BUSINESS IN THE COMMUNITY

The Prince's Responsible Business Network

# COVID-19: Online safety for business -- issues and solutions

Many small businesses have been put at risk from cyber security breaches as a result of coronavirus and the consequent lockdown. This is largely due to a combination of more employees working remotely and weak cyber security strategies (Crowdstrike, 6 April 2020). Business in the Community (BITC) has been working with members of its Business Emergency Resilience Group to identify some of the top cyber security risks during the COVID-19 outbreak.

This factsheet gives two examples - based on information provided by our insurance partners - which bring to life recent issues seen by small businesses and illustrate how cyber security can easily slip under the radar. The case studies have been anonymised to protect the identity of customers. We then outline several common issues realised over the last few weeks in the UK since lockdown on 23 March. Alongside this, we have provided easy-to-implement solutions to reduce these risks in order to improve safety online and enhance business continuity. More detailed information about specific cyber security risks arising from COVID-19 has been produced by the National Cyber Security Centre.

## Bringing cyber security risks to life: two notable incidents

INCIDENT 1

Greg has been asked by his employer to purchase and expense a suitable work phone as they were unable to source one for him before the COVID-19 lockdown came into effect. He browses the web on his work laptop looking for a reasonably priced and reliable make and model as he wasn't given specific purchasing criteria. He remembers that he received a targeted email from PC World with the latest discounts to his personal email address, so he logs in to check. When asked, he saves the password for his personal email on his work device to save time.

INCIDENT 2

Susie has been working in her box-room at home since the COVID-19 lockdown came into effect. She lives in a small flat, and so must work in the same room as her husband. After Susie takes a call from a client, she pops to the kitchen to make a cup of tea leaving her work device open in the room. A notification pops up her computer, she hears it and asks her husband to check if it's important.

HRH THE PRINCE OF WALES ROYAL FOUNDING PATRON

## Cyber-security problems and solutions

| Issue | Potential problems | Suggested solutions |
|---|---|---|
| **Use of equipment** | Businesses of all sizes have had to rapidly provide their employees with the correct equipment to be able to work from home.<br>Some companies may be forced to ask their employees to purchase and expense their own IT equipment. | • If it is not possible to courier a standard-issue company device, then employees should be given clear instructions on the make and model of any IT equipment to purchase for work. This makes it much easier for IT departments to: consistently and accurately bring those devices under their control; deploy and configure the security policies; install updates; and use the appropriate device management software to secure remote devices.<br>• Where possible, do not allow access to internal servers from personal devices.<br>• For further guidance on securing employee-owned assets, we recommend following the National Cyber Security Centre's 'Bring Your Own Device (BYOD)' guidance. |
| **Susceptibility to attacks** | Cyber-attackers use organisations' working patterns against them. According to research by IBM, the volume of malicious emails with attachments spikes more than 38% on Thursdays over the average weekday volume[1]. | • Working from home can result in added distractions (e.g. parcel deliveries, children, pets and fatigue) meaning that social engineering attacks could be less easy to spot. Therefore, encourage employees to be extra vigilant when processing customer data and/or invoices.<br>• Fatigue, lapses of concentration and small screens can lead to mistakes such as copying in the wrong person into your emails or attaching sensitive data to emails. Raise awareness within your workforce to these common human errors.<br>• In order to remain vigilant throughout the working week, BITC recommends encouraging breaks – away from a screen – and ensuring that your employees get enough sleep.<br>• Check out BITC's wellbeing guidance. |

[1] https://www.csoonline.com/article/3199997/don-t-like-mondays-neither-do-attackers.html

| | | |
|---|---|---|
| Consider website policies | Working from home can blur the lines between home and work life. Even before COVID-19, research showed that, on average, only 10% of employees do not use their work devices for personal reasons at home, with a staggering 76% using it to reply to personal emails and 55% giving access to their friends and families[2]. | • Clearly communicate with employees that work devices should only be used by them and to avoid the temptation to allow their children or partners to use them.<br>• If possible, employ white or blacklisting to prevent access to sites that pose a higher risk to your organisation. If listing is already used, increase its scope to recognise the increased risk profile<br>  ◦ Whitelisting refers to the practice of blocking all entities except those that are explicitly allowed to communicate with you or your infrastructure (Twistlock.com)<br>  ◦ Blacklisting means accepting most entities, but excluding those that you believe to be malicious or otherwise wish to avoid (Twistlock.com)<br>• Where restrictions on websites cannot be enforced, remind colleagues that accessing private emails should be avoided due to the increased cyber security risk of malware-laden spam that could affect work devices. |
| **Different working environments** | Many employees are working in new environments. Some are working in close proximity to partners, flatmates, and other family members. Others are working collaboratively on platforms that encourage screen sharing | • Remind employees to be mindful of their working environment and ask them to take care not to expose confidential information when screen-sharing on conference calls.<br>• Consider whether employees should use a screen filter when working with client data at home.<br>• When employees are speaking on the phone, encourage them to think about sensitive client information that might be overheard by others at home. We suggest when taking client calls that employees use headphones to prevent the breach of sensitive information and refrain from naming clients if the information is sensitive. |

For more details, contact: info@bitc.org.uk

[2] https://www.secureworldexpo.com/industry-news/employee-risk-corporate-devices-personal-use