What is Multi-factor Authentication?

Multi-factor Authentication (MFA) is simply a security system that requires more than one method of authentication in addition to a password to verify the identity of an individual. This will be in the form of an "authenticator" mobile app to approve a login attempt.

Why are we using Multi-factor Authentication?

In short, MFA increases security and reduces the risk of unauthorised access to corporate systems and data. Using plain passwords, even secure ones, are often not enough to keep your account secure. There has been a significant rise in sophisticated phishing attempts that can dupe even the most security-conscious individual. Even strong passwords can be accidentally given away without the user's knowledge.

More information regarding Multi-factor Authentication can be found here.

Who will be impacted by MFA?

All Park Holidays team members and vendors who access our systems will be required to enrol for MFA.

How will this impact me?

Park Holidays will be implementing MFA to protect your Microsoft 365 sign-in. This means going forward you will be prompted for MFA on all devices when using applications such as Microsoft Outlook, Microsoft OneDrive, Microsoft Teams etc. along with platforms that contain sensitive data such as MyHub. Factors such as your location and devices will help decide how often you are prompted by Microsoft MFA – for example if you are based in head office (a “trusted” location) on a laptop you’ll get less prompts then if you were at home.

I already use SecureAuth, will this still apply to me?

Yes – SecureAuth is MFA at device level whereas Microsoft MFA is a method of authentication at software/cloud service level. We are looking at ways to combine these into a single MFA solution for better user experience long term.

Does registering for MFA give Park Holidays/IT access to my device?

No. Registering for MFA does not give Park Holidays access to your device.