a window into cyber

March 2021

a note from Ben Maidment

Class Underwriter, Brit Cyber Services

Spring is traditionally the time when many of us declutter and spruce up our homes. We can – indeed we should – do the same with our digital lives; ideally more than once a year though! The UK's NCSC recently announced that almost half of UK businesses and a quarter of charities reported a security breach or cyber attack in the last 12 months; a sobering reminder that a digital spring clean should be high on all our lists.

Even the simplest steps can make a big difference. This month, our guest author Dr Jess Barker writes about Multi-Factor Authentication. It has a huge impact on cyber crime; put simply, if a company has good MFA, it is less likely to have a breach. We're also flagging-up a couple of new training courses from Datasafe, so do check them out.

Most of us are still working from home, but there's a feeling that brighter days are on their way. In the meantime, stay safe – and don't hesitate to get in touch if you need us.

this month's author: **Dr Jessica Barker**

Co-CEO and Head of Socio-Technical Security, Cygenta

Dr Jessica Barker is a leader in the human side of cyber security. She has been named one of the top most influential women in cyber security in the UK and has been recognised with a TechWomen50 award. She is the co-founder of co-CEO of Cygenta, where she follows her passion of positively influencing cyber security awareness, behaviours and culture in organisations around the world.

Along with being the Chair of ClubCISO, she is a popular keynote speaker who regularly shares her expertise in the media. In 2020, she was the keynote speaker at RSA San Francisco and her book 'Confident Cyber Security; How to get Started in Cyber Security and Futureproof your Career' was published in September by Kogan Page.

Why MFA matters – no matter your size

Dr Jessica Barker | Co-CEO and Head of Socio-Technical Security, Cygenta

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, that it is asking them to use another password – or follow another step – without a recognition of the value in this.

Thankfully, over time, that barrier has come down, 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.

To start, let's address a fundamental question: what is 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

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 had no need 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-

continued on next page

> "More and more employees and employers see the benefits of MFA and, importantly, some consumers are starting to demand it."

"MFA enhances security way beyond a single factor of authentication"

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.

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) click here to see the survey. 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 to withdraw money. Hence MFA does not have to be onerous, and it enhances security way beyond a single factor of authentication.

When it comes to online accounts, usernames are not considered as factors 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.

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 that can be 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 minimal cost.

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

@drjessicabarker
linkedin

stop press

Urgent cybersecurity alert

Microsoft has detected multiple zero-day exploits attacking on-premises versions of Microsoft Exchange Server – and the associated email accounts. The 2013, 2016 and 2019 versions are affected.

Click here for more information and what to do.

proud to share our knowledge

BRIT

Adelle Gruber, Senior Cyber, Privacy & Technology Underwriter is a member of an advisory committee at the UK's Police Digital Security Centre, aimed at improving cyber cover for SMEs.

Investing in cyber security has never been more important and whilst many businesses believe that they are protected against cyber threats, only 70% of businesses who have undertaken our Digitally Aware certification have passed it, leaving the other 30% vulnerable to cyber crime and fraud.

PDSC POLICE DIGITAL SECURITY CENTRE

www.policedsc.com

The data collected from Digitally Aware assessments highlights the gaps SMEs have in relation to their security posture.

Only **39%** of organisations have a cyber security training plan in place for their staff

However, EVERY SINGLE organisation that failed Digitally Aware at their first attempt, did not have a cyber security training plan in place

Only **45%** of organisations have given staff cyber security training in the last 12 months

65% of organisations allow staff to connect their work devices to public WiFi

Of organisations that failed the assessment at their first attempt:

56% have not made password managers available for their staff to secure their passwords

67% do not have a password policy in place

78% do not enable Two-Factor Authentication on their devices

33% do not set their devices to automatically update their software

These vulnerabilities are easy and simple to resolve. Using the resources from our Digitally Aware platform, designed specifically for SMEs, business can quickly improve their security posture and reduce their vulnerability to the most common types of cyber-crime.

Source: Police Digital Security Centre

news from datasafe

Datasafe provides the latest risk management resources, enabling Brit's clients to proactively manage their data protection and privacy risks.

New training courses for 2021

These online courses cover the basics of privacy/data security for individuals who handle sensitive information.

Introduction to breaches

Employee mistakes: an introduction to the common cyber security mistakes that can lead to a costly data breach – and how to prevent them.

Social engineering

Business email compromise: explains the various ways attackers can steal company funds through email scams – and identifies the simple steps to avoid becoming a victim.