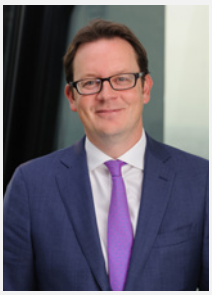
a window into cyber



a note from Ben Maidment

BRIT

Ransomware is fast becoming one of the most common types of cyber-attack with even the most unsuspecting people aware of its existence. As recent high-profile incidences of Netwalker ransomware attacks on institutions have shown, ensuring an organisation is educated and equipped to protect against this growing threat is important.

With new threats increasing, cyber literacy is vital for the continued success of businesses and organisations. To that end, the Datasafe site has been updated to highlight key ransomware training materials which are available as an unlimited resource to our policyholders.

At Brit, our goal is to help you face a more secure future, confidently. And we hope this issue gives you insight into ways to navigate this ever-changing cyber landscape.

this month's author: Dr. Jessica Barker

Co-CEO and Head of Socio-Technical Security, Cygenta *@drjessicabarker*

Dr. Jessica Barker is a leader in the human side of cyber security. She's been named one of the top 20 most influential women in cyber security in the UK and was awarded as one of the UK's Tech Women 50. She is co-founder and co-CEO of Cygenta, where she follows her passion of positively influencing cyber security awareness, behaviours and culture in organisations around the world. She is also the Chair of ClubCISO and a popular keynote speaker who regularly shares her expertise in the media. In 2020, she was the keynote speaker at RSA San Francisco and is due to have two books published.

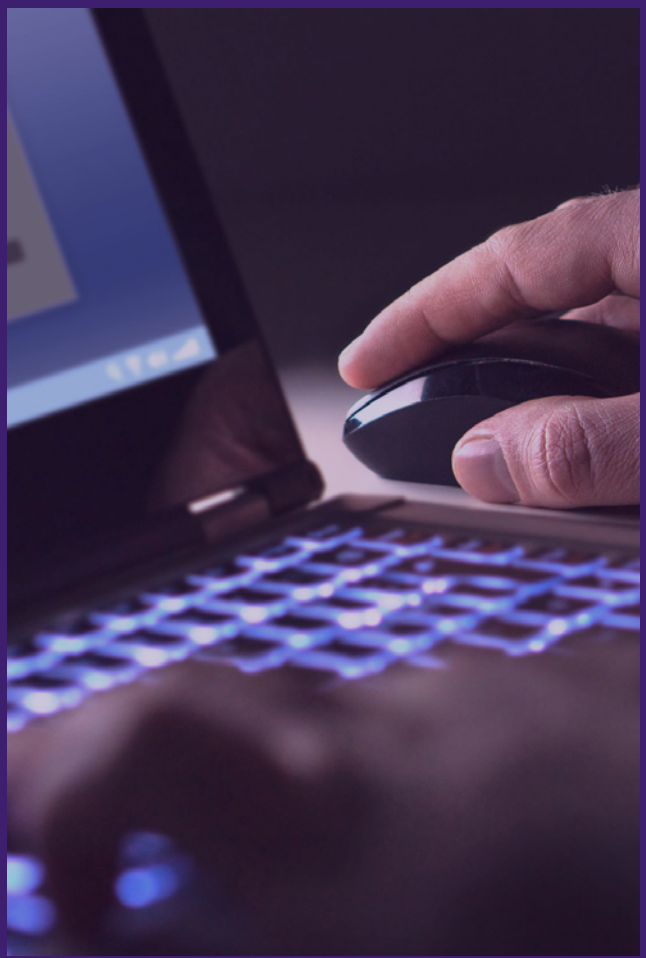
BRIT

why do people fall for phishes?

by Dr. Jessica Barker | Read time: 3 minutes

The first known ransomware was created in 1989 and now,over 30 years later, ransomware has evolved to be one of the most prevalent forms of cyber-attack. It has changed from something that was pretty basic to a much more mature form of attack. We now see ransomware being used as a distraction tool to mask more complicated forms of attack. We have also witnessed the emergence of 'leakware' or 'extortionware', in which your data is not simply locked up, it is also stolen. The cyber criminals threaten to publish the data unless you pay the ransom.

There are many different ways that ransomware can spread, some of which are technical. However, the most common threat vector is phishing. Those scam emails that come in looking like they come from your bank, boss or best friend and encourage you to click a link, download an attachment or transfer money. Sometimes they're incredibly easy to spot, but other times they are much more sophisticated.



There are many different ways that ransomware can spread, some of which are technical. However, the most common threat vector is phishing. Those scam emails that come in looking like they come from your bank, boss or best friend and encourage you to click a link, download an attachment or transfer money.

I've worked on the human side of cyber security for nearly a decade and helped many organisations that have been a victim of a phishing-based incident or who are trying to protect against social engineering. One of the most common misconceptions I have come up against, is the idea that people are stupid if they fall for a scam. I think people tell themselves that to reassure themselves that they could never become the victim of a phishing email. The reality is, we're all susceptible to being scammed.

continued on next page

the long lens continued

BRIT

So, why do people fall for phishes?

One reason is that many people simply do not understand the harm that can be wrought from clicking a link or downloading an attachment. A linked issue that we face, is that many people do not comprehend the scale of cyber-crime. Statistics do not mean much when we are trying to convey an unseen, intangible threat; they are too easy to dismiss.

The good news is that we have all become savvier with phishing emails. We know to look out for grammatical errors and to be sceptical of emails from royalty wanting to share their wealth with us. The bad news is that cyber criminals know we have evolved, so they have evolved, too. Many phishing emails are much more targeted now than they used to be and they try to manipulate us by influencing how we process the information in the emails.

The criminals move ahead by looking at our behaviour and our evolution; by understanding their methods, we can do the same.

The criminals have embraced Nudge theory and understand that if they use certain psychological triggers (time pressure, shame, temptation and curiosity – to name a few), we are more likely to process the information quickly and not give ourselves time to question before we click. They make us panic, and when we panic we have less capacity to consider that everything may not be as it seems and that our reaction could have unintended consequences. The criminals move ahead by looking at our behaviour and our evolution; by understanding their methods, we can do the same.

an underwriter's outlook

cyber criminals still busy amid pandemic

James Bright ACII, Senior Underwriter, War and Terrorism | Read time: 5 minutes

Contending with COVID-driven demand destruction has captured much of the oil and gas industry's attention in recent months. But another formidable threat, which has risen markedly since last year, deserves just as much vigilance: the potential physical and financial consequences of cyber-attacks for oil and gas firms.

Learn more about what firms can do to better protect themselves against cyber-criminals who are currently exploiting many oil and gas industry players' preoccupation with COVID-19.

click to read full article on Rigzone

highlights from Datasafe

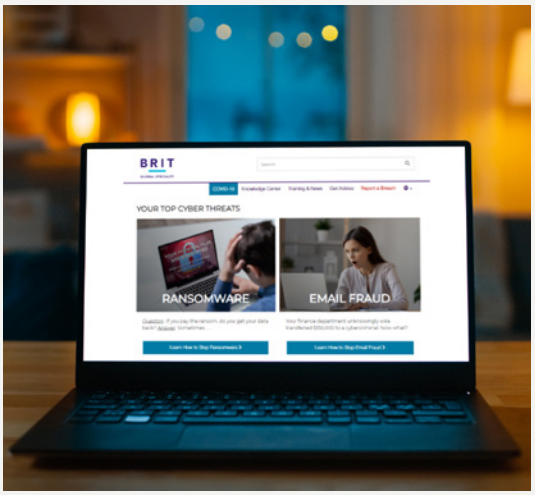
BRIT

Datasafe delivers the latest risk management resources so clients can proactively manage their data protection and privacy risk.

The Datasafe site has been updated to highlight resources for ransomware – one of the biggest causes of claims. This will help alert Brit policyholders to new threats and remind them that they have free, unlimited access to cybersecurity experts and training coordinators dedicated to equipping them with relevant training exercises.

These are just some of the resources available on Datasafe:

- **"New Attacks" section** for the latest cyber threat attacks and stats
- **Cyber Blog** for additional articles and stats
- **Ransomware page** for an article on the top 8 ways to beat ransomware
- **Free online ransomware training course** for policyholders, including assistance from a concierge-level training coordinator



Thursday, June 25, 2020
Time: 10:30 AM Pacific Time, 1:30 PM Eastern Time

Protecting Against Your Top Cyber Threats

Ransomware and email fraud are your top cyber threats and can cost your organization millions. Half of businesses have experienced a cyber scare since the COVD lockdown.

Learn effective strategies your organization can implement to protect against these threats. Many safeguards are easily implemented with practical steps you can take now to reduce the likelihood of falling victim to an attack.

register now

britinsurance.com/cyber