biometrics

Multi-factor authentication typically involves the user entering a password and then entering a one-time code (typically emailed or texted) to gain access. There are now even easier methods, such as using your fingerprint or clicking a one-time link emailed to you or pop-up push notifications on your phone.

After logging in to any major modern service, you can set up multi-factor authentication (MFA). Always turn this on if you have the option. At the very least, it is a must on the most sensitive services you subscribe to e.g., banks, insurance companies and social media.

These all mean that as a result, even if an attacker has your password, they will still struggle to gain access. However, if your password is leaked, you should still change it as soon as possible.

Get in touch with us if you need help building an MFA solution for your company.

Update your software and apps when prompted

Update your software and apps when they are ready since they will likely include patches that help keep them performing at their optimal level. More importantly, however, they improve their security. When software is not updated, it becomes more vulnerable to malware attacks.

Some software packages allow you to update it automatically. Make sure you enable this if it gives you the option.

Key things to remember

Securing your online safety may seem complicated, but it only requires a simple solution: **training.** By making yourself aware of the points above and putting them into practice, you will drastically **minimise the risk of being a victim** of a cyber attack.

If you want to keep yourself up to date with continual security awareness training or test out your existing skills to protect yourself, reach out to us today.