STEVEN FURNELL *Professor of Cyber Security, University of Nottingham*
www.nottingham.ac.uk/computerscience/people/steven.furnell

With over 25 years of experience in cyber security, Steve is internationally recognised in the field and has research interests including security management, awareness and culture, usable security technologies, and cybercrime. He has authored over 340 published papers, plus numerous books and book chapters, chairs Technical Committee 11 (security and privacy) within the International Federation for Information Processing, and is a board member of the Chartered Institute of Information Security.

TIP 1. APPRECIATE YOUR ASSETS AND RECOGNISE YOUR RISKS

You need to understand the systems and data that your business depends upon, and the impacts that would result if they were to be involved in a breach. Performing even a basic risk assessment will help to guide security activities and investment in a more targeted way.

TIP 2. IT REALLY COULD HAPPEN TO YOU

Many cyber threats are indiscriminate, and so there's no basis to assume that they won't happen to your business. There are also various breaches that can occur from accidental incidents and other unforeseen causes. Remember that it's not all about an attacker picking you out and targeting you; attacks can happen simply by having systems online with exploitable vulnerabilities.

TIP 3. UNDERSTAND THE BREADTH OF CYBER SECURITY

Don't fall into the trap of seeing cyber security as a technical issue that can be left to the IT people. It's a business issue and needs to be understood accordingly. There needs to be a holistic view of the people, process and procedural aspects alongside the inevitable need to address the technology elements.

TIP 4. PREVENTION IS BETTER THAN CURE

The cost of protection is likely to be less than the cost of handling a significant incident. Cyber security is an insurance against the threats that are undeniably out there and causing problems for others. Thinking about things in advance, having plans in place, and knowing where to turn for support will all be invaluable to make things easier if the worst still happens.

TIP 5. BEGIN WITH THE BASICS

There are a variety of standard protection measures, such as using anti-malware protection, performing backups, installing software updates, and selecting strong passwords, all of which get regularly mentioned in security guidance. There is of course a good reason for this, and it's important to establish a solid foundation.

TIP 6. DEFEND THE DIVERSITY OF DEVICES

Your organisation is likely to be using a range of devices, which in turn will have access to your network, systems and data. Today's threats extend well beyond traditional PCs, and we need to consider smartphones, tablets and various other smart/connected devices that may be in use in the business and by your employees.

TIP 7. EMPOWER YOUR PEOPLE

It's important to help staff to understand their role and responsibilities in protecting the business, ensuring that they are aware of the threats they may encounter and that they have a suitable level of cyber security literacy to respond. And remember to reinforce and refresh the messages on a regular basis, because people will forget or assume that problems have passed.

TIP 8. IT'S NOT JUST ABOUT YOU

Effective protection depends upon more than just your own actions, as those you partner with could also bring problems to your door. As such, it's important to understand security in the supply chain (from the perspective of any partners that supply you, as well as anyone you supply), with appropriate recognition and expectations laid out within contracts and service agreements.

TIP 9. IF YOU'RE UNSURE OR DON'T KNOW, SEEK HELP

It's quite reasonable to feel confused or unclear about what to do, or to need further assistance if something goes wrong. There are various sources of further advice, from service providers, security practitioners and professional bodies. Some will cost money, but there is also an abundance of free resources, and there may also be tailored support for specific business sectors.

TIP 10. DON'T PANIC

Addressing your security needs may appear daunting to begin with, but it's a journey and it gets easier. Be ready to recognise that some things will be high priority to address as soon as possible, but equally that it won't all be done instantly and the overall process will take time, and should become part of your 'business as usual' operations.