a window into cyber

October 2020

a note from Ben Maidment

Class Underwriter, Brit Cyber Services

BRIT

We've become used to all kinds of new behaviours associated with Covid-19. These include thinking twice about what we do, where we go and who we see. Keeping a social distance, wearing a mask and regularly sanitising our hands has become second nature. Consciously and unconsciously, we're all now making new risk assessments on a daily basis – to keep ourselves and others safe.

October is Cyber Security Awareness Month. Originally launched in the US in 2004 and extended to Europe in 2012, the campaign highlights the threats of online attacks and promotes cyber security issues. It also provides access to resources that help organisations and individuals understand and mitigate the risks. In this month's issue, Dr Jess Barker shares her tips for raising awareness of cyber security – and our Datasafe page highlights the risks of ransomware.

At Brit, we go beyond simply insuring against risk; we help businesses take control of it, so they can operate with confidence. Given that many of us will be working from home for months to come, Cyber Awareness Month reminds us that practising rigorous cyber hygiene is more critical than ever.

Stay safe everyone; we're here 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.

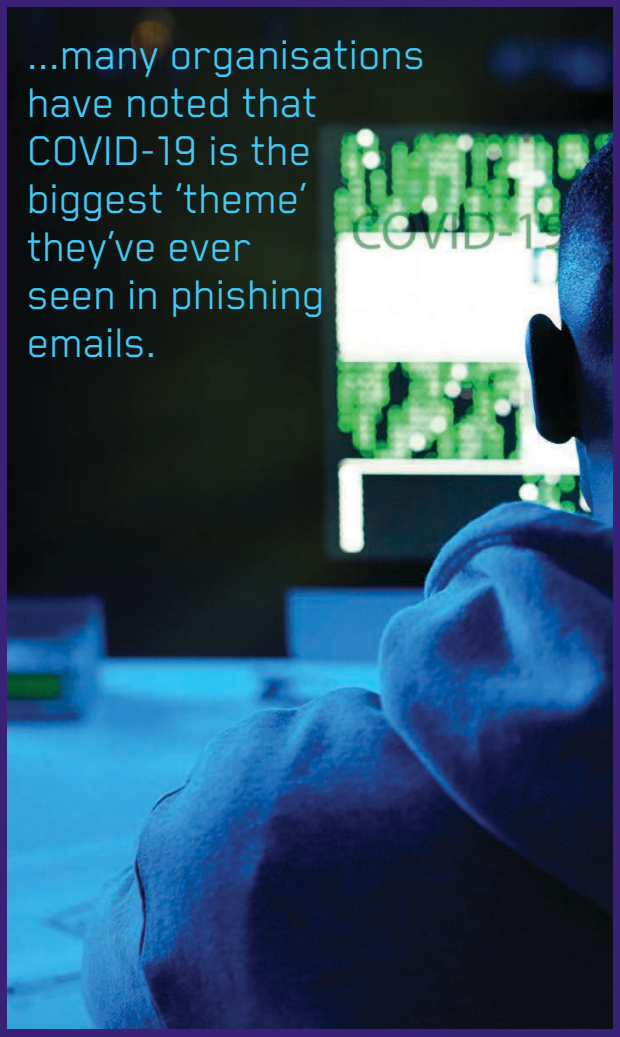
BRIT

How to make the most of Cyber Security Awareness Month

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

October is Cyber Security Awareness Month (CSAM), and it seems to have come around quickly this year. Using CSAM to focus on cyber security awareness initiatives has grown in popularity in recent years and now most big organisations will incorporate CSAM in their awareness programme in one way or another.

This year should be no exception, although plans will have undoubtedly had to shift. Many organisations embrace CSAM as a time for the security team to get out and about in the business, running physical events, hands-on workshops and generally getting people together to focus on security. Over the last six months, those plans have morphed for many and now some organisations have a virtual programme mapped out and others are wondering how to make the most of CSAM in the current circumstances.



The current circumstances, while we are globally dealing with COVID-19, makes awareness-raising even more important. Security teams across many organisations have noted that COVID-19 is the biggest 'theme' they've ever seen in phishing emails. Combining this with the fact that many of us are working from home and the threat landscape for organisations has opened up massively, it's clear that the need for security awareness has never been greater.

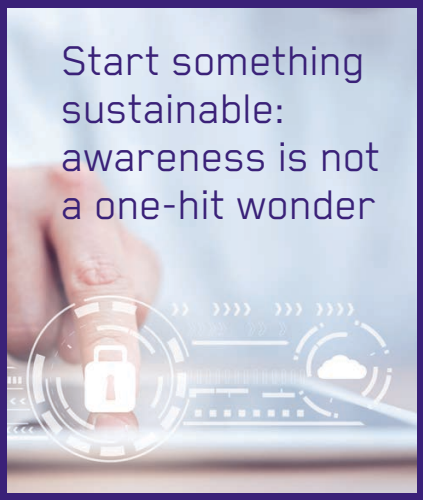
Whether it is for CSAM or beyond, what can organisations do to engage people in cyber security awareness-raising remotely? I've been designing and delivering cyber security awareness-raising for the last ten years, and these are my top tips:

1. Prioritise the personal: many of us have relied on technology more than ever in the last six months, with our personal and professional lives blending even more than they did before. Building this into your awareness efforts can help the organisation and the individual, so why not support your workforce with awareness-raising that focuses on security for people at home, giving advice aimed at enhancing security for families.

2. Elevate the experience: the most impactful awareness-raising is that which doesn't just tell people about security, it shows people why security matters and gets them involved. This can be tailored for an online format, with live hacking demonstrations, virtual escape rooms, phishing tournaments and online scavenger hunts some of the options you could explore.

3. Start something sustainable: awareness is not a one-hit wonder and whatever we do when it comes to awareness-raising will be most effective when it is part of a wider plan. For large organisations, this is likely to be detailed, for smaller organisations this may be far more straightforward. Regardless of the organisation, a great way to develop a sustainable security awareness programme is to build a security champions network. Security champions are not security experts,

continued on next page



and instead act more like health and safety representatives – or fire wardens – but for security. They can represent a friendly face for security awareness and be a fantastic mechanism for two-way communications between the security team and the rest of the organisation. Security champion programmes require a bit of work and planning to make them effective and long-lasting, but when you can do that, they pay dividends.

Security awareness doesn't have to be costly or too complicated. If you don't have a programme in place, start off simply and see what resources you already have at your disposal. Whether you do it in October, for Cyber Security Awareness Month, or any other time of the year doesn't really matter at the end of the day. When you do it matters a lot less than what you do.

@drjessicabarker
https://www.linkedin.com/in/jessica-barker/

Cyber Underwriting
innovation of the year

Brit Cyber Attack Plus

Insurance Insider
Cyber Rankings Awards 2020

in insurance insider

innovation winner

Our specialist BCAP product meets the unique needs of industrial and trade business clients. We're delighted that it's been recognised by this year's Insurance Insider Cyber Rankings Awards. Congratulations to the whole team!

For more details visit:
www.britinsurance.com/cyber/bcap

Adam Taylor

the best in the business –

as voted for by our peers

We're delighted to report that Brit's Adam Taylor was awarded 'Cyber Underwriter of the Year' in the fourth Insurance Insider 2020 Cyber Rankings Awards, announced on 23 September.

Unlike many awards, which typically involve a judging panel picking category winners, the Cyber Rankings Awards are derived from aggregated survey data. This year 928 London Market cyber underwriters and brokers were questioned in July and August, to establish who the market believes are the leading companies and professionals.

highlights from datasafe

BRIT

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

Current hot topics for Brit policyholders

top resourced accessed:

Employee Mistakes

Identifying Fraudulent Payment Cards

Phishing

Inspecting Credit Card Machines

Malware

Password Best Practices

top training courses completed:

Password Management Policy

Acceptable Use Policy

Cybersecurity Fitness Check

Wire Fraud Reduction Policy

Human Resources Security Policy

Clean Desk Policy

On the increase: ransomware

Datasafe is receiving a high volume of calls relating to incident response planning and phishing training and campaigns. These are a direct reflection of the increase in ransomware attacks, which we all know is on the rise. Criminals are now stealing data before encrypting victims' on-premises copies and demanding millions for a decryption key and/or the promise not to publish stolen data. Ransom demands are so high they typically exceed insurance policy limits. But no-one has to be a ransomware victim. Essential safeguarding steps include:

- Training employees to recognise phishing emails
- Protecting all remote access (including any Microsoft RDP access) into your environment with two-factor authentication. If you are not using RDP, close port 3389.
- Installing software patches in a timely manner
- Backing-up all critical systems and data regularly

For more information visit Learn how to Stop Ransomware. Our top eight ways to beat ransomware can help prevent costly loss of time, productivity and money. Additionally, we have a recorded webinar which includes information about preventing ransomware. This can be found in our Webinar section.

Datasafe's October email campaigns align with Cyber Security Awareness month.

Our weekly campaign topics:

- If you connect it, protect it
- Securing devices at home and work
- Securing internet-connected services in healthcare
- The future of connected devices