Cyber crime

CRIME GUIDANCE

Cyber Crime is crime that can only be committed through the use of online devices and where the devices are both the tool to commit the crime and the target of the crime.

Cyber crime is an active threat to all UK businesses including the convenience sector. Convenience retailers must review their cyber security measures and colleague training to protect their business from cyber-attacks.

What Cyber security measures should I have in place?

This guidance is based on the National Cyber Security Centre *Small Business Guide: Cyber Security* available in full here: **ncsc.gov.uk**

Back up your data

All businesses, regardless of size, should take regular backups of their important data, and make sure that these backups are recent, separate from your computer and can be restored. Consider using cloud storage solutions.

Protect from malware

This is malicious software that can damage your business. Install and turn on anti-virus software, which is often free with your existing operating system, turn on your firewall and keep IT equipment updated with the latest software updates. Reduce your colleague's ability to download software and apps and control the use of USB drives in your business.

Keep smartphones and tablets safe

Switch on password protections such as pin or facial recognition, keep your device and apps updated and make sure mobile devices can be tracked and remotely erased in case they are lost or stolen. Make sure your colleagues do not use unknown or public wi-fi hotspots when using mobile devices.

Strengthen your passwords

Switch on password protection across all your IT equipment such as screenlock password, PIN, or other authentication method (such as fingerprint or face unlock) and avoid using predictable passwords. The NCSC advises you to use three well-chosen random words that can be quite memorable but not easy to guess such as TreeMugCar.

Phishing emails

Phishing emails are reported as the most common type of cyber crime experienced by convenience retailers. Phishing emails are fake emails asking for sensitive information. You should consider the following actions:

Minimise colleagues IT permissions

Give colleagues the lowest level of user rights required to perform their jobs.

Look out for common tricks

Common tricks include sending an invoice for a service that you have not used or sending emails impersonating members of your team asking for money or information.

Report all attacks

Encourage staff to report phishing emails by forwarding questionable emails to report@phishing.gov.uk. If you have become a victim of online fraud, report it to **Action Fraud** here: https://www.tinyurl.com/yckkhcba

Check for obvious signs

In phishing emails spelling mistakes often appear and grammar is often poor. Is the email addressed to you or 'valued customer' or 'friend'?

Our website www.acs.org.uk **Our social media** @ACS_localshops on X, Bluesky, TikTok and Instagram
Association of Convenience Stores on LinkedIn, Facebook and YouTube

ACS the voice of local shops