Cybersecurity for SMEs

A record 657,790 new businesses were formed in the UK in 2016, and if you've taken the decision to go it alone, it's an exciting time. You're probably looking forward to getting your first customers, your first premises and hopefully your first employees. But in all the excitement and planning, have you considered cybersecurity? With so much to think about, there's a good chance that it has fallen through the cracks. So, we've put together this quick guide to cybersecurity for SMEs, including everything from encryption, to VPNs, to passwords, and updates.

Whether you're a tech company developing an app, a freelance designer or an entrepreneur. Everyone is a target for cybercriminals and it's essential that cybersecurity measures are put in place to protect yourself, your fledgling organisation and your customers.

Cybersecurity can seem daunting at first, especially if it's an unfamiliar area. But there are some simple measures you can take to improving your security posture.

Here are four tips to improving your cybersecurity, as a start-up or SME.

Encrypt your data and protect your intellectual property

Do you have a business idea that's set to change the world? What would happen if a competitor or a malicious threat actor gained access to it? It could be the end. Therefore you need to protect it at all costs.

It may be a business idea, a new product or process, or a blossoming client list. Whatever it is, you need to ensure it's secure and that you've put robust security measures in place around it. Passwords, firewalls, access privilege rights, segregated networks; these can all help ensure your secrets remain just that.

Data encryption is also key, both in transit and at rest. By encrypting your key data it means that, if the worst was to happen, the data extracted by hackers would be useless.

HTTPS and VPN

Many startups and freelancers use shared work spaces, or work from coffee shops to make use of the facilities, especially the Wi-Fi. But how do you know if your connection is truly secure?

Ensuring connection via HTTPS is one way and many browsers will now alert you to the fact that a site may be insecure. If not, you need to look out for the green secure padlock in the url address bar. The same applies to mobile sites too.

You also need to be wary of evil twin attacks; this is where an attacker can mimic a legitimate wi-fi, say from a coffee shop or an office, and once a victim connects they can alter traffic to collect personal details. They could even set up an official-looking login page on entry, to try and con users into sharing their login credentials. If you do spot a number of similarly named wi-fi networks, you need to alert whoever looks in charge.

Finally, utilise a Virtual Private Network (VPN) such as TunnelBear or Windscribe. By doing so you add a layer of encryption to your connection and prevent attackers from being able to access your information.

Password management

Using the same password and email address across many different websites isn't a great idea: if one channel was to be breached, attackers could use the information gathered to access further accounts, as well as your business network.

This is especially true if you are using the same passwords for your work or personal computer, as attackers with stolen login credentials could access personal files as well as any critical business files you may have.

Strong passwords are essential and you should ideally have individual passwords for each account you set up. A password manager such as LastPass or Dashlane can help keep track of these for you. Of course, this may not be practical for all accounts, but you need to ensure you are protecting your most critical logins at the very least.

If still insist on using the same password across sites, please keep an eye out for any news of a potential breach and check your information has not been compromised with a service such as haveibeenpwned.

Update regularly

Nobody likes updating their software: it takes valuable time away from other, more pressing work and it's always tempting to hit the remind me later button. But by putting off updates you become increasingly vulnerable to attack.

This is because new updates carry with them vital security patches, allowing you to stay protected against the latest and most serious threats. Cyber-criminals are fully aware of this, and once an update is released they are becoming increasingly adept at reverse engineering the updates, finding the vulnerabilities and launching attacks against those who have yet to update their systems.

What used to take months in terms of this reverse engineering process now takes days, and the time from update to attack is getting shorter all the time. We no longer live in a world where you can put security updates off.

Stay secure with Secarma

We're here to support your security improvement efforts, and to help you protect your fledgling business. As well as our full range of penetration testing services, we also offer a simple but effective half-day consultation – which takes place on-site at your premises. During the consultation our experienced security professionals will work with you to understand the security challenges you face, and help you take a fresh look at your current security posture from the perspective of a hacker.

To find out more about our half day consultation, or to find out more about our security services please visit our website.