Osprey Approach: Securing your Practice with Two-factor Authentication (2FA)

This help guide was last updated on
Apr 11th, 2024

The latest version is always online at
https://support.ospreyapproach.com/?p=22062

Osprey™ Approach

The most valuable asset that most companies own these days is not their offices or fleet of company cars but instead, their data. This is why the fines for poor data management are so high, £20 million or 4% of annual turnover, whichever is the greatest.

We only need to look at the news to see that state funded agents are mounting sophisticated attacks to get data or even influence elections. The value of data and in particular your data must not be underestimated.

The most valuable asset that most companies own these days is not their offices or fleet of company cars but instead, their data. Learn how to protect your practice with our 2FA guide.

The SRA guidance

The Solicitors Regulatory Authority, in their Priority Risks Information and Cyber Security report, state that in order to mitigate risk you should **"use two-factor authentication for emails and log-ins where possible."**

They also recommend that "**you and all staff avoid predictable passwords**."

Both of these security mechanisms are provided as standard in Osprey.

All practices are at risk

The SRA report also states that "in the first six months of 2019, law firms reported a loss of £731,250 of client money to this type of crime", and that "27% of businesses who identified a breach in 2019 lost staff time dealing with breaches or attacks [and] 19% had staff stopped from carrying out daily work."

As firms begin to transition back to the office, and with staff spending time working on multiple devices in multiple locations, it is now more important ever to ensure your user access management is infallible.

PCW's Annual Law Firms' Survey demonstrated that 100% of the Top 100 law firms suffered a cyber security incident in the last year.

The coronavirus pandemic has led to a marked increase in targeted phishing scams. Action Fraud stated that Britons were conned out of £3.5million in the first two months of the lockdown.

The chance that you or a member of your team will be targeted by a phishing task is very high. If that were to happen, and a user accidentally divulged both their username and password, **Osprey's 2FA would prevent that hacker from accessing your data**. Using 2FA is another weapon in your fight to keep your data safe. It is another lock to the vault that holds your data.

A checklist to stay safe

We have put together a short checklist to assist you in employing appropriate user access controls across your organisation.

We are pleased to be able to provide you with a service that helps you meet the SRA recommendation and provides enforced 2FA and strong password management as a standard.

The additional measures and behaviours need to be implemented within your organisation. Our support team will be only too happy to answer any questions you may have on this topic.

- **Use two-factor authentication where possible**
- **Use strong passwords** - minimum of 8 characters alpha/numeric
- **Do not share credentials** - not only is this a breach of your licence it also poses considerable risk and entirely invalidates your computer generated audits
- **When a user leaves, immediately deactivate access** - do not repurpose the user account. Create a new user account. Users should not be logging on under someone else's name.
- **Review access levels** – ensure each user has access levels appropriate to their use of Osprey. Do not provide users with access to data or functions that they do not need.
- **Do not autosave passwords** – ensure that under no circumstances any passwords or username are saved by default. Both computers and mobile devices will offer this to you. Always choose the "Never save my password" option
- **Ensure mobile devices have strong pin codes** - ideally 8 characters, alpha numeric. Do not use your date of birth or year of your birth or the same digit multiple times. These are often the codes hackers will try first
- **Ensure mobile devices are enrolled in Mobile Device Management** – if your staff have access to emails and company data on their devices you must have the facility to remotely wipe those same devices should they be lost or stolen.

If we can assist you further with any other security questions or access management queries please do not hesitate to contact us.

Read more

- Why we are making 2FA compulsory
- Set up Two-factor Authentication