RISK INSIGHTS

hamiltonleigh
Insurance Brokers
020 8236 5350
www.hamiltonleigh.com

The Importance of Two-factor Authentication

Cyber-security is an integral part of risk management for any organisation. Cyber-criminals are capable of executing devastating attacks that can result in financial losses, reputational damage and government fines. With those potential consequences in mind, employers should be mindful and take any precautions that might be able to protect them, such as using two-factor authentication.

Understanding Two-factor Authentication

Two-factor authentication requires employees and other authorised personnel to prove their identity and qualifications to access certain files or systems. For example, while many services may require users to enter a password, two-factor authentication goes one step further by requiring a second piece of information.

Using two-factor authentication can provide a strong second layer of cyber-security for organisations, inhibiting criminals from breaching an organisation's data with only a stolen password. Since hackers can steal even strong passwords, these cyber-criminals could gain access to important accounts, private systems, customer files and other sensitive information without a required second form of proof.

The National Cyber Security Centre (NCSC) recommends organisations set up two-factor authentication on any 'high value' accounts that protect particularly important information. It's also recommended to use this type of cyber-security for email accounts, as hackers who gain access to an email account may then be able to use that to reset passwords for other accounts and services.

Setting Up Two-factor Authentication

Many online services may inherently have two-factor authentication enabled. If this is not the case, the extra security can often be turned on in the security portion of an account's settings.

There are a number of different options when it comes to two-factor authentication, including:

- **Text messages**—Receiving a text message and relaying its contents to an online service is one of the most common forms of two-factor authentication. By providing a mobile phone number, services can send a code to users that must then be entered to finish the login process. Some services may also be able to provide a voice message instead. It's worth noting that text messages may not be the safest form of two-factor authentication, as cyber-criminals could potentially gain access to your mobile device, SIM card or mobile network.
- **Authenticator apps**—These apps for mobile phones or tablets are the most common alternative means of two-factor authentication after text messages. Once installed, these apps, such as the Google Authenticator and Microsoft Authenticator, can be used for a number of services. Unlike text messages, using these apps does not require a mobile signal.
- **Backup codes**—Some online services can provide users with a list of backup codes for two-factor authentication. This method may be particularly

useful if users do not have reliable access to a mobile phone; however, each code can only be used once. Users should be especially careful about where this list of backup codes is stored, as the information falling into the wrong hands could severely compromise cyber-security.

Organisations should consider consulting qualified cyber-security professionals to determine what type of two-factor authentication would be optimal.

Once two-factor authentication has been established, many users will only have to prove their identity in certain situations. For example, when logging into an account from a new device or attempting to change a password, the additional security may be activated.

In Conclusion

The NCSC hopes that, eventually, two-factor authentication will be offered on all online services that deal with personal data, finances or other valuable information. For now, employers should be sure that if two-factor authentication is not available for important accounts, then strong, unique passwords are used and changed regularly. Organisations may even want to consider switching services altogether to an option that does provide this additional level of cyber-security.

For more information on cyber-security, contact us today.