Osprey Approach: Two-factor Authentication (2FA) as standard for all customers

This help guide was last updated on
Aug 6th, 2024

The latest version is always online at
https://support.ospreyapproach.com/?p=17424

This guide will take you through our 2FA best practices

To ensure the security of your Osprey site and in line with the SRA Cyber Security guidance, we will soon be making Two-factor Authentication (2FA) compulsory for all customers.

There is every chance that now, and over the coming months, you will be accessing Osprey across various computers and devices. Firms are transitioning back to the office and develop new working practices across both home and office environments.

To ensure you continue to access your data in a secure and safe manner we will be introducing compulsory 2FA for Osprey logins over the next few weeks.

This in line with the recently updated SRA Cyber Security guidance notes.

At the same time we will be adding a minimum password complexity of eight characters using a mixture of numbers and letters.

What is 2FA and how is it more secure?

Two Factor Authentication (2FA) is an extra layer of security in addition to your username and password. You may have used this already with online services like banking, shopping or social media that send you a text message with a code. Osprey uses your email address instead.

1. **Each time you sign in** using your password **you will be emailed a one-time security code** that is only available for a short period of time.
2. When you sign in, you'll be asked to enter the security code from your email.
3. **After you enter the code**, you'll be signed in to your account.

This increases the security on your account because even if somebody guesses your password, they won't be able to access your account without also having access to your emails.

Over the coming weeks, 2FA will be required to access Osprey anywhere - via the browser, Windows App, our Office Add-Ins and our apps on iOS and Android devices.

At the same time, we will be adding a minimum password complexity of 8 characters using a mixture of numbers and letters.

Why will this be compulsory?

Two-factor Authentication (2FA), and enhanced password complexity features, have been available in Osprey for a long time and we have always encouraged customers to utilise them.

With changes to people's working patterns due to Coronavirus, and the latest updates to the SRA Cyber Security guidance, we have decided to make these security features compulsory.

This helps all of our customers stay compliant and secure whilst using Osprey.

We will be rolling this out over the coming weeks.

How do I enable it early for my organisation?

To ensure a smooth transition, we are encouraging customers to enable these features before they are enforced over the coming weeks. This gives you adequate time to communicate the change to your staff.

We have an Academy Guide which explains how to enable 2FA and set password complexity.

Read the Academy Guide

How can I receive more support with this?

Our support team are able to assist you in setting this up and are ready to answer any further questions you may have.

Contact Support