

a window into cyber

December 2020



a note from Ben Maidment

Class Underwriter, Brit Cyber Services

BRIT

The rate at which organisations continue to embrace digitalisation is accelerating. Yet for most, their ability to secure themselves from attack isn't keeping pace – and the pandemic has thrust this growing divide into the spotlight. While COVID-19 created challenges for us all, both personal and professional, it also provided new opportunities for hackers.

The abrupt worldwide shift to remote working was a gift to cyber criminals, who have exploited every weakness: from vulnerable corporate systems to individuals' pandemic-related anxieties. This month, Madeline Howard reflects on 2020, highlighting how psychological manipulation – better known as 'social engineering' – is on the increase.

Against this turbulent backdrop, cyber security has never been more critical. That's why we at Brit – and our colleagues at Datasafe – are committed to keeping you informed and reassured. Whatever 2021 holds, we've got your back.

Wishing you a happy Christmas – and a safe and healthy New Year.

this month's author: Madeline Howard

Socio-technical Engagement Manager, Cygenta
@Madzzhoward

With a wide range of global clients, Madeline focuses on the human aspects of cyber security. As a CyberFirst Ambassador for the National Cyber Security Centre, she works with young people to highlight the importance of cybersecurity and the diversity of careers in the field. Madeline is also a Director of Cyber Cheltenham, the UK's largest cyber cluster.



reflections on 2020

the rise and rise of social engineering

Madeline Howard | Socio-technical Engagement Manager, Cygenta

2020 has been an unprecedented year for many reasons; the most obvious being the COVID-19 pandemic. And unfortunately, cyber criminals across the world have exploited this global crisis: increasing the number of attacks, creating more targeted attacks and impacting critical national infrastructure. However, such incidents do represent an opportunity for us to consider what we can learn from them; and be better prepared and protected.

COVID-19 phishing

Phishing attacks aren't new – and they are probably here to stay. Cyber criminals are always looking for new themes to use to engage us and sadly, they have exploited COVID-19 due to the heightened levels of emotion and uncertainty surrounding it. It has been reported that there was a 667% increase in phishing scams in one month alone during the pandemic. We have seen a huge rise in COVID-19-related phishing attacks that prey on our willingness

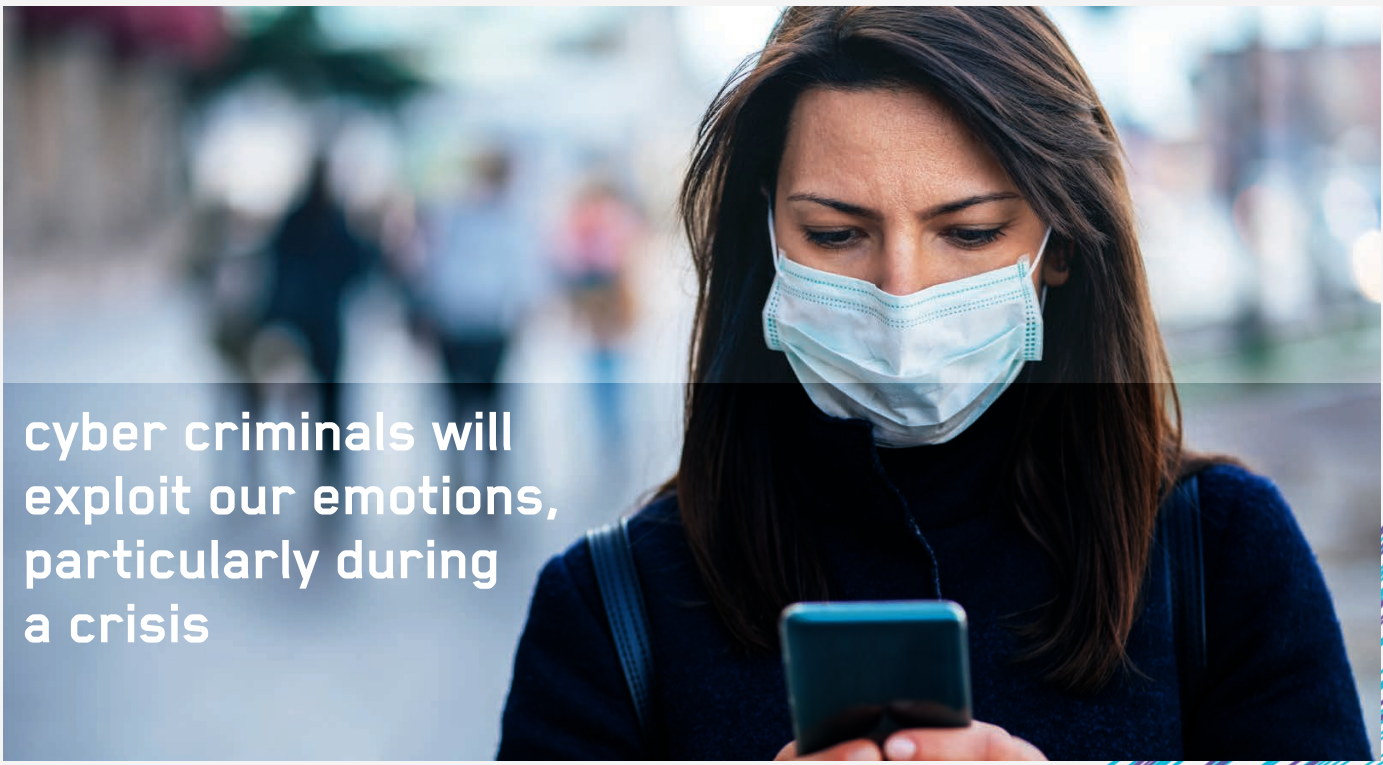
to help others, our financial worries, concerns about PPE, testing, cures and discount codes to name a few.

The rise in phishing attacks – and COVID-19-themed attacks in particular – is a reminder that cyber criminals will exploit our emotions, particularly during a crisis. This is the key message we need to raise awareness of when it comes to social engineering: if you receive a communication that you're not expecting, which asks you to do something and makes you feel emotional, be aware this could be social engineering.

Twitter hack

2020 has also reminded us that phishing is not only carried out over email. In July we saw the extraordinary compromise of 130 high-profile celebrity Twitter accounts through vishing (voice phishing). The criminals obtained the phone numbers of a handful of Twitter employees

continued on next page



cyber criminals will exploit our emotions, particularly during a crisis



and used social engineering techniques, such as friendly persuasion, to gain their usernames and passwords, giving them access to internal systems. The criminals then went on to compromise high profile accounts, send tweets, access private direct messages and download some content. Twitter observed: 'This was a striking reminder of how important each person on our team is in protecting our service.'

This hack was a stark illustration of the different methods used by cyber criminals to engage us with their scams. It is important to remember that all organisations, even the most tech-savvy, can fall victim to social engineering – and that raising awareness of cyber security is crucial for all businesses.

Ransomware in hospitals

Ransomware is an unforgiving attack at the best of times, let alone when it impacts healthcare during a global pandemic. Ransomware spreads through a network and locks down data, with a promise that it will be unlocked when the ransom is paid. In September, hospitals in both the US and Germany were targeted with ransomware attacks. In Germany it is reported that a woman died, sadly

making this the [first death directly linked to a cyberattack on a hospital](#). [US hospitals](#) in California, Florida, North Dakota and Arizona were forced back to using pens and paper due to their digital systems being locked down.

To protect ourselves from ransomware, we must always be vigilant when clicking links and downloading files, because it is often spread by social engineering. The prolific spread of ransomware also reminds us of the importance of regularly backing-up data, storing these back-ups offline and testing them to ensure they are working as we would expect.

2020 will be a year that many of us will want to forget. However, the lessons from some of the biggest cyber security incidents of the year are things we should not. It is important we move into 2021 feeling empowered by technology – and confident in how to use it securely. Reflecting on lessons learned is one of the most powerful ways we can understand the cyber security threat landscape – and be better prepared for, and protected from, the attacks of tomorrow.

[LinkedIn: Madeline Howard](#)

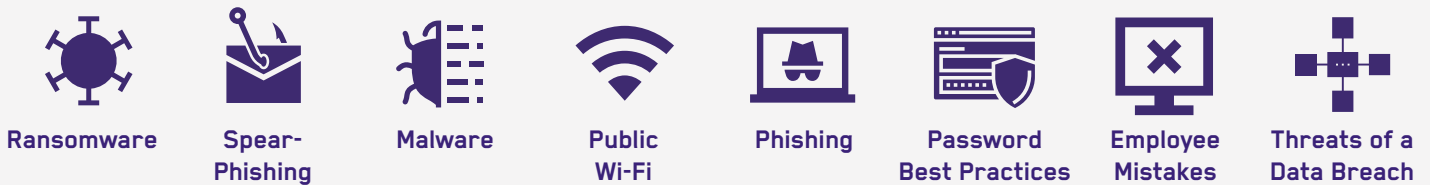
highlights from datasafe

BRIT

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

Hot topics for Brit policyholders in 2020

top training courses completed:



top resources, documents and policies accessed:

- Cyber Security Fitness Check
- Email Policy
- Information Security Incident Response Plan
- Password Management Policy
- Coronavirus Cyber Hygiene Poster
- Information Security Policy
- Acceptable Use Policy

ransomware update

The 2020 Q3 findings from ransomware experts Coveware show that Remote Desktop Protocol (RDP) is still the primary attack vector.

Worryingly, the falling price of stolen remote access credentials indicates that supply is outpacing demand. Hence securing RDP ports (removing them from the public internet and placing behind a VPN/RD gateway with MFA) is more critical than ever.

No target too small

Small and medium-sized companies are suffering a disproportionately high number of attacks, yet they generally have less adequate back-up and fewer resources to completely recover. Most ransomware victims have annual revenues of less than \$50m, with professional service firms being especially vulnerable.

A constantly evolving threat

A recent example of ransomware involves using Facebook to publicly shame victims. The Ragnar Locker gang hacked an individual's Facebook page and then bought ads to pressure a victim, the Campari Group, to pay the ransom. The ad campaign warned that the hackers would release Campari's data if they failed to pay - and reached almost 8,000 Facebook users before being shut down.

Source: [Coveware Q3 report](#)