

12 Top Tips for Building Cyber Resilience at Home

12 Top Tips for BUILDING CYBER RESILIENCE AT HOME

WHAT IS 'CYBER RESILIENCE'?
Cyber resilience focuses on three key areas: reducing the likelihood of a cyber attack, limiting damage to your accounts, devices or data; reducing the potential impact of a cyber incident; and ensuring the recovery from a cyber attack occurs, should an attack not happen at all.

- 1. PASSWORDS LONGER AND LESS PREDICTABLE**
The longer, less consistent and more difficult to guess your password is, the better. Use a mix of upper and lower case letters, numbers, symbols and punctuation. Avoid using common words, phrases or predictable patterns.
- 2. AVOID RE-USING PASSWORDS**
When you use the same password across multiple accounts, a cyber criminal only needs to guess one password to gain access to all your accounts.
- 3. USE A PASSWORD MANAGER**
A password manager is a secure online or offline tool that stores your passwords for you. It generates strong, unique passwords for each account and updates them for you.
- 4. BACK UP YOUR DATA**
Using a copy of your data using a secure method (cloud or external storage) is a good way to ensure your data is safe. It's also a good idea to test your backup regularly to ensure it works.
- 5. ENABLE MULTI-FACTOR AUTHENTICATION (MFA)**
Multi-factor authentication is a security process that requires you to provide two or more pieces of evidence to verify your identity. This could be a password and a code sent to your mobile phone.
- 6. CHOOSE RECOVERY QUESTIONS WISELY**
Recovery questions are used to help you regain access to your account if you forget your password. Choose questions that are not easily guessable and that you can answer easily.
- 7. SET UP SECONDARY ACCOUNTS**
Having a secondary account for your most important data can help you recover your data if your primary account is compromised.
- 8. KEEP HAVING FUN WITH TECH**
Staying up to date with the latest technology can help you stay secure. Regular updates to your devices and software are essential.
- 9. CHECK FOR BREACHES**
If you suspect your account has been compromised, check for breaches. You can do this by using a password checker or by contacting your service provider.
- 10. CHANGE DEFAULT IOT PASSWORDS**
Many IoT devices come with default passwords. Change these to something unique and secure.
- 11. KEEP HOME DEVICES UPDATED**
Regular updates to your home devices (TVs, smart fridges, etc.) can help protect them from vulnerabilities.
- 12. STAY SCEPTICAL**
Be wary of unsolicited emails, messages or offers. If something seems too good to be true, it probably is. Don't click on links or download attachments from unknown sources.

Meet Our Expert
NOS is supported by the National Cyber Security Centre (NCSC) and the National Crime Agency (NCA). We work with experts from these organisations to ensure our advice is up to date and effective.

National Online Safety®
#WakeUpWednesday

www.nationalonlinesafety.com | @nationalonlinesafety

Most of us habitually check our doors are locked each night. We don't leave our cars open with the keys in the ignition. We take care not to let anyone watch us enter our PIN at the cash machine. When it comes to cyber-security, however, many people aren't anywhere near as routinely cautious – which is one of the reasons that online crime continues to pose a major threat.

The UK had the largest percentage of cyber-crime victims per million internet users in 2022; the US had the second-highest ratio. Nations with (relatively) wealthy populations who spent a lot of time online are, therefore, lucrative hunting grounds for cyber criminals. Our #WakeUpWednesday guide this week has useful tips to help you avoid joining the growing number of victims.

In 2001, an average of six people an hour had an online account compromised. Now, the average is 97 every hour. The pandemic undeniably added to this level of risk, as work and education went remote and cyber criminals sensed an opportunity. More recently, Russia's invasion of Ukraine has accelerated the growth of cyber threats, with both sides carrying out online attacks.

The irony is that many of these incursions are facilitated by devices designed to make our lives easier. Smart home appliances, wearable tech, streaming services ... virtually any internet-enabled device is a potential entry point for a competent cyber-criminal. Check out the tips in our #WakeUpWednesday guide to see if your home is as cyber-secure as it could be.

Please [click here](#) to download the guide