Phishing Attacks during Coronavirus

As with any significant change, the coronavirus pandemic and the rapid deployment from office to homeworking has created anxiety and significant risks to businesses. More than ever before, staff are falling prey to sophisticated cyber-attacks, which could destroy the business.

The move to homeworking has happened at breakneck speed for many, with little time for planning, and has caused a decrease in IT infrastructure security. Often staff are now using business devices to search the internet for information on COVID-19 and for hard to find products and in so doing, they risk inadvertently clicking on the wrong link and infecting the device and the organisation's infrastructure.

Recent research has shown that during the lockdown, 66% of employees working from home have no cyber security and have received no training in how to protect themselves and their employer from cyber-attacks. In addition, some businesses found that security enabled equipment designed for the office is less efficient in a homeworking environment. However, instead of providing staff with security training and properly enabling equipment, they remove essential security features such as multi-factor authentication because staff, many of whom have not previously worked from home, are struggling to cope and they believe that security is affecting productivity.

Unfortunately, these changes have not gone unnoticed by cyber criminals, who see this uncertainty and reduction in security as a golden opportunity and since the beginning of March 2020, phishing emails have in one security expert's words 'gone through the roof due to COVID-19'.

Phishing is a cyber-attack in the form of an email. The criminal's goal is to trick the email recipient into believing that the link will take them to something they want or need or that it contains a request such as from a known individual in their company. The recipient is asked to click a link or download an attachment, which deploys a virus, trojan or worm.

Staff are falling prey to increasingly bespoke phishing emails that are hard to distinguish from a genuine email, particularly when sent to already anxious staff.

Businesses who handle people's financial information and especially SMEs have seen a dramatic growth in phishing emails, from fewer than 500 per month before the coronavirus to over 3,000 per month since the government lockdown. More worrying is that a higher than ever number are getting through security netting the criminals millions of pounds in April alone.

These are extremely dangerous developments at a time when IT security and staff security awareness in many businesses is at an all-time low and when businesses have effectively moved from one or two offices to a hundred or more. Added to which, the password for most domestic routers and internal Wi-Fi equipment is available on the internet and security is little better than that on a public network.

Well-known businesses have already suffering the loss of thousands of clients' or customer's personal data including their credit or debit card details and other financial information. These businesses now face ICO and other regulatory action and damages claims that will far outweigh their insurance cover. Businesses should give urgent consideration to protecting their IT infrastructure and devices during the pandemic and to having early discussions with their IT and data security partners.

Written by:
David Sinclair, Senior Solicitor at rradar