12 Top Tips for BUILDING CYBER RESILIENCE AT HOME

As a society, we’re increasingly using technology and tech services in the home. Digital assistants which can adjust the heating or turn lights on and off, streaming services for shows and movies on demand; games consoles; smart speakers; phones; laptops... the list goes on. As we introduce each new gizmo to our homes, however, we increase the level of threat from cyber criminals. It’s essential, therefore, that we learn to become more cyber resilient in relation to the devices and digital services that the people in our household use.

WHAT IS ‘CYBER RESILIENCE?’
Cyber resilience focuses on three key areas: reducing the likelihood of a cyber attack gaining access to our accounts, devices or data; reducing the potential impact of a cyber incident; and making the recovery from a cyber attack easier, should we ever fall victim to one.

1. PASSWORDS: LONGER AND LESS PREDICTABLE
The longer, less common and unpredictable a password is, the more difficult it becomes for cyber criminals to crack. The National Cyber Security Centre’s ‘three random words’ guidelines are ideal for creating a long password which is easy to remember but hard to guess.

2. AVOID RE-USING PASSWORDS
When you use the same password across different logins, your cyber resilience is only as strong as the security of the weakest site or service you’ve signed up for. If cyber criminals gain access to your username and password for one site or service, they’ll definitely try them on another.

3. USE A PASSWORD MANAGER
A good way to juggle different passwords for every site or service you use is to use a password manager. This software stores all your passwords for you, so you simply need to remember the master password. LastPass, Dashlane, password keeper are all excellent password managers.

4. BACK UP YOUR DATA
Keep a copy of your data using OneDrive, Google Drive or another reputable cloud-based storage solution. If it’s extremely important or sensitive information, you could even decide to keep more than one ‘back-up version’ – say, saving it to a removable USB drive or similar device, for example.

5. ENABLE MULTI-FACTOR AUTHENTICATION (MFA)
Multi-factor authentication is where you need access to your phone (to receive a code, for example) or another source to confirm your identity. This makes it far more difficult for cyber criminals to gain entry to your accounts and your data, even if they do manage to get your username and password.

6. CHOOSE RECOVERY QUESTIONS WISELY
Some services let you set ‘recovery questions’ – such as your birthplace or pet’s name – in case you forget your password. Take care not to use information you might have mentioned (or are likely to in future) on social media. More unpredictable answers make cyber criminals’ task far harder.

7. SET UP SECONDARY ACCOUNTS
Some services provide the facility to add secondary accounts, phone numbers, and so on to help with potentially recovering your account. Make sure you set these up: they will be vital if you’re hacked (or vulnerable to hacking) or if you’re trying to take back control of your account after a cyber attack.

8. KEEP HAVING FUN WITH TECH
Consider our tips in relation to the gadgets and online services your household uses: protect yourself and your family, and don’t let the bad guys win: devices are not only essential to modern life but also a lot of fun – so as long as you keep safety and security in mind, don’t stop enjoying your tech.

Meet Our Expert
Gary Hendron is the Director of IT at a large boarding school in the UK, helping pupils to adapt to a digital world and the online world. With a passion for risk, digital citizenship and cyber security, he believes in ensuring that pupils and children alike become more aware of the risks associated with technology as well as the many benefits.


#NationalOnlineSafety
#WakeUpWednesday