beazley

Article

MFA - the (not so) secret way to prevent Cyber Attacks

December 19, 2022

For many cyber insurers, Multifactor Authentication, or MFA, is now a key condition on which they insist before providing coverage. This is because in today's world, it is considered essential in the fight against cyber-crime. But what exactly is it, and what makes it so important?

What is MFA?

MFA works by ensuring users verify their identity in two or more ways before granting them access to computer resource, such as email or a website/portal. It asks users for a password or PIN alongside a biometric verification, such as a fingerprint. This ensures that the user is who they claim to be, bolstering security and reducing the chance of a cyber-attack.

Why is it important for small businesses?

Cyber-attacks become more sophisticated, with attacks happening every 44 seconds. It's becoming increasingly important to protect yourself from cyber-attacks. MFA stops cyber criminals in their tracks as they attempt to access personal or commercially sensitive data because, if MFA is in use, simply knowing your password is not enough to allow a cyber-criminal to hack your system.
Not using MFA can be catastrophic for a business. Without the crucial second step, brute-force attacks – where multiple attempts are used to access an account or passwords are obtained somehow by the cyber-criminal – become a viable way of accessing your data. Such an event is often followed by a more serious one, such as a ransomware attacks. This is why a client who uses MFA to protect their systems is such an attractive one: it demonstrates that you not only have an understanding of the risk, but you are committed to reducing that risk, too. Currently under a fifth of UK businesses have implemented MFA; can you really afford to be one of them?

How can you implement MFA?

Implementing multi-factor authentication (MFA) is a great way to secure your accounts and protect your data. The best way to implement MFA is to use a verified third-party authentication service. To get started, you'll need to create an account and obtain an API key. Then, you'll need to integrate the service into your application, website, or platform. Once the service is installed, it can be used to generate a one-time password (OTP) for each user's login attempt. The user will then need to enter the OTP to authenticate their identity and complete the login process. With MFA in place, you can reduce the risk of unauthorized access and ensure your account is kept secure.

beazley