7 Cyber Security Best Practices For Law Firms

naq

Keep your firm's online accounts secure and sensitive information protected with these easy to implement cyber security practices.

Keep Passwords Secure

A strong and unique password for each account is one of the most effective things you can do to reduce the chances of an online account becoming compromised, especially when companies like Facebook suffer a data breach.

Install a password manager such as LastPass, and change all of your existing passwords to a unique combination of letters (upper and lower case), numbers and special characters. Now, you'll never have to click that "forgot password" button again!

Enable 2 Factor Authentication

With multi-factor authentication, even if someone gets hold of your password, it's unlikely they'll be able to access the information needed to complete the second step of verification. You can verify via your email, or with an authentication app, to receive a unique code to grant you, and only you, access to your account.

Secure Your Networks

Change your WiFi name and standard issued password if you haven't done so after receiving it from your internet provider.

Even after you've configured your WiFi securely, you should always use a Virtual Private Network, or VPN, to secure the connection between your computer and the internet. **NordVPN** is a great, affordable VPN provider.

Beware how you share

Only share personal data via a secure cloud platform such as Google Drive or Dropbox.

These platforms not only encrypt your data to make your information illegible to an unauthorised reader, but you can password-protect the links and disable them after a certain period of time.

Keep viruses at bay

The best way to prevent viruses or malware infecting your computer is to not download them in the first place. Simple right?! You do this by making sure you don't click on any suspicious links in emails, download or open any files from suspicious or unexpected emails and don't visit any websites which could host viruses (you know what we mean, right?).

However, in case you do download something nefarious, it is important that you have an (up to date) anti-virus installed (such as Windows Security or Avira on MacOS) and enable your firewall (free on both Windows and MacOS, just check your security settings).

Take a break and update!

The well-known pop-up that says "there's a new update available" isn't just an annoyance - it is an extremely important part to securing your device and personal information. When we ignore those pop-ups, we are giving criminals the perfect opportunity to exploit the little holes in our software or operating systems that the update is intended to repair. So set your updates to "automatic" and simply take a little break whenever it's time for an update.

Backing up can be a life-saver

Imagine... It's late and you've just finished the preparations for a brief. You intend to finish first thing in the morning. But then, fate strikes, and your laptop has crashed. You've lost everything. Wouldn't it be nice if you had a backup? Yes, it would. So make sure you always back-up your data, including data in any cloud provider such as Google Workspace or Office 365. Ideally, back up your data to a remote location or cloud backup provider such as CloudAlly.

Would you rather somebody else take care of all this?
Contact us at lawoffer@naqcyber.com for a 50% discount on all our monthly subscriptions.

Cyber Accelerator Alumni

in association with National Cyber Security Centre

CYBER ESSENTIALS