Cybersecurity Fundamentals

Here is your critical checklist of do’s and don’ts when it comes to keeping your small business safe from unwanted cyber attacks, hacks and human threats!

□ **No unknown downloads.** Make a rule against downloading files from unknown senders.

□ **Check your Firewalls.** Make sure everything is up-to-date on all machines.

□ **Use current virus protection on all devices.** Keep it current and updated whenever new patches become available.

□ **Insist upon strong passwords.** Weak passwords are like an open door to your business.

□ **Update your operating system regularly.** This is especially important when new security patches come out. Many computers do this automatically, but make sure you have the auto update function turned on so you don't miss out.

□ **Use a virtual private network (VPN).** These connect you to the web with an encrypted connection so data being shared online can't be seen by third parties. VPN providers offer secure data connections between remote workers and your network too, which can be especially helpful if you send workers into the field (for deliveries or repairs, for example).

□ **MFA/2FA.** Enable multi or two factor identification on all devices and accounts where it is offered. Help can be found **here**.

□ **Make sure mobile devices used for work are secure.** Don't store important passwords on any mobile device. Learn how to use remote wipe capability on your phones and tablets.

□ **Disaster recovery plan**. Not having a plan is a disaster. By thinking through the critical elements of your business that could be compromised, and what the damage may be, you can apply the fixes and antidotes before anything happens - and have a plan of attack when it does.

□ **NDB (notifiable data breach).** Never send sensitive data unencrypted and unsecured, not just end to end via email, but physically controlling who has access to the data/file. A document containing personally identifiable data or medical records for example should be transmitted via a password protected PDF (for example) as a minimum.

□ **People are flawed.** Yes, even you. So don't assume everyone is doing the right thing, and be actively alert and across your staff, their actions and all elements of your business and give them adequate security training.

□ **Outsource overwhelm.** All too hard? There are plenty of companies and consultants who will happily come in, audit your business and provide solutions. Whether it is your time and money or their time and your money, this is a non-negotiable expense that will save you far more than it will cost you in the long run.