HFW CONSULTING

MAY 2020


# COVID-19 AND CYBER CRIME

**The impact of the COVID-19 pandemic has undoubtedly changed our lives and will continue to do so for some time to come. During this uncertain time, organisations and people are looking for information, support and safety through government, health and media channels.**

This desire for information is leading to an increased presence of organised crime groups who are exploiting the fear, uncertainty and doubt which COVID-19 brings to target organisations and individuals in a variety of ways.

## What are the threats?

Since the start of the pandemic, security organisations have reported the rapid build-out of infrastructure by cybercriminals used to launch COVID-19 themed spear-phishing attacks in an attempt to lure individuals to fake websites seeking to collect personal information or organisational credentials.

## The response

There are some key steps you should take to reduce the risk to your organisation and your employees, particularly as working conditions remain flexible:

- Raise awareness amongst your team warning them of the heightened risk of COVID-19 themed phishing attacks
- Share definitive sources of advice on how to stay safe and provide regular communications on the approach your organisation is taking to the COVID-19 pandemic
- Make sure you set up strong passwords, and preferably two-factor authentication, for all remote access accounts; particularly for Office 365 access
- Provide remote workers with straightforward guidance on how to use remote working solutions including how to make sure they remain secure and tips on the identification of phishing
- Ensure that all provided laptops have up to date anti-virus and firewall software
- Run a helpline or online chat line which employees can easily access for advice or report any security concerns including potential phishing
- Disable USB drives to avoid the risk of malware, offering employees an alternate way of transferring data such as a collaboration tool

Over the past few weeks organisations have relied on video conferencing technology to keep in contact with its suppliers, clients and internal colleagues, but these platforms have also provided for security breaches. It is therefore critical, as we continue to rely on these platforms, to ensure that your organisation has an alternate audio and video conferencing environment available. This alternate platform will be needed if you have a ransomware incident that disrupts your IT systems, whilst providing a back-up if your primary conferencing provider has capacity or availability issues.

As we begin to enter the next normal, and restrictions begin to ease, our focus will inevitably shift towards adaptability; we will have to learn to live and work in a new environment. This potential “drop-in-guard” will afford cybercriminals new opportunities to infiltrate networks and steal data. Therefore it is now critical to ensure that the security systems remain in place and organisations remain vigilant to attack.

For further advice or to find out more about our Cyber services please contact:

**CHRIS O’CALLAGHAN**
Director of Consulting
**M** +44 (0)7769 364113
**E** chris@hfwconsulting.com

**HFW Consulting works with clients around the world to help them develop their businesses, enhance their people and protect against risk.**

**hfw.com**