# Cyber Security, Life As We Know It

## “How the world answered a 15-year debate and what we know about 2020 so far”

# Introduction

As business as usual starts to return and we adjust to the new normal, it's important to understand the ways cyber security has changed throughout the lockdown period, and what new threats have evolved along with how to mitigate against them.

A good place to start is a brief overview of the state of cyber security during the Covid-19 pandemic. Indeed, all those but key workers were confined to their homes while the virus spread across the globe, some working from home, others not. During this time, Covid-19 was unfortunately not the only virus we need to be aware of as cybercriminals work continuously to compromise individuals and businesses networks.

In terms of financial damage, a cyber born virus has the capacity to do equally, if not much more damage to organisations from an economic standpoint compared to a biological virus than ever. The repercussions this may have on reputation is also not to be underestimated.

## A 15-year debate answered in 2 weeks, can we work from home?

When lockdown was announced, many organisations were forced into a digital transformation when preparing to setup a secure remote workforce. This for many involved IT projects which previously would have taken weeks, if not months to process. Instead, this happened almost overnight. With the unforeseen pressure of securing networks for remote access, those that did not have a cloud-first strategy had a significant challenge. At worst this created opportunities for threats to infiltrate organisations as both systems and people adapted to the new normal, working remotely without the backing of your IT resources, both staff and equipment. it is no surprise to hear of the increase in cyber-attacks over the last 3 months, whether it be phishing attacks or malware

It became increasingly important for businesses to have sufficient technology in place for a secure work force, such as sufficient VPN's and MFA, however another important element in security is the safety of their people. With many employees distributed across the world, accessing networks from various and sometimes unknown locations, the need for staff education increased.

To educate those responsible for cyber security, and even those outside of IT departments, we've broken down what threats may have evolved from this 'new normal' and how to address these issues as the world continues to adapt. looks like, why you need to evolve as times are changing, and step you can take to do this.

# The arising challenges while the new normal evolves:

- **500% increase in cyber-attacks** leveraging Covid-19 (WHO) in the first month of lockdown alone

- **60% of employees Work from Home (WFH)** - Employees/students WFH create a new threat vector and access points to your systems are dispersed nationwide

- **8.9million jobs furloughed in the UK** – For furloughed employees, cyber security may not have been at the forefront of their minds recently and workers may have become unfamiliar with existing cyber security policies

- **Multiple sites, limited collaboration** – with staff not working collectively in one space, it makes it difficult for colleagues to collaborate over suspected threats/attacks. This lack of communication could have serious repercussions

- **600,000 decrease in number of employees on payroll** – From March – May unemployment rates have dropped for the first time in years. This will have undoubtedly left some individuals disgruntled, and perhaps triggered to access the network maliciously

- **New Starters While WFH** – how can senior IT leaders guarantee they are fully up to speed on cyber security strategies during the on boarding process?

- **Public/Home Wi-Fi** – it is impossible to gauge the safety of Wi-Fi networks your workforce is accessing and difficult to monitor their activity

- **Business Continuity Plans** – The majority of business continuity plans will not involve a global pandemic, or the impact COVID-19 would have

## 89% of Business Leaders see Cyber Security as a top 5 priority now

# Adapt to the new normal, address the issues and reduce risk by protecting your people, wherever they are:

## REDUCE RISK

### Revise -

Revisit business continuity programmes and include the possibility of a global pandemic. We might think and hope the chances of a situation like what we have experienced happening again are unlikely, however, we cannot be sure. This could happen again, and when it does, businesses must ensure they have made suitable amendments to BCP's  to protect themselves.

These revisions may also involve HR team members, particularly when dealing with employees who may no longer be within the business. Ensuring the relationship between ex-employees and your organisation is amicable is desirable from a cyber security perspective.

### Expense -

Why, if an organisation already has various email security measures in place - which do not come cheap - is cyber security awareness training a necessary expense for the business. Indeed, existing email security is needed. What we must remember is however, although it is designed to defend your network against cyber threats, it cannot be 100% accurate in preventing them.  All it takes is for one threat to bypass your existing solution – which could be a mature multi-layer defence barrier - to reach an uneducated end user for there to be a data breach which could potentially damage your organisation financially, but it's reputation also.

The missing piece of the cyber security puzzle here is the knowledge of the end user, which, had they received more training, could have been stopped. Should they have been educated, the induvial could have been able to spot the threat early on, report it and carry on with their day, organisation unharmed. This critical change in security and shift in mindset will probably cost far less than your traditional email security yet be a critical component within your network security. It's worth noting that people, like technology cannot be 100% effective in stopping cyber-attacks either; but by marrying traditional email security and the human firewall, organisations can form a multi layered, sophisticated barrier against cybercrime .

# Reducing Human Factor Risk

**D**iversity - With 90% of security breaches involving humans, cyber security awareness is extremely important. Within that 90% however, will be people with a plethora of preferred learning techniques. With any learning avenue one size does not fit all, and so a variety of approaches is necessary for an effective programme. Catering for different types of learning not only increases the effectiveness of the training but also creates a more enjoyable environment of learning. This can be done using quizzes, videos, simulations, and infographics for example. Keeping staff members engaged are the foundations of an evolving cyber aware mindset, which can be extended outside of the office to personal devices and while perhaps travelling .

**U**se IT resources wisely: To preserve IT admin time, having an automated training system is also beneficial – not only can employees be educated on cyber awareness while their day to day role is undisturbed, but IT teams can focus their efforts on other tasks while having the peace of mind that their colleagues are constantly learning.

## Gmail is currently blocking 18,000,000 phishing emails per week

**C**onsistency - The journey of increasing cyber awareness should start in the onboarding process and should be maintained throughout a person's employment period. As threats evolve near daily, continuous training is essential for up to date knowledge and awareness. This should be shared among new starters from the offset to promote not only an awareness around cybercrime but also instil your organisations cyber aware culture.

## A Phish Frenzy – its estimated 530,000 Zoom credentials are available on the Dark Web

# Turn Your Employees into Security Assets

**E**nquire – curiosity will breed effective learning if encouraged in the right way. Encourage employees to air concerns over cyber threats and emphasise this does not have to be only in the office. While we continue to adapt to the new normal while working throughout the era of video calling and messenger, end users should feel comfortable using these platforms to ask for help on any queries. By encouraging this inquisitive behaviour, end users will collaborate between themselves or them and their IT team forming a cyber aware culture, which, although will be driven by IT leaders will also make users more aware and accountable for their online habits on an individual basis .

**R**eporting – what gets measured gets improved . By using a solution which provides a detailed report, on an individual and organisational basis, IT leaders can identify high risk users within organisations and monitor progress as a company on their learning journey to becoming more cyber conscious. It can be difficult for IT leaders to constantly monitor end user's online behaviour while they work on other tasks, whether it be in a small or large business. Having a detailed report readily available to review is another time saving tool for IT departments and senior leadership teams.

**I**ntervals – little and often is the best approach to learning. Delivering training in bite sized portions ties in with the consistency element of this approach to cyber security. Long, basic training formats will become boring and employees may become complacent, making the training ineffective .

**''Learning that is spread out over time drastically increases knowledge retention.''**

- *Source: Effective Learning Techniques, Promising Directions from Cognitive and Educational Psychology*

## Large Data Breaches in 2020:

## EasyJet cyber attack exposes 9m customers details

# Educate Your People on How To Identify Social Engineering

System Firewall vs. Human Firewall - the Human Firewall is equally as valuable as the System firewall, and it can complete your cyber security portfolio and is often the missing link : in the same way your traditional email security does, humans receive and process information which requires decision making as to whether this information is safe and secure. For technology, this process can be automated and managed at a system level, for humans however, this criterion utilised when evaluating the legitimacy of information is acquired through continuous education around evolving threats, and exposure also. By learning the varying approaches cyber criminals can take, and exposure to these through simulations, for example, allows their knowledge to evolve as threats do. This coupled with regular testing of progress is when a behavioural pattern is formed around cyber security awareness .

Keep it simple - It is important to note that cyber security awareness training does not have to be complicated, or time consuming. Employees within organisations are expected to fulfil their allocated role, and aside from those within the IT team that does not require hours of intricate, technology led training. It could be as simple as educating employees on password protection best practices for example. The simplicity of cyber awareness training is another important element to an effective training programme, over complication can lead to misunderstanding and incompletion.

## 4 Tips To Spot The Current Phish – Look Out For....

1. **Authority** – usually claiming to be someone official
2. **Urgency** – given a limited time to respond to the request
3. **Emotion** – praying on fears, curiosity or hope
4. **Scarcity** – offering product in high demand

## About Boxphish

Boxphish offer automated, intelligent & interactive training in Cyber Security Awareness to teach organisations to identify email-borne threats and change behaviours accordingly. Our defence strategy centres around our four features - Simulator, Reporting, Artificial Intelligence & University - which are designed with industry knowledge in mind for an effective solution against phishing, ransomware, social engineering & CEO Fraud. With online training modules, simulated phishing attacks, videos, quizzes, and helpful resources sent straight to your email, there is an option for every schedule and learning style, all can be delivered as a managed service.

For an initial discussion and demo visit **www.boxphish.com**

BOXPHISH

BOXPHISH.COM