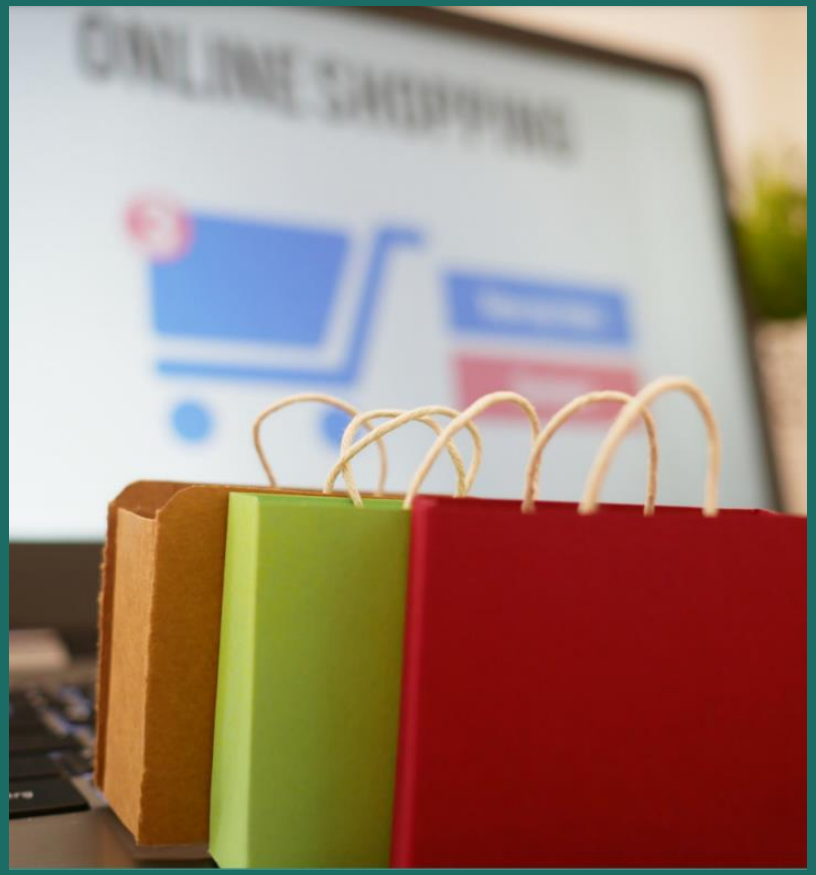


THE
EASTERN
CYBER
RESILIENCE
CENTRE

Retail
Cyber Guide 2022

Introduction

THE EASTERN CYBER RESILIENCE CENTRE

Why does Retail need to be aware of cybercrime?

As you will probably be aware retailers have experienced some major ups and downs over the past 2 years, with almost every business having to adapt to new ways of shopping caused by the pandemic.

Websites and social media have become increasingly important for businesses to drive brand awareness and interact with customers. And most shops without an online presence in March 2020 have now moved some or most of their business onto the internet.

Unfortunately, retailers were not the only ones adapting. Cyber criminals have increased their attacks globally. And criminals who operated in the real world in 2020 have now moved online to exploit the internet themselves.

This guide has been specifically created to give you, a retailer, an overview of the key threats. It also provides some guidance that you can implement to help protect your business.

I hope you find this guide useful but more importantly I hope you feel able to take some steps in protecting your business from the villains out there who just want to steal your money and steal your customers data.

And as a member, I look forward to working with you in the months and years to come – I believe we can genuinely make your business safer and more secure. And that's good for everyone!

Paul Lopez

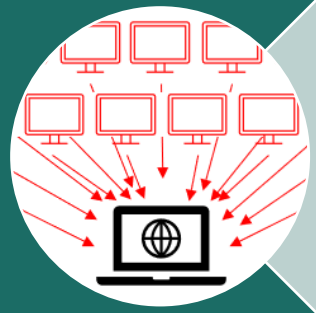
Director of the ECRC
Detective Superintendent Paul Lopez

Key Threats

These are the top threats you need to be aware of

Phishing - this is where a cybercriminal will impersonate a trusted person or organisation to trick the victim into clicking a link or downloading something which will infect the victim with malware. This is the most common form of cyber attack and can be the most difficult to guard against.

Ransomware - once an attacker has got into your system, they will encrypt all your files, stopping you from being able to view them. They will demand a payment for the files to be decrypted. Be aware even if you pay you might not get any or all your files back. Criminals have started to steal the files before they encrypt so they have another way of getting money, through blackmailing you, selling your secrets or both.



Denial of Service (DoS) - this is another way that criminals make money. They will bombard your website with so much traffic that your services become overwhelmed and stop working, meaning your customers can't see your site or use it. They want you to pay them to stop the attack.

Credential Stuffing - when a data breach occurs, criminals buy the usernames and passwords that have been stolen and then try them in other platforms, along with easy to guess passwords such as MyBusiness1.

Known vulnerabilities - it seems like new security issues are found every day in the software and hardware we all use. Criminals also know about these and will design attacks to specifically exploit that weakness.

Key Statistics

In 2021 there were 344 reports of cyber crime in the Eastern region costing a reported loss of £114,400

99% of vulnerabilities exploited will continue to be ones known by security and IT professionals for at least one year (Strategic Planning Assumptions (SPAs) by Gartner for security)

Using customer data to create personalized experiences can multiply return on investment by 5 to 8 times and can increase sales by 10% or more.

30.43% of attacks on retail are **Phishing attacks**

SecureLink found that 81% of malicious breaches start with **compromised passwords**.

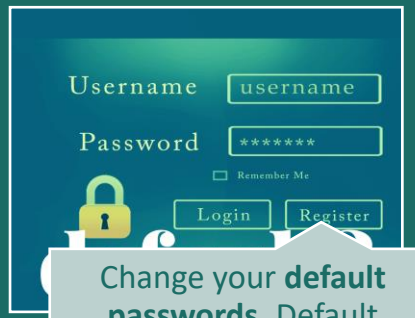
92% of malware is **delivered by email**

13.04% of attacks on retail are Ransomware

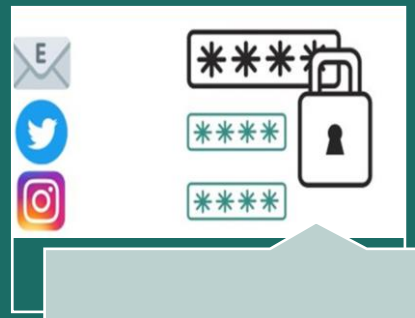
Top Tips

These fundamental security controls can prevent some of the most common cyber attacks.

Use **strong passwords** - they should be unique (not used anywhere else) and complex. Watch our short video for more information.

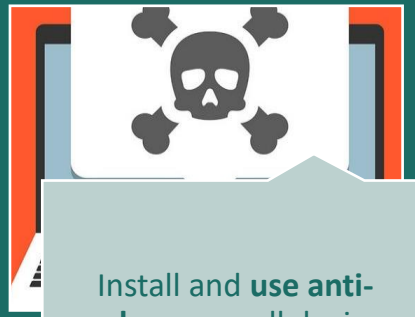


Change your **default passwords**. Default passwords are often publicly available so everyone may know them.



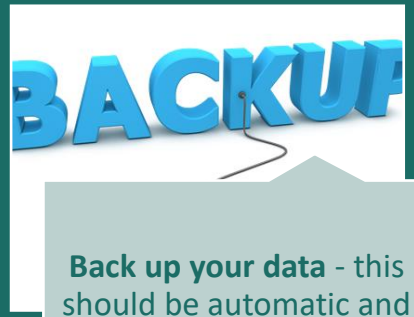
Use a **password manager** to help remember all your different passwords

Enable Two Factor Authorisation (2FA) wherever possible especially on your email, social media & where financial details are stored

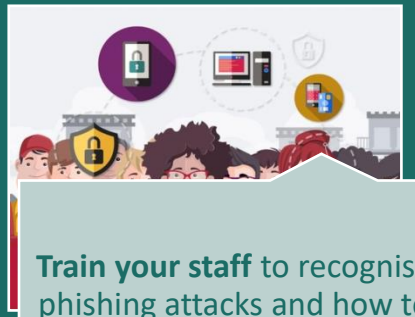


Install and **use anti-malware** on all devices

Install security updates as soon as possible on your applications, systems and devices



Back up your data - this should be automatic and offline



Train your staff to recognise phishing attacks and how to report them

Keep up to date with the latest guidance. Our free membership can help with this.

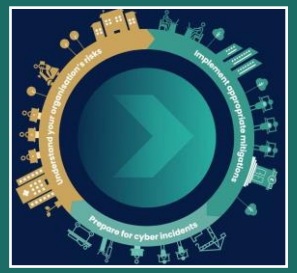
Tools

Cyber Action Plan

- Learn how to protect yourself or your small business online with the Cyber Aware Action Plan. Answer a few questions on topics like passwords and two-factor authentication, and get a free personalised list of actions that will help you improve your cyber security.

Small Business Guide

- An easy-to-understand guide with five key steps you can take to manage your cyber security risks.



10 Steps to Cyber Security

- Guidance is designed to help organisations protect themselves in cyberspace. It breaks down the task of defending your networks, systems and information into its essential components, providing advice on how to achieve the best possible security in each of these areas.

NCSC Board Toolkit

- Boards are pivotal in improving the cyber security of their organisations. The Board Toolkit has been designed to help board members get to grips with cyber security and know what questions they should be asking their technical experts.

Cyber Security Training for Staff

- Your staff are your first line of defence against a cyber attack. The NCSC has developed an e-learning training package 'Stay Safe Online: Top Tips for Staff' to help educate your staff on a range of key areas including phishing, using strong passwords, securing your devices and reporting incidents.

Incident Response Plan

- To help you minimise the impact of a cyber attack we have created a Cyber Incident Response Plan for you to use.

POLICE CYBERALARM

Police CyberAlarm

- Police CyberAlarm is a free tool to help your business understand and monitor malicious cyber activity. Police CyberAlarm acts like a "CCTV camera" monitoring the traffic seen by a member's connection to the internet. It will detect and provide regular reports of suspected malicious activity, enabling organisations to minimise their vulnerabilities.

Tools – NCSC Active Cyber Defence

The ACD programme seeks to reduce the harm from commodity cyber attacks by providing tools and services, free at the point of use, that protect against a range of cyber security threats. Tools include:

Self service checks (things you can sign up for and do)

- **Early Warning** – get notified of malicious activity that has been detected in information feeds.
- **Exercise in a Box** – test your response to a cyber attack through a toolkit of realistic scenarios

Detections deployed by organisations (things you can install)

- **Logging Made Easy** - a basic logging capability for routine end-to-end monitoring of Windows systems.
- **Protective Domain Name Service** - prevents users from accessing domains or IPs that are known to contain malicious content and stops malware already on a network from calling home.

Disrupt threats (how to report cyber criminals)

- **Suspicious Email Reporting Service** - report suspicious emails by sending them to report@phishing.gov.uk or installing an outlook add-in

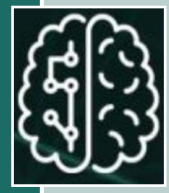
THE EASTERN CYBER RESILIENCE CENTRE

Affordable Services

We offer an affordable range of cyber security services designed to help businesses identify their vulnerabilities, assess current plans and policies and work with their teams to build their cyber awareness.

The ECRC partners with local academic institutions, such as Universities, to identify a pool of talented, reliable, students, who are then trained and mentored to enable them to deliver these services.

If you would like to find out more about our Cyber Security services and the associated costs, please contact the ECRC team.



Security Awareness Training - The training is focussed on those with little or no cyber security or technical knowledge and is delivered in small, succinct modules using real world examples.

Corporate Internet Investigation - This service may be used to learn what is being said on the internet about an organisation, what information employees are releasing or if there are any damaging news stories, social media posts or associations.

Individual Internet Investigation - The information gathered in this type of investigation might be used to support pre-employment checks, to manage potential threats to a Director of an organisation or their families, or to understand more about a specific person of interest.

Security Policy Review - This service offers a review of your current security policy, how it is written and how it is implemented.

Cyber Business Continuity Review - This service offers a review of your business continuity planning and the resilience of your organisation to cyber-attacks such as ransomware or when attackers take control of your core systems.

THE EASTERN CYBER RESILIENCE CENTRE

Affordable Services

Remote Vulnerability Assessment

Remote vulnerability assessments are focussed on identifying weaknesses in the way your organisation connects to the internet. Service reporting will provide a plain language interpretation of the results and how any vulnerabilities might be used by an attacker, as well as simple instructions on how any vulnerabilities might be fixed.

Internal Vulnerability Assessment

The service will scan and review your internal networks and systems looking for weaknesses such as poorly maintained or designed systems, insecure Wi-Fi networks, insecure access controls, or opportunities to access and steal sensitive data.

Web App Vulnerability Assessment

This service assesses your website and web services for weaknesses. The service reporting will describe in plain language, what each weakness means to your business and the risks associated with each. Service reporting will include plans and guidance on how to fix those weaknesses.

Partner Resource Support

Student resource will be used to fill temporary resource gaps, support extended resource requirements to support projects, or during incident response.

Contact Us

THE EASTERN CYBER RESILIENCE CENTRE

If you have found the information within our guide useful and would like to have more information on our services or guidance please contact us.

- Email: enquiries@ecrcentre.co.uk
- Tel: 01223 856020
- LinkedIn: /the-eastern-cyber-resilience-centre
- Facebook: /ECRCentre
- Twitter: /EasternCRC