BRIT

writing the future

why multi-factor authentication (MFA) matters

Just recently, the National Cyber Security Centre (NCSC) announced that almost half of UK businesses and a quarter of charities reported a security breach or cyber-attack in the last 12 months. While many of us use multi-factor authentication (MFA) every day, too few understand what it is and how it can help. Dr Jessica Barker, Co-CEO and Head of Socio-Technical Security at Cygenta, shares her passion for cyber security awareness and the importance of MFA.

Companies adopting MFA

Since the invention of Multi-Factor Authentication (MFA) methods in the late 1990s, the uptake by companies has been slower than many security professionals would like. There can be a perception that MFA is an overcomplication for people, asking them to use another password – or follow another step – without recognising the value in this.

Thankfully, that barrier has come down over time, and many companies now implement one of many off-the-shelf MFA solutions. More and more employees and employers see the benefits of MFA and, importantly, some consumers are starting to demand it.

MFA works by granting access to a system after the user provides two or more pieces of evidence (or factors) to the authentication system that validate their identity.

It is worth noting that MFA encompasses two-factor authentication (2FA). Factors may include:

- Something a person has: a security token, a card, a key
- Something a person knows: a PIN or password
- Something a person is: biometric data such as a fingerprint or facial recognition
- Somewhere a person is: a specific connection point or GPS location

COVID-19's Impact on security

With COVID-19 having pushed companies of all sizes into remote working, MFA is even more vital in securing networks from attack. While virtual private networks (VPNs) have been around for years, many people have not needed to use one – until 2020. A VPN allows remote workers to connect to their company network over the internet. Without MFA helping to protect these connections, it's often just a matter of criminals 'brute-forcing' account email addresses and passwords – and see everything that employees can see. Hacker tools make this easy, being able to guess billions of password combinations an hour. Simply put, adding MFA to your environment is an effective layer of defence for your network.

Lack of Knowledge around MFA

The biggest issue with MFA is perhaps an image problem. In 2019, we found that 62% of UK internet users did not know what two-factor authentication is (out of a sample of 1,000). Beyond that, 45% did not know whether they used it – and only 26% said that they did. In fact, most people will be using MFA/2FA without even realising it, for example, when they withdraw money from an ATM. The combination of a bank card and PIN prove to the bank your access is valid; if they do not match, authentication is denied. An attacker can steal a card, but without the PIN is unable

continued

to withdraw money. Hence MFA does not have to be onerous, and it enhances security way beyond a single factor of authentication.

Usernames are not considered factors when it comes to online accounts since they are often based on email addresses – or can be easily guessed. Therefore, if an account is secured by a password only, it is secured by only one factor. We all know there are many issues with passwords, from multiple breaches that involve passwords to the fact that many people use (and reuse) passwords that are easy to remember and thus easy to crack and bypass.

Protect Your Clients and Consumers

Like all cyber security solutions, MFA is not infallible. But any form of MFA is far better than none at all, representing a simple and effective layer in your defences. Many solutions are almost 'plug and play', with authentication platforms and frameworks easily implemented. Free software MFA applications, such as those provided by Google, allow any size company to offer MFA to their clients and consumers, providing enhanced security at a minimal cost.

No form of defence will protect you completely, but layered defences will make you a less attractive target, make criminals work harder, and make attacks easier to spot when they happen.

78% of people do not enable Two-Factor Authentication on their devices. Even the most straightforward steps can make a big difference. Check out our Cyber Security page to find out more about MFA and how Brit can help protect your clients.