**7 IT Solutions and Practices to Protect Your Business**

In uncertain times like these, you need to ensure you’re doing what you can to protect your business. Here are some IT practices and solutions to help you do just that.

**Step #1: Protect Home Computers**.

Due to budget, low availability of computers in distribution channels, and the need for quick deployment, many of you will decide to set up teleworkers with remote access from their home computers. This is fine, as long as those computers are just as protected as your office computers. Some questions to ask yourself are A) is the home user’s WiFi properly secured? B) is their computer firewall enabled? C) do they have active, up-to-date and effective antivirus on their computer?

During this crisis, we are offering free installation of our corporate class monitored antivirus solution to ***anyone’s*** home computer, whether or not you have a service agreement with us – you just pay the monthly service fee.

**Step #2: Use Multi-Factor Authentication**.

VPNs are awesome, but not perfect. If VPN credentials become stolen for whatever reason, attackers can get right into your network. Adding multi-factor authentication protects your network by adding something you have (a cell phone with notification app, for example) with something you know (your VPN password) to help keep the bad guys out.

**Step #3: Use Password Managers.**

You have a different password for every system you access, already, right? (If you don’t, you should!!) But a great password policy makes remembering all those different passwords a pain. So, set up a password manager like LastPass and let it remember all those passwords for you. If the bad guys can only get one password, they can’t attack everything you can access.

**Step #4: Be Extra Vigilant about Email.**

You can bet that the bad guys are taking advantage of this crisis, touching on your fears to send bogus emails that look like they are from the government, or local hospital or the like, asking you to download files, click on links, or give away your credentials.

Be very cautious about every email you receive. Check to be sure that the email address it came from actually matches the person it says it’s from. Double check the email domain name – is it really from the organization it says it is?

And remember, we have multiple tools we can implement to help protect you, like our corporate class email spam and malware filtering, Dark Web Credential Theft monitoring, and Proactive Phishing Tests and Employee Training.

**Step #5: Secure Client Data.**

Working from home means more communication via email. This means more possibility of data leaks by sending personal financial, identity or health information through potentially insecure channels. If you have to send such information through email, be sure you have a way to do so securely. We can set up secure, encrypted email solutions to help you protect your clients and stay in compliance.

**Step #6: Backup, Backup, Backup!**

Backups are your last defense. If all else fails and you have an up-to-date backup of your data, then the failure is just an inconvienence, a tiny blip on the radar screen.

Are your servers backed up? What about your workstations? Office 365 documents? Your Exchange Online email? These are things to consider to ensure that no matter what happens, you can continue to operate.

During this crisis, we are offering free installation of our corporate class cloud backup solution to ***anyone’s*** computer, whether or not you have a service agreement with us – you just pay the monthly service fee.

**Step #7: Have A Plan.**

If the worst happens, do you have a plan? Have you put everything in place you can think of to protect operations? And is someone testing your systems to be sure they can be restored in case of failure? Most times, your plan doesn’t even have to be complex: just a list of scenarios and who to call when they happen.

For clients with our Disaster Recovery testing in place, we like to download a full copy of their critical systems and ensure we can restore them to brand new hardware. It never hurts to test!

Always remember, if you need immediate IT support or if you need help in setting up your business to ensure you’re ready for anything, contact us today.

****

**Joe Strosnider**

**Director of Client Solutions**

**Dynamic Networks**

[joe@dmcnets.com](mailto:joe@dmcnets.com)

740-399-3522