IT 365
NEWS BITES AND INSIGHTS

How to protect your business data from children and hackers

It can take a while to build a strong business or organisation. But all that hard work can be threatened by just one click or tap by a child.

In just a moment someone using a tablet or computer to download something that looks cool, exciting or simply useful. That download could be carrying something much more sinister, like a virus, that opens the way for a hacker to raid corporate data, or that locks you out of that data and demands a ransom.

Sadly, this is a real problem afflicting many organisations, large and small, across the country. Everyone, from home-based sole trader to global multinational, faces the same threat.

And it's about to get worse, because the school holidays are approaching.

Kids can be the cybercriminal's best friend

Parents have a love/hate relationship with tablets and smartphones. On the one hand they provide an easy way to keep the kids entertained, particularly when you're out and about. But when they're connected to the internet, as they increasingly are, this convenience is offset by the risks of encountering something unpleasant.

While many parents might worry about how the internet could endanger their children, they could well be overlooking an equally important concern: the danger to their device and the data it connects to.

Creeping digital connectivity means that a growing number of our digital devices communicate with many areas of our life, including the workplace. Is that smartphone or laptop your child is using connected to data used in the business you run or work for?

Cybercriminals are looking for the easiest routes into data and financial information – whether to steal it or to lock you out of it for a ransom. Our kids could unwittingly help them to unlock that route. All it takes is to entice them into making a single click or tap.

This threat isn't theoretical. There is no shortage of school-gate stories about children inadvertently bringing a virus to their home computers. A quick look at discussions about tablet use in the home on parenting forums reveals tales of children using workplace devices for play.

Practical cybersecurity tips for parents

Here are our thoughts on helping keep not only your children safe from digital dangers, but also protecting your personal and business data.

1. Don't let children use devices that could give access to commercial data. This really is the safest option. Using computers supplied by your employer may be cheaper and more convenient than having another for personal use, but if it becomes infected with malware, it can quickly give you a very expensive, very inconvenient problem to solve.

2. Use antivirus software and keep it up to date. This is basic good practice.

3. Don't rely on that antivirus software to protect you from every threat – use your common sense. Cybercriminals are increasingly trying to manipulate us into agreeing to download nasties through phishing attacks and the like.

4. Learn how to use the parental control options on your device. These vary between operating systems and again, they're not foolproof.

5. Talk with your children about how they use the device and the internet. Make it a conversation, not a lecture. Learning about what they like to do will help you direct the conversation to safe practices.

6. Encourage children to ask you before downloading anything and help them understand the importance of downloading from trusted sites. Older children can be tempted into illegal downloads of music, videos and games, which are prime carriers for viruses.

7. Having a dialogue with your kids about their internet use should mean they're more willing to talk with you when there's a problem.

8. Talk about how other people have run into problems using the internet. Sharing stories and discussing how issues can be avoided will help you and your children learn from the mistakes of others.

Protect your data by talking to us

While you can help your children manage their internet use, you have less control over how other members of your team use their devices.

It pays to have a cybersecurity strategy in place that offers maximum protection and can help you out of a hole should the worst happen.

The costs of a malware incident can mount up. One recent attack described in the media on a hairdressing business involved a ransom of £1,000. This was paid, but not all the data was recovered and the business owner estimated the cost of the entire episode to be around £20,000.

As specialists in supporting IT networks for businesses across the UK and further afield, part of our role is to help keep networks and data secure. We keep ourselves up to date with current best practice, so we're well placed to advise our clients on the latest trends in cybercrime.

If you would like to know more about protecting your critical business systems and data, give us a call on 0808 168 9135 or email enquiries@itsupport365.co.uk. We would be pleased to have a no-obligation conversation with you.

Alternatively, you can follow us as we share news on Twitter, Facebook or LinkedIn.

The holidays are meant to be a time of freedom and fun for our children. Adding in common sense and good practice can help you enjoy the break with peace of mind, while at the same time frustrating the cybercriminals.