CYBER SECURITY TIPS
THE BIG 7

The threat of theft of your data, money and identity has never been higher. The 'bad guys' are targeting people and businesses more effectively and in increasingly ingenious ways. That means that you will never be entirely secure. But by following these rules you can avoid 90% of problems:

1. Back up anything you don't want to lose

If you have photos, videos, documents, emails, spread sheets, contacts, calendars that you don't want to lose then make sure you know where they are and get them backed up somewhere safe. To get you started try these links to articles on backing up iOS devices, Android devices, Windows PCs and Apple Macs.

2. Install security software

All your devices need to be protected from malware and viruses. If you don't already have some security software, then look at the AV Test website for up to date, independent reviews. Get the software installed and make sure that you keep it up to date.

3. Keep your devices up to date

The latest version of your software is the most secure. Keep an eye out for updates and apply them when prompted. If you have software that you don't need then remove it from your device. AND don't download apps or application unless you are happy they are legitimate. If in doubt look them up on Google before installing.

4. Make your passwords secure

Make sure you are using strong passwords. See this advice from the government for an easy way to make them secure and memorable. You should have different passwords for each site, change them regularly and never share them with others. Sounds like a nightmare, right? Password management software such as LastPass can make your life a lot easier.

5. Be suspicious

I know it's daunting but you are the first line of defence. So be suspicious of anything that looks unfamiliar. Take a close look at emails with attachments or links before clicking. Whenever something is free, be wary. Once you've clicked on an untrusted link there are two possible outcomes. At best, you'll have to watch an advert, or give away your email address. At worst, you will be at risk from identity theft or ransomware.

6. Don't give out personal information

The more the bad guys know about you the easier it is for them to scam you. Key pieces of information include your full name, contact details, date of birth, mother's maiden name, national insurance number and, of course, financial information. Guard your personal information and be wary whenever you are asked for it.

7. Get educated

Learning more about cyber security will help reduce the chance of unhappy outcomes. Understanding how you can be attacked will help you avoid a scam. Knowing how to react if you've been compromised will reduce the impact. Start at the Get Safe Online website.

Microsoft Partner
Silver Midmarket Solution Provider
Silver Small and Midmarket Cloud Solutions

Download your copy from here:
evolvecom.co/security

CYBER SECURITY TIPS
7 MORE

If you are already following the Big 7 Rules of Cyber Security and want more tips for improving your security, look no further.

1. Don't use someone else's computer

Avoid Internet café computers (yes they still exist), but also the devices of your friends and family. Despite the owner's assurances they don't know whether their device is secure. Once you have typed your password into an unprotected device you will never know whether it has been logged and sent off to a bad guy

2. Put a password, passcode or PIN lock on all mobile devices

A golden rule and although I feel that I shouldn't need to tell people this I am still surprised to find that people switch this feature off. The password or PIN lock is the only defence you have if your mobile device is lost.

3. Don't use personal stuff at work

You don't want to be the employee that caused the system breach at work. It's embarrassing but that's not the half of it. It's also a threat to your job. Familiarise yourself with your company's computer policy. Even then, however, avoid using your personal email, social media, USB sticks or mobile devices on the business network.

4. Encrypt your data

Even with a strong password it is possible for someone with physical access on your device to get your data. A phone thief can connect your stolen mobile to their computer and access all your files. Encryption prevents this by scrambling your data so that no one can read it unless they have the encryption key. On Windows it's called BitLocker. On a Mac it's called FileVault. On iOS it is enabled with a passcode. Android devices can be a bit complicated but a useful guide can be found here.

5. Subscribe to identity protection

Usually by the time you become aware that you are the victim of identity theft it is too late. When it comes to preventing it you need help. Experian operate a credit monitoring service; and banks and credit card companies bundle protection with their products.

6. Use multifactor authentication

Also known as two-factor authentication, this combines your usual log in details with 'something you have' such as a mobile phone, a security key or your fingerprint. If someone manages to steal or guess your password, they still won't be able to log in. More and more websites offer this as an option and we'd recommend switching it on for all your key accounts – banking, email and social media.

7. Guard your Wi-Fi

When you are on the go there are lots of opportunities to connect to the Internet using the Wi-Fi provided by trains, hotels, coffee shops and airports. Although tempting it is usually safer to use your phone as a hotspot and tether your device. If you have to use these free networks, then remember the following:

- If there is no password, then the Wi-Fi network is not secure. Disconnect immediately
- Double check the Wi-Fi name with the establishment
- It is preferable to choose the Wi-Fi network manually. Switch off auto-connect

Download your copy from here:
evolvecom.co/security