Multi Factor Authentication: Client Advisory

Multi Factor Authentication (MFA) is a cyber security tool that requires an additional step of verification on top of a password to verify a user's identity. It is most frequently used when logging into a network or accessing critical data and is usually done through an authenticator application, token or by using your mobile phone to send you a piece of information which helps prove you are the intended user.

Whilst hackers may already have compromised a staff member's login details, it is extremely unlikely that they will have access to the second authentication method and often you will be notified that there has been an unauthorised login attempt.

Enabling MFA is an effective way of protecting against unauthorized access or hacks, which could lead to a more severe cyber incident. Users can unknowingly reveal their login details to cyber criminals if they fall for a phishing email or social engineering incident. By adding MFA, you are increasing the protection of your accounts across the applications you use as it creates another barrier to stop unauthorised access.

Please get in touch with your IT professionals for the best way to implement MFA.

Jenny Arkell
Senior Underwriter - Cyber
E: jennya@atcis.com.au
P: 03 9258 1735

Lawrence Ormrod
Senior Underwriter - Cyber
E: lawrenceo@atcis.com.au
P: 02 9928 7107

Issued by ATC Insurance Solutions Pty Ltd ("ATC") (ABN 25 121 360 978, AFS Licence No. 305802), Level 4, 451 Little Bourke Street, Melbourne VIC 3000 acting under a binder as an agent of certain underwriters at Lloyd's EXTF143v1