GET CYBER SAVVY

The essential 6 point checklist for SME's

1

Create A Short Data Protection Policy And Communicate To Your Staff

Document and implement a short data protection policy. This is an essential step for minimising your business' risk of cyber-attack or data breach. It doesn't have to be a lengthy document, just the key points simply written and communicated to your staff, making them aware of your practices and policies. As a result they will be more vigilant to identifying and reporting potential attacks.

Remember not all data-breaches are malicious external hacking attacks. There are many statistics showing how the majority of mishaps are caused accidentally by employees.

2

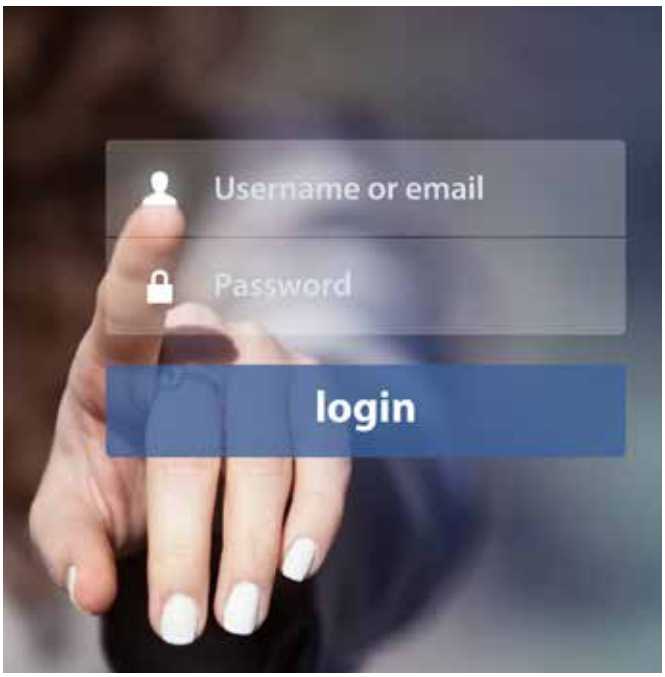
Stay Vigilant!

Once you've documented your policy and shared it with your staff, encourage them to stay vigilant. This will add a vital layer of protection to protecting your business privacy. Consider them your 'first and last line of defence' to prevent issues before they happen. Show them what to look out for, and make it easy for them to communicate any suspicious activity to you.

3

Implement A Simple Password Management System

Passwords are a fundamental way to protect your company data. They're also one of the easiest best practices for your staff to follow. Give guidance to your staff on how to generate strong and unique passwords that are not used anywhere else. Define a policy whereby passwords created are always unique, of a minimum length, and contain a mixture of uppercase letters, lowercase letters, numbers and symbols. Password storage goes hand in hand, but is often overlooked. Make sure you have a secure place for your staff to store these complex passwords. Created correctly, these passwords will not be memorable, so make sure there is safe place to store them. (i.e. Not written on a sticky note attached to a monitor).



The final piece in the puzzle when it comes to successful password management is to ensure that passwords are regularly updated. Two to three times a year is sufficient, or if you suspect that something has been compromised.

4

Device & Data Management (Including BYOD Policy)

Controlling access to your business data, through company and personal devices is a crucial step in protecting your business privacy. Most employees will bring at least one personal device to work. These range from personal Laptops used for company business, to personal mobile phones used on breaks for social messaging. Ensure you are aware of what business data your employee has access to, what they can share, and who they can share it with. A simple 'BYOD' (Bring Your Own Device) policy will add this vital control to your business.

Provide a simple way for your staff to tell you if a device is lost, stolen or compromised. There are often way to destroy data remotely should this be the case, but the key is to report it quickly.

5

Control Social Messaging For Business Use & Apply Privacy Settings

Social Media and Social Messaging has become a convenient way for businesses to communicate and enhance day-to-day processes. Unfortunately it brings a range of vulnerabilities, so you need to define a simple policy for how and when your staff can use these tools for company business. Every time a member of your staff conducts activity online its leaving a digital trail of information that can be used for phishing attacks or other malicious intent on your business data.

Educate your team on how to be vigilant, and specifically how to apply privacy settings when using LinkedIn, Facebook, Twitter, WhatsApp, Google + or similar social sites.

6

Don’t Use Open Email / Cloud Accounts To Share Data

Don’t use open / unencrypted Email or Cloud Accounts as a method for transferring or sharing your company data. Implement a simple system for Secure File transfers. Such systems will protect your data, files and attachments shared inside or outside of your business. They are relatively low cost, and work by encrypting all of your company contacts, content and data, thus making your information useless to hackers, or authorised parties.

Protect Your Business Data With Siccura

Sponsored by:

siccura
Private & Secure Digital Life

www.siccura.com