DRAGON

Cyber Security: 10 top tips for small businesses

Keeping your company data and that of your customers' secure is a top priority for businesses.

It's also a legal requirement, with the arrival of GDPR bringing strict new rules for how certain data must be held and processed.

With stats showing 10,000 attacks are aimed at small businesses every day, having secure and robust IT systems and processes in place, and staying on top of your cyber essentials, is a vital first defence.

Here are 10 ways you can improve your cyber security today:

Protect your Internet connection with a firewall

The internet is a core tool for most businesses, but it can also be a weak spot when it comes to a company's cyber security. Using a firewall ensures that whatever information you access online is processed through a third-party buffer. A firewall can also analyse all incoming email traffic, preventing anything from getting through that looks suspicious and may pose a threat.

Check your security settings

It's common for companies to issue smartphones to their employees but these devices can allow hackers to harvest data. Check the security settings on all business-issued devices to ensure the highest levels of protection is in place and turn off any data sharing functions that may make it possible for third parties to connect to a device.

Use a password manager tool

Many of us are guilty of using the same password across multiple accounts and only changing these when prompted to do so. This is partly because it's difficult to remember a different password for all the different sites and applications we now use in the course of our daily lives. A password management tool can securely store and remember all your passwords for you, so you can use ones that are long and complex. You then only need to remember the one password needed to login to the manager.

Secure important data using two-factor authentication

To keep highly sensitive data safe, and to protect your company bank accounts and administration access, you should consider using two-factor authentication (2FA). This type of technology issues an email or text to a registered device that is connected to the account being accessed. It's an extra layer of security that can help prevent unauthorised access.

Limit who can access your data servers

Sometimes the threat to your security can come from within your organisation. One way to mitigate this risk is by limiting who can access any sensitive information your business might be holding. You can do this by making specific locations on your network or hard drive permission-only, which prevents unauthorised employees from accessing valuable data.

Only download applications from official sources

Installing software from an unofficial source can seriously compromise the integrity of your devices. To get around this, only install apps and software from approved manufacturers and through their official channels. This will reduce the risk of your device becoming infected by malware – which you may not even know is there!

Restrict administrative access

Not everyone in your organisation will need an account that allows full administrative access. Check the status of your accounts and ensure that everyone, with the exception of your approved IT administrator, is using a standard account. That way, if the worse does occur and an employee's account is hacked, the damage is more easily contained.

Install anti-malware software

Most companies know to have anti-virus and anti-malware software installed. Check your settings to make sure it is switched on and updated regularly. If you don't have malware protection, then get some quick! Malware is a serious threat to your cyber security. In extreme cases, a hacker may be able to lock you out of your own devices and then demand a ransom for reinstating access

Keep your software up to date

Being promoted to update your apps or software isn't just so you can access the latest features. Often a software update is a development patch to counter known security vulnerabilities, so it's vital you update your operating system and apps as soon as new versions are released, to prevent a potential breach in your cyber security

Never open a link if it seems suspicious

Phishing emails (impersonating legitimate companies to access information) is a popular and effective method for cyber criminals. It can be used to harvest passwords or accounts information, or to access a system or spread viruses. If you don't trust the origin of the email, don't open it. A virus on just one networked computer can infect every device it's connected with. Make sure staff are trained regularly on cyber awareness, so they understand the scale of the threat, what to look out for and what to do if they see something suspicious.

Bonus tip – Think about the third parties you are working with

Another area of weakness being exploited by cybercriminals is the third parties who may not have systems and processes that are as strong as the company they are supporting. Always ask suppliers and third parties you are working with, what they are doing - not only cybersecurity, but in relation to GDPR.

About Dragon IS

Dragon IS, based in Milton Keynes, is an IT support company and cyber essentials certified supplier. Established over a decade ago, we specialise in working with small and medium sized businesses.

For more advice, please contact:

Lionel Naidoo
CEO
Dragon Information Systems
lionel@dragon-is.com

01908 613 080

For proven, trusted IT systems support to keep your business trading profitably