

Online Safety

Building Cyber Resilience at Home

Online safety is everyone's responsibility.

According to National Online Safety, we need to build cyber resilience at home. They draw upon the analogy that most of us habitually check our doors are locked each night, we do not leave our cars open or with the keys in the ignition, we take care not to let anyone watch us enter our PIN at the cash machine. Yet when it comes to cyber security, people are not anywhere as routinely cautious resulting in online crime posing a major threat.

Statistically, UK had the largest percentage of cyber-crime victims per million internet users in 2022. Further statistics show that in 2001, an average of six people an hour had an online account compromised with the average now of 97, which is a staggering increase. Most of these incursions are facilitated by devices designed to make our lives easier: smart home appliances, wearable tech, streaming services and virtually any internet-enabled device is a potential entry point.

These smart devices that many of us now use as standard are simply a convenient back door into our lives. Be aware of the potential risks and how you can protect yourselves and your children.

This week's guide, see below, are 12 top tips for building cyber-resilience at home.

What is cyber-resilience?

1. Reducing the likelihood of a cyber attack gaining access to accounts, devices or data
2. Reducing the potential impact of a cyber incident
3. Making the recovery from a cyber attack easier should we ever fall victim to one.

Please take note of what your parental responsibility is to ensure that your child is safer online.



Working together to keep our children safe and happy online.