EVERSHEDS SUTHERLAND

# Black Friday & Cyber Monday Alert

## Issues for employers while staff are WFH

Black Friday and Cyber Monday means – DEALS, DEALS, DEALS! The 2020 holiday season will be unlike any other we have experienced. In many cases, COVID-19 will keep us in our own homes and away from crowded shops. That may be a good way to curb spending, but the reality is, your employees still want to shop. Starting with Black Friday and Cyber Monday, it is open season for online shopping and online fraud.

Between today and tomorrow, it may be a good time to review and remind employees of your IT policy. Whilst it is very important to allow employees opportunities to buy their Christmas gifts in a safe way, that should not have a negative impact on the productivity of your business.

**Reduction in productivity**

Employers report that there is often a drop in productivity over the next week. It is not as easy for your people managers to be a bit more present over the coming days to keep productivity up. Whilst operating in a remote world, it may be difficult to enforce active working hours without appearing like Scrooge. It's a good idea to organise virtual team meetings or brainstorming sessions with tangible follow up action items to keep a focus on your goals.

**The Employee "Shopping Hour"**

Business permitting, you could turn a "don't" into a "do". For example, you could proactively contact your employees in advance and outline that this year, you are providing all employees with a "shopping hour" to be taken in one go or in several slots over Friday, Monday and cyber week. The reality is that many employees will take this time anyway so you can turn this into a positive message. It also allows you to proactively remind employees of your IT Security policy and the appropriate use of company equipment.

**Security Risks**

Many companies have identified increased security risks and security breaches with employees working from home. Albeit that employees may still be using their company equipment, many employees, in the comfort of their home, do not think twice about clicking on a too good to be true offer.

We have drafted the below top tips so that you can easily send them on to your staff.

Scammers will be looking to take advantage of one of biggest shopping event of the year by tricking unaware shoppers.

By taking a few precautions, our business can avoid becoming a victim.

- **Never click on a suspicious link** – scammers might target you with emails with promotional links, appearing to be from a legitimate retailer. This is an attempt to get your attention and trick you to click on a link which carries malicious malware. If the links look suspicious to you or you're not sure of the source of the email, do not open them. Better to go directly to the retailer's website to verify the deal.

- **Beware of phishing emails** – phishing emails are designed to look like they were sent from a legitimate company, such as your bank or the retailer you shop frequently from. They'll ask to verify your details. Do not provide details in an email reply.

- **Make sure the site is secure** – a key rule when shopping online is to check that you're on an encrypted page, meaning that you should check that the page's URL starts with "https". If you don't see it, the site you're on may not be legit.

- **Avoid shopping on public or open Wi-Fi** – cyber criminals know how to thwart unsecured Wi-Fi to gain access to the information you send over it. So, it's better you eat into some of your data to make sure your financial information is secure, than logging onto a public Wi-Fi to shop the latest bargain.

- **Use a credit card or shop through Apple Pay or Android Pay** – credit cards offer consumer protection if things go wrong with a purchase. Mobile payments solutions such as Apple and Android Pay are also good to use because they combine biometrics with other digital safeguards, making sure your details are secure.

- **Use complex passwords for online retailers** – having strong, secure passwords is essential to keeping your online identity and accounts safe from hackers.

These security practices should be followed throughout the year but it's essential to put them into practice during the holiday shopping season when cyber criminals increase their attempts to steal your online credentials or infect our system with malware.

**For further information, please contact:**


**Lisa Bryson**
*Partner, Employment & Immigration*

**T:** +44 28 9526 2020
LisaBryson@
eversheds-sutherland.ie

**Laura McManus**
*Associate, Employment & Immigration*

**T:** +44 28 9526 2021
LauraMcManus@
eversheds-sutherland.ie