Is Your Law Firm Protected?

Take The Quiz

All small to medium-sized businesses have security threats, but the level of data held by law firms requires a particularly high level of consideration.

It may be hard to know where to start, so we've devised this 8-question quiz for you to evaluate your practice and see where you stand.

Does your law firm pass the test?

50%
of phishing links are clicked on within the first hour of being sent.
*Verizon Data Breach Investigations 2015

Q.1

Does Your Law Firm Provide Cyber Security Awareness Training For All Staff?

Your staff members are your biggest asset, but also, your largest cyber security vulnerability.

Phishing attacks are a prominent technique used by cyber criminals and target anyone sat in front of a PC in your organisation. All staff members should be trained in how to avoid falling victim. The most common sign of a phishing attack is an email with a call for you to take action, but this can happen on websites too.

Make sure you make regular cyber security training available to them along with simulated phishing attack drills.

Q.2

Does Your Organisation Have Strong Password Requirements?

Each person will log into tens of unique accounts. They each require a password and memorising them all becomes challenging, resulting in employees re-using the same, or similar passwords over again. Those re-used passwords create a scenario where our email password is the same (or slight variation) to the password we used to sign-up for a free phone app. If a hacker gets in, he has a master-key to every application and file the employee has been accessing with that password.

In this case, no amount of device security will stop the breach. Your employee just opened the door and invited the hacker in for lunch. The only way to stop this large-scale breach is by encouraging your employees to use complex passwords, autogenerated by a password manager.

The National Cyber Security Centre were able to compile a list of 100,000 passwords that had been involved in data breaches.

*ncsc.gov.uk

Q.3

Do You Protect Your Law Firm with Updated Software?

Your devices are only as secure as your least protected device. Your security patches may be updated on 19 devices and machines, but the one that you forgot will be the weakest link.

One way to track updates is to use a device checklist. This list allows you to have a record of all devices, who is using the device, what permissions they have, and when updates are due or completed, among other things.

Your employees may have gotten tired of the annoying “update now” prompt and disabled it, or they may wait too long and allow hackers to take advantage of the time between when a new hacking application is discovered and when your devices are updated.

If you have an internal IT team, make sure they are staying ahead of all updates. If you don’t have an internal IT department, outsourcing your IT services allows professionals to keep track of updates and security patches.

Jupiter

Q.4

Does Your Law Firm Require Multifactor Authentication and Dual Approval to Access Your Network?

Using Multifactor Authentication tools can lock down your personal information and make it significantly harder for cyber criminals to compromise your accounts and information. A combination of a device login pushes, texts and passwords are a great first step to using multifactor.

You can also use human-to-human dual approval when possible. If you receive an email requesting you change the routing of payment that is coming from a vendor or client, give them a quick call to confirm before acting. Using a different medium to authenticate or confirm can stop a malicious attack dead in its tracks.

Q.5

Is Your Security Multi-Layered?

Having anti-virus and malware protection is good. Having a firewall is good. Having web filtering is good. Having email filtering is good. However, each one of these on its own is not enough to fully protect your law firm. Each security platform is subject to exploits, hacks and vulnerabilities.

The best anti-virus platform combines multiple overlapping forms of cyber security that can authenticate the identity of the correct user. Out-of-the-box anti-virus isn't enough to pass the rigorous rules and regulations governing legal practices, so you may benefit from having an IT partner that manages, updates, evaluates and makes changes strategically and proactively.

Q.6

Do You Have Disaster Recovery Backup?

Business continuity plans, including disaster recovery backup, are a key component to keeping your network up and running, regardless of the circumstances.

Ransomware is one example when backups can save your bacon. Ransomware encrypts your data and holds the key hostage for ransom. That leaves you with two possible outcomes: paying a criminal and hoping they give you the data back without selling or exposing it; or restoring the data from backups.

Even if ransomware seems far-fetched for your law firm, consider natural disasters such as storms, flooding, or fire and unavoidable data loss due to hardware failure or accidentally deleted files.

Cyber crime now accounts for over 50% of all reported crime in the UK

*National Crime Agency

Jupiter

Q.7

Is Your Law Firm Partnered with a Reliable Managed Services Provider?

An MSP can act as a "buffer" between your legal practice and compliancy violations. In short, if you have an agreement with an IT services provider and a breach occurs, the courts will be more lenient on you if you can prove you have taken good-faith measures to protect your law firm, such as hiring an MSP.

If you have an internal IT team, opting for a co-managed services platform is a great choice to make sure your existing IT department is fully able to secure your network. Outsourcing some of your IT needs is also a good way to make sure your internal IT department is up to date on trending cyber security threats and new, cutting edge technologies that your law firm needs to stay competitive.

Outsourcing your IT can be over 50% cheaper than employing a team.

Make sure to choose a company that has experience with protecting legal practices.

Did You Pass?

If you were able to check these questions with a firm "yes," you are well on your way to having a secure network. If you didn't, you need an IT audit to help you understand your vulnerabilities and how to bridge the gaps in your IT strategy.

Jupiter IT offers a comprehensive audit, free of charge and with no obligation, for any legal firm looking to strengthen its network security, functionality, and efficiency.

Delivering proactive IT support in Hull and the Yorkshire region that puts Cyber Security at the forefront of all we do.

Jupiter

CYBER ESSENTIALS CERTIFIED PLUS

UKAS ISO 9001

www.jupiterit.co.uk | hello@jupiterit.co.uk | Hull 01482 97 44 44 | Leeds 0113 887 8922 | Scunthorpe 01724 706 235