COVID-19 and the importance of 'cyber-hygiene'

Ashley Quenault
English Solicitor
+44 (0) 1534 760 856
ashley.quenault@bcrlawllp.com

Introduction

With many businesses now working remotely, it is even more important that business leaders and those responsible for risk management consider and address good cyber hygiene practices and steps as it is almost inevitable that cybercriminal activity will surge during this crisis as they seek to exploit and take advantage of this already stressful and demanding situation.

What should businesses be doing to ensure good 'cyber hygiene'

Businesses should be frequently reminding their workforce about the basics of good cyber hygiene which would include:

- Reporting suspicious emails to the IT or other appropriate department and thoroughly checking the providence of emails to make sure that the email is genuine
- Ideally emails should not be sent to employee's personal accounts as these can be less secure than accounts within the businesses firewalls
- If receiving an email from a personal account rather than a business account extra attention should be given to examining the email header and the contents of the email to ascertain whether this could be a phishing attempt
- Not sharing any personal or financial information by email unless it is sent through a secure email facility to a verified recipient
- Being aware of social engineering, namely a phone call or email purporting to be someone represeting the government or technical support
- Ensuring that data is regularly backed up to a secure location
- Ensuring that passwords are made as strong as possible and changed more frequently

Whilst social distancing is possible, cyber-distancing is not. The only way to combat cybercriminal activity is to be hyper-vigilant.

This briefing is only intended to give a summary of the subject matter. It does not constitute legal advice. If you would like legal advice or further information, please contact us on the details above.