# BUSINESS CONTINUITY MANAGEMENT: CYBER ATTACKS

**IT systems are often crucial to the running and continuity of a business. They can be used to sell products for your business, communicate with customers and suppliers, and to control your finances. Therefore it is important to become resilient to attacks that may affect your continuity.**

## CYBER CRIME IN THE UK HAS COST BUSINESSES £87 BILLION SINCE 2015

HTTPS://WWW.BEAMING.CO.UK/PRESS-RELEASES/UK-CYBER-CRIME-HAS-DOUBLED-SINCE-2015/

## BACK UP YOUR DATA!

- Back up any electronic files regularly on an external hard drive and an online storage system such as Google Drive. Making hard copies of files is also recommended and these should be locked away both on and offsite.
- Ensure any copied files or storage devices aren't connected to the device holding the original copies, not physically or over a network.

## PROTECT DEVICES USED IN THE WORKPLACE

- Ensure that they are password protected. Use unique, strong passwords with numerous characters, numbers and symbols.
- Do not use public WIFI when sending sensitive files in public spaces, use 3G or 4G.
- Ensure staff only have access to information which is necessary for their role.

## WAYS OF PREVENTING MALWARE DAMAGE

- Install up-to-date anti-virus software on all of your business' computers, laptops and electronic devices.
- Turn on any automatic software and computer updates where possible.
- Ensure that emails containing sensitive data are encrypted.
- Prevent staff using removable and personal media devices such a USB or SD cards in the workplace as they can sometimes contain unreliable or risky files. If these devices are necessary to carry out their job, they should be either provided by the company or approved for use by IT staff.

Creating a strict IT policy for staff members will also help to reduce the chance of a cyber attack happening. Companies should always make sure that their IT security is up to date.

## AVOIDING PHISHING ATTACKS

- Educate yourself and your staff to be aware of scam emails. For example, emails containing poor spelling and grammar, low quality logos or those asking for specific details or link clicks.
- Make staff wary of clicking on certain links or entering login details on unfamiliar pages.
- Check that emails and email addresses are legitimate.
- Ensure staff do not browse the web or check personal emails on a works account or network.

Last reviewed: January 2025
**For more information visit: www.thefloodhub.co.uk**
This resource has been produced by Newground