National Cyber Security Centre
a part of GCHQ

How to Protect Your Business From Cyber Attacks

National Cyber Security Centre
a part of GCHQ

National Cyber Security Centre

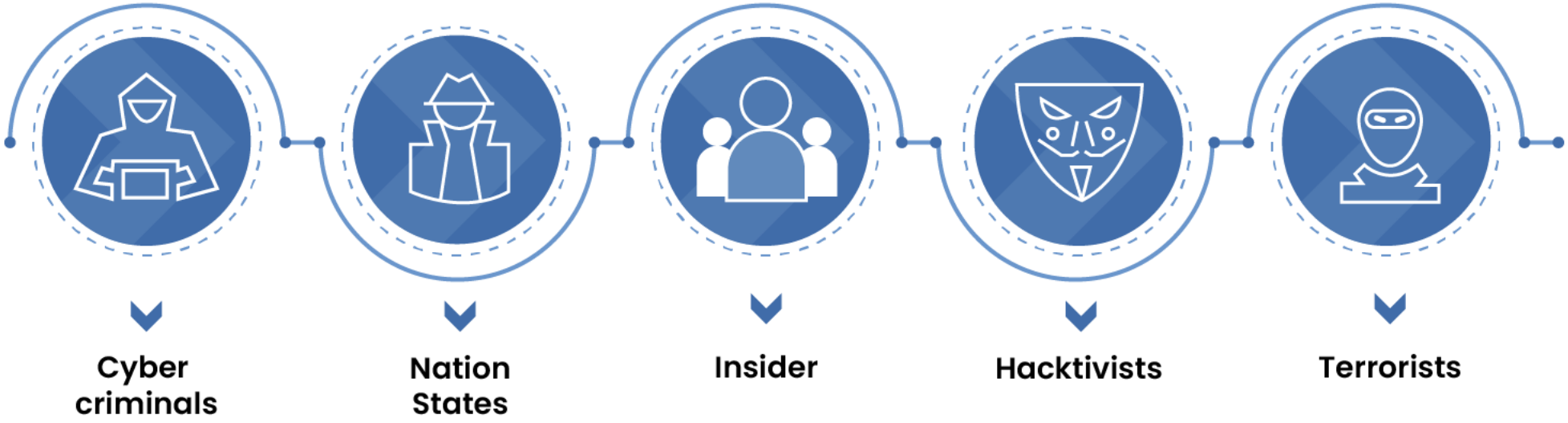
The National Cyber Security Centre (NCSC), a part of GCHQ, is the UK's technical authority for cyber threats.

Since the NCSC was created in 2016 as part of the Government's five-year National Cyber Security Strategy, it has worked to **make the UK the safest place to live and work online.**

National Cyber Security Centre
a part of GCHQ

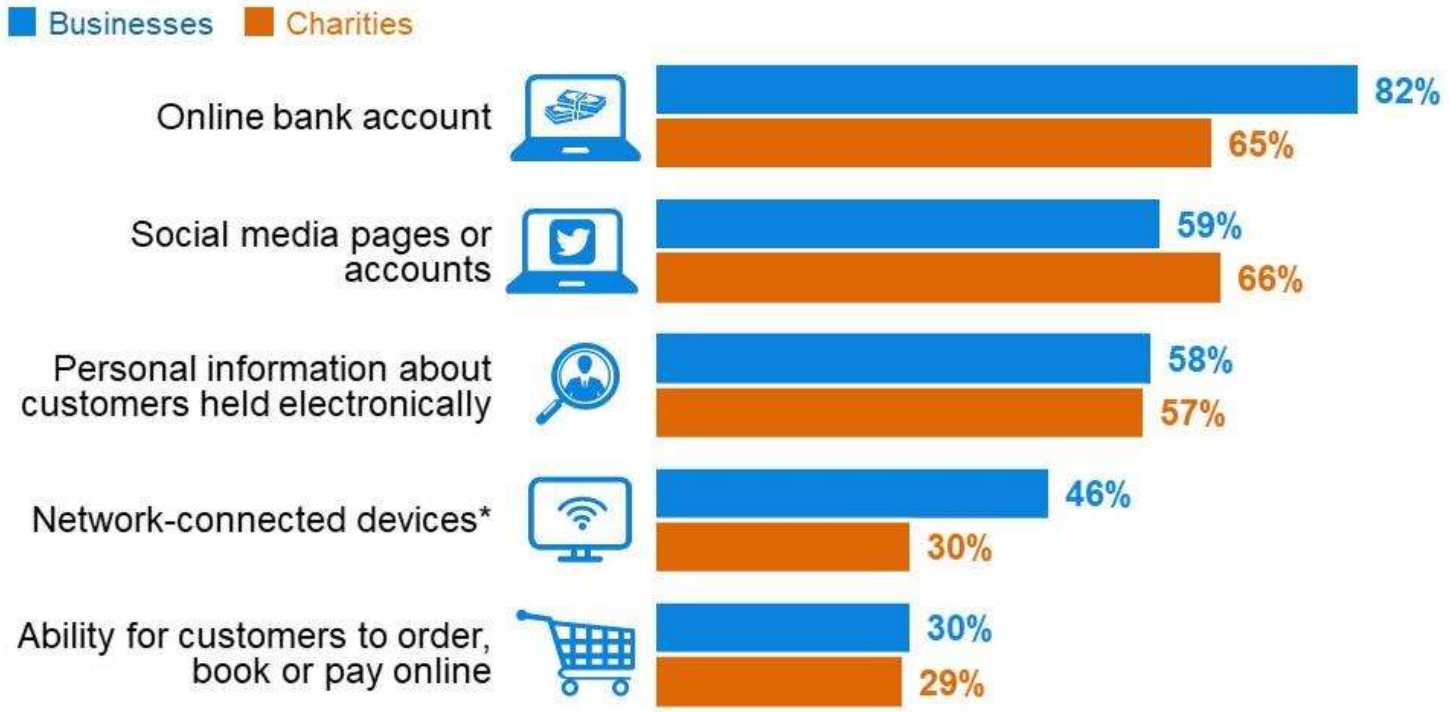
The Cyber Threat

The threats we face are on many fronts. From hostile state actors to organised criminal groups to terrorist organisations, cyber space offers a place to enact, enable or conceal malign actions to inflict considerable harm to our society, economy and national security.



National Cyber Security Centre
a part of GCHQ

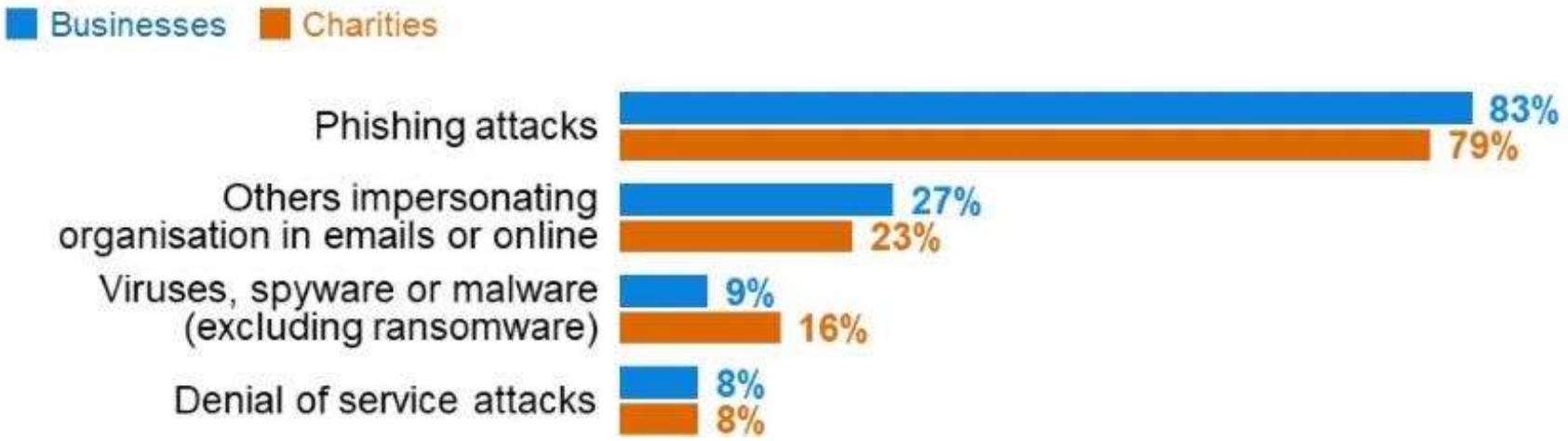
Cyber Breaches Survey 2021 – Digital Footprint



Bases: 1,419 UK businesses; 487 charities
*New codes added for 2021

National Cyber Security Centre
a part of GCHQ

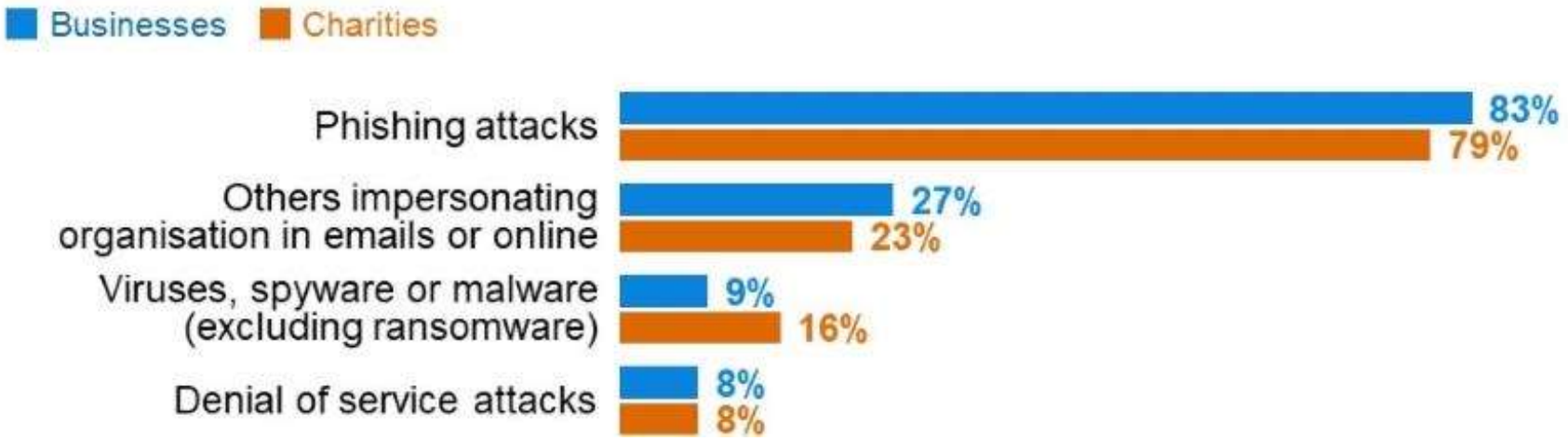
Cyber Breaches Survey 2021 – Breaches Identified



National Cyber Security Centre
a part of GCHQ

Cyber Breaches Survey 2021 – Breaches Identified

Staff vigilance is vital. The vast majority of breaches and attacks identified are ones that come via staff members' user accounts. If in doubt – call it out



National Cyber Security Centre
a part of GCHQ

Signs of a Phishing Email

- Poor spelling, grammar and punctuation
- Generic greeting
- A sense of urgency
- Offer of money or exclusive benefit
- Email from high-ranking persons within organisation, requesting a payment is made to a particular bank account

National Cyber Security Centre
a part of GCHQ

National Cyber Security Centre
a part of GCHQ

Case Study: Local County Council

The incident

- A member of staff opened a malicious attachment to email (zip file) at about 9.30am . Incident was not reported until midday.
- Increased activity on network file stores was identified and the true severity of the incident was recognised.
- A ransom demand was presented on screen ($500 bitcoins for each affected device). It encrypted files preventing access to the files it attacked.

The impact

- The email which introduced the malware spread to 300 users and over 47,300 files were encrypted by the time the shutdown was in place.
- Damage was limited by containment action.
- Staff were left with pens, paper and telephones, and business continuity plans were activated.

National Cyber Security Centre
a part of GCHQ

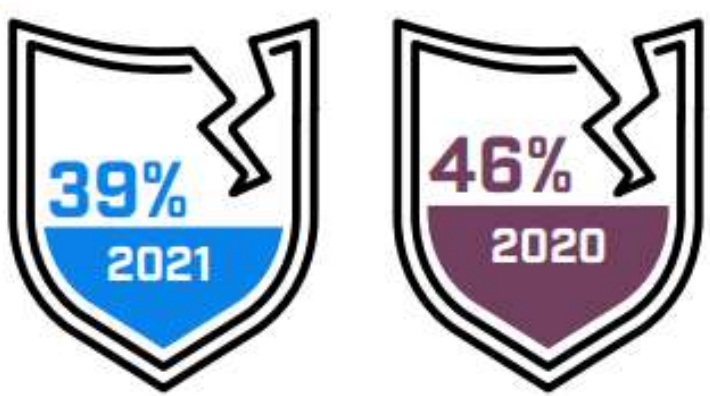
Business Impacts of a Cyber Incident

- Temporary loss of access to files or networks
- Websites, or online services, taken down or made slower
- Software or systems corrupted or damaged
- Money stolen
- Lost access to relied-third party services
- Damage to physical devices or equipment

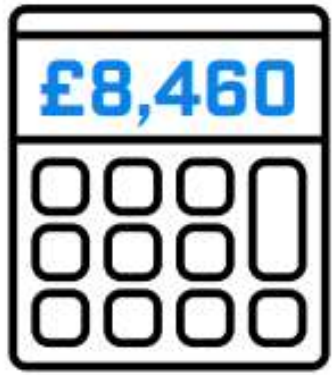
National Cyber Security Centre
a part of GCHQ

National Cyber Security Centre
a part of GCHQ

Financial Impacts of a Cyber Incident



of businesses identified cyber security breaches or attacks in the last 12 months **(down from 2020)**



is the average annual cost for businesses that lost data or assets after breaches

National Cyber Security Centre
a part of GCHQ

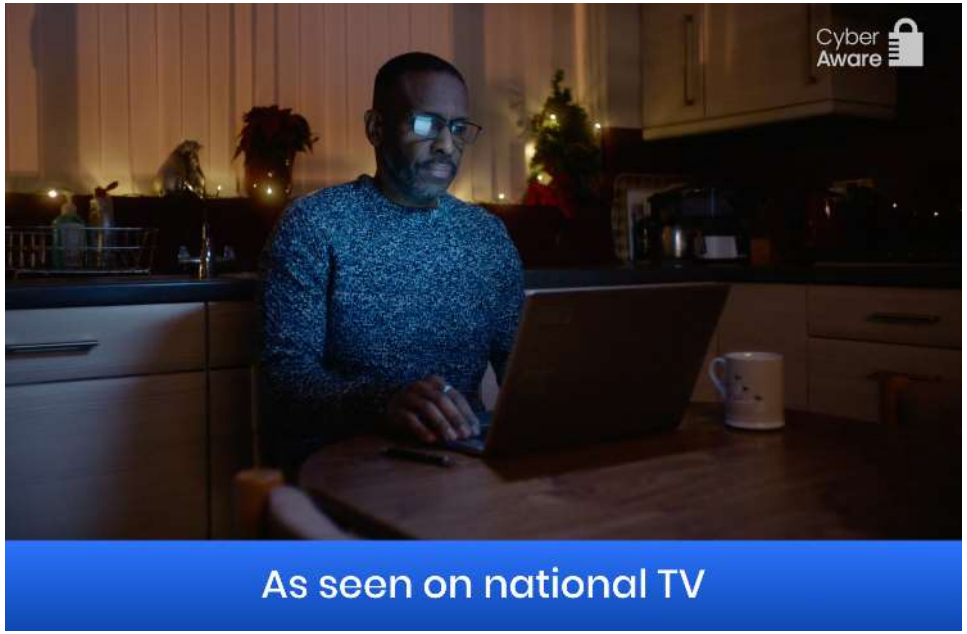
Financial Impacts of a Cyber Incident

	Short-Term Costs	Long-Term Costs
Direct Costs	• Cyber ransom and extortion costs • Financial theft • Staff response (overtime/contracting external staff)	• Loss of investors, donors or funding • Training costs (external resources) • Cyber security improvements
Indirect Costs	• Interruption of service • Lost, damaged or stolen outputs, data assets or property • Interruption of staffs' business as usual activities	• Reputational damage • Supply chain attrition • Loss of new and existing customers

National Cyber Security Centre
a part of GCHQ

Cyber Aware

Cyber Aware is the government's advice on how to stay secure online.



Cyber Aware

- Create a separate password for your email
- Create a strong password using three random words
- Save your passwords in your browser
- Turn on two-factor authentication
- Update your devices
- Turn on backup

National Cyber Security Centre
a part of GCHQ

Cyber Aware

Self-Assessment Tool

Answer a few questions and get a personalised list of actions to help protect you or your business online.

Get Your Cyber Action Plan

National Cyber Security Centre
a part of GCHQ

Small Business Guide

How to improve your cyber security; affordable, practical advice for businesses

- Backing up your data
- Protecting your organisation from malware
- Keeping your smartphones (and tablets) safe
- Using passwords to protect your data
- Avoiding phishing attacks

National Cyber Security Centre
a part of GCHQ

Response and Recovery Guide

Guidance to help business prepare their response to and plan their recovery from a cyber incident

- Prepare for incidents
- Identify what's happening
- Resolve the incident
- Report the incident to wider stakeholders
- Learn from the incident

National Cyber Security Centre
a part of GCHQ

Exercise in a box

An online tool which helps organisations find out how resilient they are to cyber attacks and practise their response in a safe environment.

Access EiB Service

NCSC Website using NCSC sign-on

Choose an Exercise

Guidance to choose effective exercises based on sector, objectives and resources available

Setup, Logistics & Planning

Follow guidance and instructions to setup, prepare and coordinate exercisest

Download supporting materials and resources

Exercise Delivery

Deliver exercise session to team that explore and evaluate readiness to respond to cyber security scenarios

Live exercise to detect and locate simulated cyber threat on an organisation's own IT estate

Discussions based exercise to explore an organisation's response to an unfolding business critical cyber security scenario

Post Exercise Activity

Reflective exercise with participants to identify challenges and opportunities

EiaB generates customised report detailing activities and outcomes to share with stakeholders

Link to associated NCSC guidance and resources

National Cyber Security Centre
a part of GCHQ

Cyber Essentials

Government backed scheme that will help you to protect your organisation

Certification gives you peace of mind that your defences will protect against the vast majority of common cyber attacks simply because these attacks are looking for targets which do not have the Cyber Essentials technical controls in place.

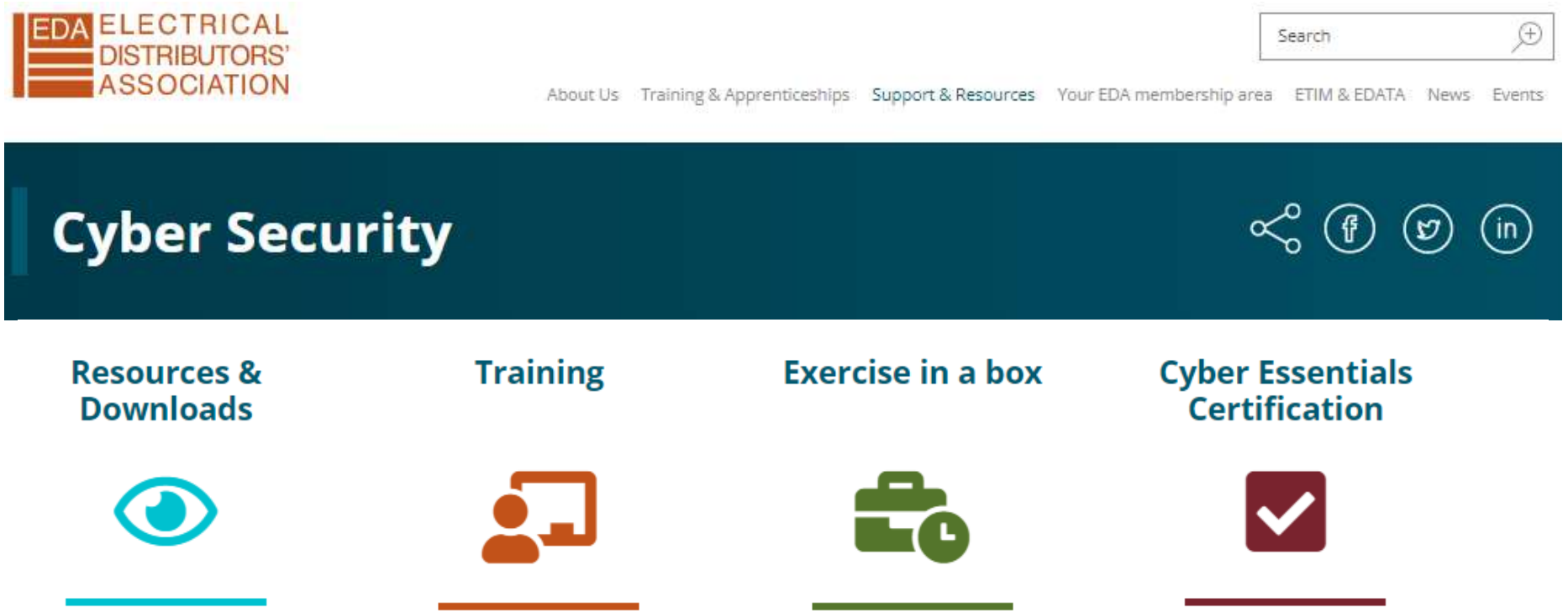
National Cyber Security Centre
a part of GCHQ

Small Organisation Newsletter

The Small Organisation Newsletter aims to break down cyber related issues into bitesize pieces which can be read in your coffee break.

We want to arm you and your business with the advice and tools to minimise the risk of a cyber-attack.

EDA Website – Cyber Security Resources



@NCSC

National Cyber Security Centre

CyberHQ