Secure Remote Work

As experts in working remotely, we want to ensure you're working as safely as possible. Protect yourself from cyber threats and ramp up your cybersecurity.

Password Protection:

Do not use your internet browser to store passwords or information. Make sure this feature is always turned off as it provides easy access for hackers to access all of your information with just one account breach.

LastPass and 1Password are two popular Password Management tools. They generate and store strong passwords for you, so you do not reuse common phrases as passwords on multiple accounts. Password Management apps also allow you to share passwords, credit card information and more with your team securely for collaboration. Download the extension for quick secure form fill-in.

Protecting your Data:

To ensure you are operating safely, install an anti-virus. Modern Operating Systems (MacOS, Windows) have anti-virus built in and turned on by default. Use a supported operating system. This ensures that the OS vendor is actively evaluating and remediating for security vulnerabilities through update patches.

Encrypt the data on your mobile devices, including laptops and thumb drives. This ensures that even if the device is physically lost or stolen, your data will be safe.

Be Aware of Phishing:

During COVID-19, attackers are leveraging fear as a tactic to manipulate users into clicking links or opening documents. Be vigilant with the documents or emails you receive. Do not open any attachments or email that may be suspicious.

Need some assistance to ensure
you're working securely?

Contact us

We can help!

ADMIN SLAYER

www.adminslayer.com