FREE GUIDANCE TO HELP YOU START PROTECTING YOUR DATA AND BECOMING SECURE TAKE THE FOLLOWING STEPS

These initial steps will get you to effective protection, without spending a lot of time or money.
Let us help you find the right cybersecurity solution for you!

80% SECURE

- ➔ Establish a security policy and enforce it.
- ➔ Educate your users – hold employee training sessions on security
- ➔ Never use an administrative level account as a user account.
- ➔ Ensure UAC – User Account Control level is enabled and working.
- ➔ Disable Windows Remote Desktop function, if you don't use it.
- ➔ Create Secure Passwords – Combination of Capital & Lower letter, Numbers, Special Characters.
- ➔ Require Passwords changed on a specified timeframe – i.e. quarterly
- ➔ Enforce Account Lock-out Policy upon multiple incorrect password entries.
- ➔ Enforce network-use permissions/guidelines for anyone with permission to access network data.
- ➔ Apply OS – Operation System and all Software Application Security patches as they become available.
- ➔ Remove any unnecessary extensions in your web browsers.
- ➔ Ensure Windows Firewall is enabled.
- ➔ Don't click on or open questionable emails, links, or attachments.
- ➔ Don't allow employees to connect their BYOB (Bring Your Own Devices) and IOT Devices to your WIFI network.
- ➔ Backup, Backup, Backup your data, two copies – secured in two different secure locations on-site and off-site.
- ➔ Use an Antivirus Software – Windows Defender is the entry point and 99.6% effective.

90% SECURE

- ➔ Use a Commercial Grade Email Scanning Solution like Barracuda.
- ➔ Did you know most attacks come via email?

95% SECURE

- ➔ Implement a Commercial Grade Firewall with Sand Box Function, Web Reputation Blocking.
- ➔ All Firewalls are not created equal, we deploy two types of Firewalls to assure

effectiveness.

- ➔ We prefer a Firewall that works with the Antivirus to shutdown computer communications for infected computers.
- ➔ At this point we have done about all that can be done to shield the environment from the bad guys. This is due to what is known as a ‘zero-day (also known as 0-day) vulnerability’. This is a brand new type of malware/virus that does not match a known pattern. It may use a door opened by another malware. This type of attack will generally come with a malware component.

100% SECURE

- ➔ Getting to 100% Secure requires a recovery method.
- ➔ Layered defenses provide multi-tiered protection – a recovery method that includes several layers.

The first layer – is a backup. Here we secure your data separate from the OS – Operating System, so your data is securely protected.

The second layer – makes a virtual copy of your machine. If your systems become infected, we can start the virtual backup. This will allow you to continue operations.

The third layer – moves the virtual copy off site. The process will start and test the core operating components, to assure operational capability.

The fourth layer – is Antivirus/Malware Software that is integrated with the offsite Recovery Layer. This will ensure that the offsite Recovery Layer is free of malware and virus.