THE
CYBER
RESILIENCE
CENTRE
NETWORK

Fully Funded Cyber Support for Care Providers

What's available and how to access it

Delivered on behalf of the CRC Network by:
Paul Lopez, *Director*
Sapphire Little, *Business Development Manager*
Lucy Dover, *Business Development Assistant*

WWW.ECRCENTRE.CO.UK

Delivered in partnership with

CARE ENGLAND
The voice of care

The Care Provider ALLIANCE

Agenda

The current threats facing the care sector

Who we are – The Cyber Resilience Centre Network and how we can support you

How to access support and get in touch

Why care providers are being targeted

Fully funded tools and resources available from local policing and the National Cyber Security Centre

THE
CYBER
RESILIENCE
CENTRE
NETWORK

The current threats facing the care sector

From Phish to Fraud

Search on YouTube: "Cyber Resilience: A social care impact by the Welsh Government"

THE CYBER RESILIENCE CENTRE NETWORK

Understanding the Scale of the Problem

Key Facts

41% of health or care organisations fell victim to cybercrime in the last 12 months

The **most common** type of **cyberattack** was **phishing attempts (84%)**

Online Fraud and Cybercrime equates for **50% of all recorded crime** in England and Wales

75% of cyberattacks are committed outside the UK

A successful cyber security breach could result in costs of around £7k for micro/small businesses

39% of staff regularly use their own devices to store sensitive information

Stats from the UK Cyber Breaches Survey 2025, Digital Care Hub and The Department of Health and Social Care

Police-led**, Business**-focused

“Why would I be a target?”

Being a care provider doesn’t mean you're off the radar when it comes to cybercrime

- **If you're online, you're a target -** e.g., Email, Care records, Banking, Social media.
- **Cyber criminals exploit vulnerabilities -** not organisation size or sectors
- **The care sector is especially at risk due to:**
  - Shared devices
  - Limited time & resources
  - Sensitive data

Theft From a Motor Vehicle

- **Common 90s crime type** where criminals simply tried handles until they came to an unlocked car
- This is **very similar** to the way **cyber attacks** work
- It’s not **if** you get **cyber attacked**…it’s **when!**

THE
CYBER
RESILIENCE
CENTRE
NETWORK

Common scams and tactics used by cyber criminals

Common scams and tactics used by cyber criminals

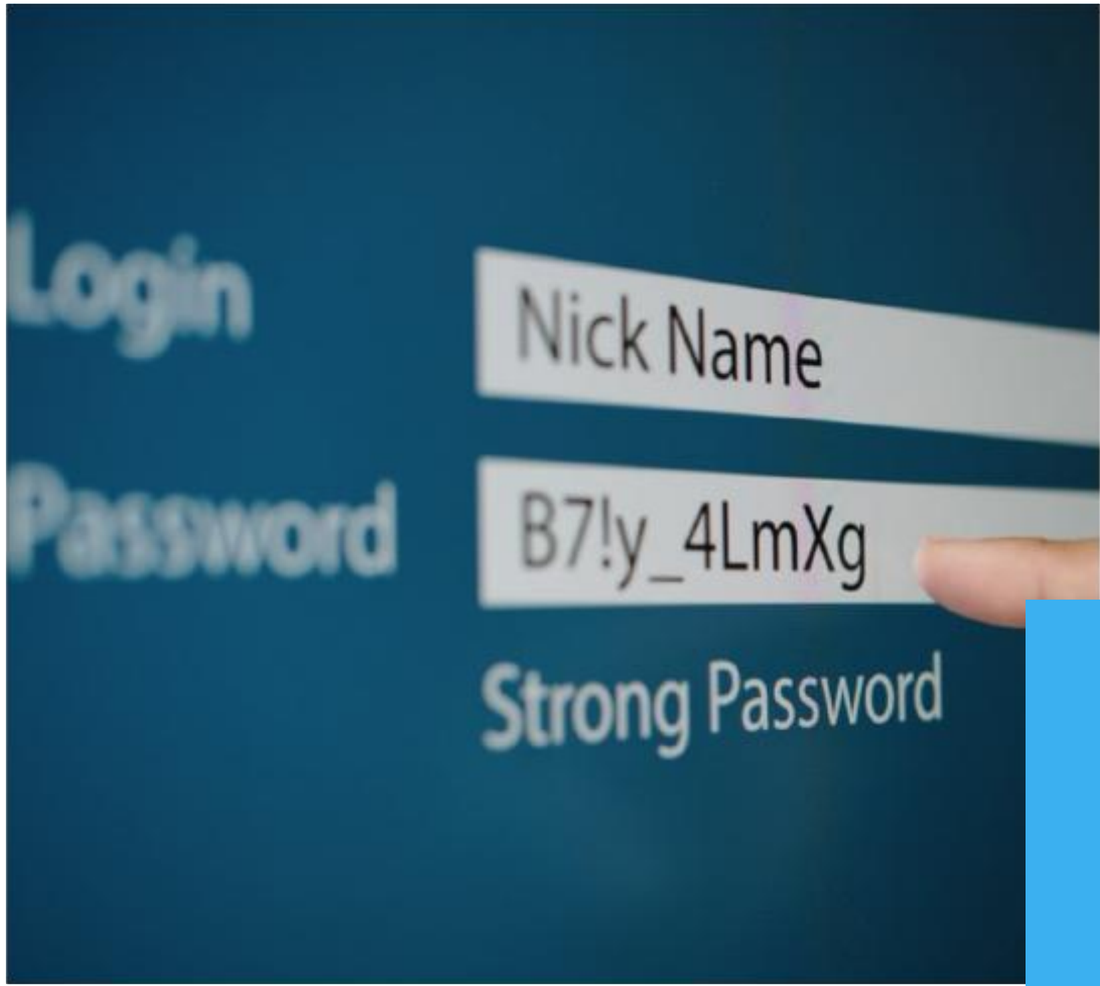
Phishing emails/Fake invoices scams

- Emails or invoices **look legitimate** — may use real logos, names, or email addresses
- **AI and design tools** make them easier to appear authentic
- Often sent **during busy periods** to distract staff and catch mistakes
- Criminals **research your organisation** using social media, websites, or company documents
- May create a sense of **urgency**: “Pay immediately” / “Final warning”
- Contain **malicious links or attachments** that steal credentials or install malware

Common scams and tactics used by cyber criminals

Stolen passwords/weak or reused passwords

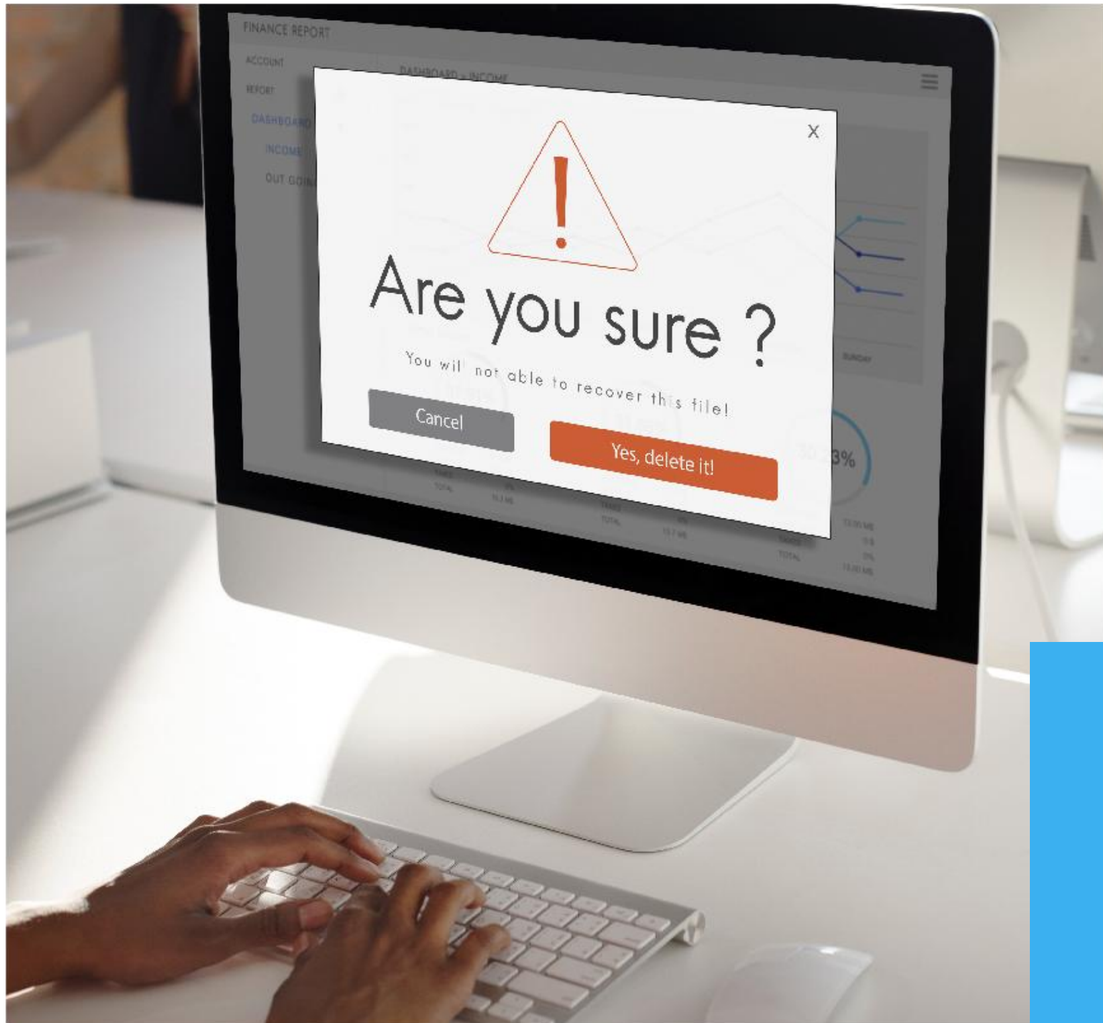
- Passwords can be **stolen by tricking you** into giving them away (phishing, fake IT requests)
- **Weak passwords** (e.g., “123456” or “Password1”) are easy to guess
- **Reused passwords** across multiple accounts increase risk - one breach can affect many systems
- Criminals may **research your company or personal info** to guess passwords
- Often targeted through **email prompts, fake login pages, or phone calls**



Common scams and tactics used by cyber criminals

Ransomware

- Ransomware is malicious software that **locks your files or devices** until a ransom is paid
- It can affect **computers, servers, or cloud accounts**
- Often starts from **a single click** on a phishing email or malicious attachment
- Criminals may **threaten deletion or leak of sensitive information** to pressure payment
- Can **disrupt care services, delay access to records, and increase stress** for staff



Example of a modern day phishing attack

REMEMBER: They are designed to get you to do something

SUBJECT: Outstanding Invoice for PPE Delivery — Please Pay
FROM: orders@caresupply-uk.com • TO: admin@rosewood-carehome.co.uk
Date: 09 Sep 2025

From: orders@caresupply-uk.com **To:** admin@rosewood-carehome.co.uk

Good morning,

Our records show an outstanding balance for the PPE order delivered to Rosewood Care Home on 28 Aug 2025.

Invoice: CS-2025-458
Amount due: £1,250.00

Please transfer the payment to the account below within 48 hours to avoid collection fees.

Payment details:
Account name: CareSupply UK Ltd
Account number: 12345678
Sort code: 00-11-22

Attached: CS-2025-458-invoice.pdf

If you believe this is an error, reply with a copy of your delivery note and we will investigate.

Kind regards,
Accounts Receivable
CareSupply UK Ltd
tel: 01632 960123

Grammar and spelling is no longer a clear indicator

Urgency – "this has to be done NOW!"

Mimicry – impersonation of individual or organisation

THE
CYBER
RESILIENCE
CENTRE
NETWORK

Top tips to help protect your organisation

How To Spot A Phishing Attack

REMEMBER: They are designed to get you to do something

- **Urgency –** “this has to be done NOW!”
- **Mimicry –** impersonation of individual or organisation
- **Curiosity –** “OMG! Have you seen this?”
- **Authority –** from CEO / senior member of staff

Things to check for:

- Go to **legitimate site** and **check information** rather than **clicking a link**
- **Confirm information** with person using **different communication method**
- **Review the URL** before clicking
- **Grammar** and spelling
- **Email address**

⚠ Always ask yourself “Is it too good to be true?”

What to do if you suspect phishing

How to report suspicious activity

- **Suspicious emails:** Forward to report@phishing.gov.uk
- **Suspicious texts**: Forward (free) to 7726
- **Suspicious websites:** Report at ncsc.gov.uk/report-scam-website

If you've shared information with a scammer – Remember:

- **Act fast by contacting** your bank, IT department, and Report Fraud
- **Early action minimises harm -** speaking up protects everyone
- **Sharing information** helps safeguard service users, colleagues, and yourself from cyber attacks

Recognising threats is a shared responsibility, not a test you can fail.

Use Strong Passwords

First line of defence against criminals or unauthorised people accessing your accounts

The stronger your password, the more protected your system will be

Time it takes a hacker to brute force your password in 2025

Hardware: 12 x RTX 5090 | Password hash: bcrypt (10)

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years

Hive Systems

Read more and download at hivesystems.com/password

NCSC guidance - Three Random Words

Take a memory and reduce it to three words	The **tree** fell down, **smashed** the fence and the dog **escaped**
Combine them in a random order	escapedsmashedtree
Add upper case letters	ESCAPEDsmashedTREE
Add special characters and numbers	ESCAPED100smashed!TREE

Enable Multi-factor authentication

- **Multi-factor authentication** - means using two or more pieces of information to prove it's really you, like a password and a code sent to your phone
- **Think of it like a chain/deadlock on your door** - even if someone has the key, they still need the second lock to get in

Types of 2SV Information

Knowledge	Possession	Inherence
Something you know	Something you have	Something you are
E.g. Password	E.g. Authenticator code	E.g. Biometrics

THE
CYBER
RESILIENCE
CENTRE
NETWORK

The Cyber Resilience Centre Network

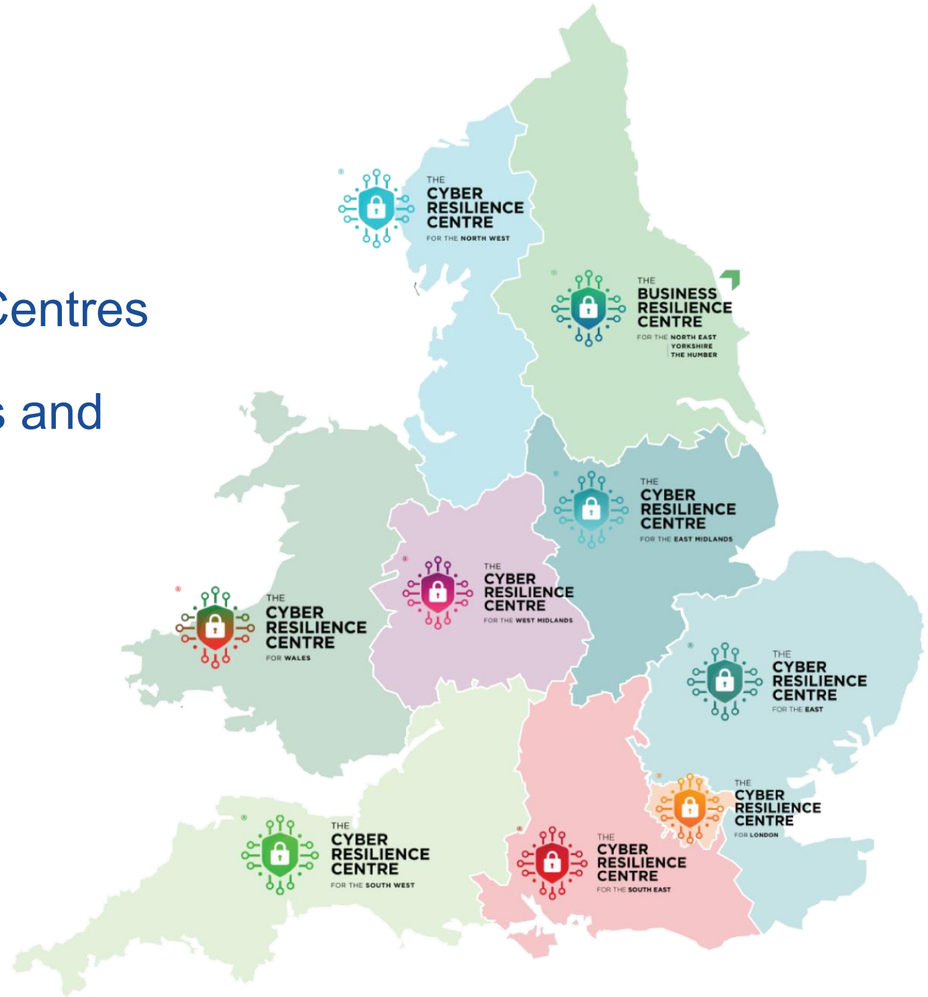
The CRC Network

Who we are

- **Police-led, government-funded** network of Cyber Resilience Centres
- **Working to support** small and medium organisations, charities and the third sector

How we can support your organisation

- **We offer a wide range of fully funded, interactive tools** and training resources to help build cyber awareness
- **These can be incorporated into** inductions, team meetings, and refresher courses



Our aim:

To increase the cyber resilience of small and medium businesses, charities and the third sector

THE CYBER RESILIENCE CENTRE NETWORK

The Support We Provide

Police-led, **Business**-focused

CRC Membership

Provides members with:

- **Regular newsletters and cyber awareness updates** featuring the latest guidance
- **Regional and national threat alerts** around the latest scams
- **Signposting to free tools and resources** from local policing and the NCSC
- **Access to a wide range of Cyber Security Services** via our Cyber PATH programme including training, vulnerability assessments, Microsoft 365 reviews etc

Scan the QR code to sign up

We operate across Bedfordshire, Cambridgeshire, Essex, Hertfordshire, Kent, Norfolk and Suffolk.

Cyber PATH Services

CYBER PATH™
POLICE & ACADEMIA TALENT HORIZONS

Security Awareness Training
Staff training for those with little or no cyber security or technical knowledge

Microsoft 365 Service
Reviews your Microsoft 365 configuration to identify any flaws in your organisation's set up.

First Step Web Assessment
Provides you with an initial assessment of your website to highlight its most pressing vulnerabilities

Cyber Business Continuity Review
A thorough review of your business continuity plan and overall resilience to cyber attacks

Sign up for our next webinar to explore fully funded support and other services we provide

Remember

THE CYBER RESILIENCE CENTRE NETWORK

Phishing remains the most common cyber-attack

The key is regular training and a healthy cyber awareness culture. Encourage reporting, always be extra cautious, and double-check information with someone else.

Review your passwords and enable MFA across your account and devices

Especially on your email and social media accounts – remember MFA is like a deadlock on your front door!

Book a 1-to-1 and sign up for our support

To continue to receive the latest police guidance around cyber crime and access a wealth of resources.

Book a 1-to-1 session with us today

Discuss anything we've covered in more detail and take your first step towards cyber resilience

Delivered in partnership with

CARE ENGLAND
The voice of care

The Care Provider ALLIANCE