



THE
**EASTERN
CYBER
RESILIENCE
CENTRE**

Cyber Fundamentals

DI Fiona Bail - Head of Cyber and Innovation, ECRC

Welcome

- ▶ Introductions - Eastern Cyber Resilience Centre - what we do and why
- ▶ What you can do to increase your cyber resilience

Aim:
To get you thinking about cyber and what you can do to build your resilience



What are the CRCs?

- Home Office supported project
- Collaboration between Policing, Industry Experts and Academia
- Not for Profit Limited company
- Membership focussed - with free of charge membership

Aim:

To increase the cyber resilience of Small and Medium businesses



THE
**CYBER
RESILIENCE
CENTRE**
FOR THE SOUTH WEST



THE
**CYBER
RESILIENCE
CENTRE**
FOR THE WEST MIDLANDS



THE
**CYBER
RESILIENCE
CENTRE**
FOR WALES



THE
**CYBER
RESILIENCE
CENTRE**
FOR GREATER MANCHESTER



THE
**BUSINESS
RESILIENCE
CENTRE**
FOR THE NORTH EAST



THE
**CYBER
RESILIENCE
CENTRE**
FOR THE EAST MIDLANDS



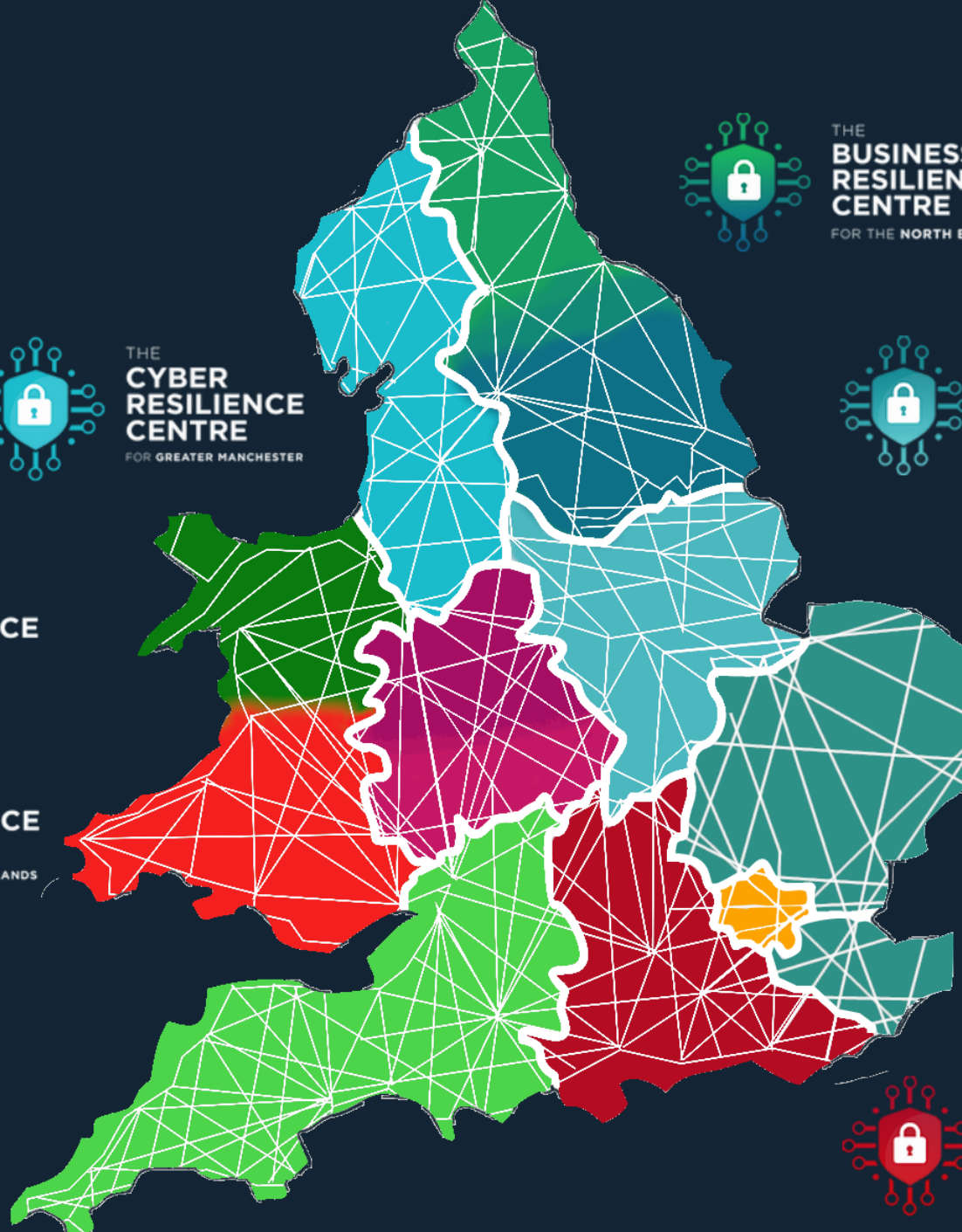
THE
**EASTERN
CYBER
RESILIENCE
CENTRE**



THE
**CYBER
RESILIENCE
CENTRE**
FOR LONDON



THE
**CYBER
RESILIENCE
CENTRE**
FOR THE SOUTH EAST



Why has the ECRC been set up?

Cybercrime is increasing

1.5 million organisations fell victim to cyber crime in 2019 (Beaming's five years in cyber security)

25% of all UK businesses and an increase from the 13% in 2015

The est. cost of cyber crime to the UK business - £21bn per year
(Detica report, Office of Cyber Security and Information Assurance, Cabinet office)

32,259 reports
£11.6M reported losses
(Action Fraud)

Most cybercrime is for one thing - MONEY, either directly (theft) or indirectly (ransomware, selling data)

“Why would I be a target”

Online = target

Cyber criminals look for vulnerabilities

If businesses do realise they are a target, they are unsure about where to start or who to trust.

The ECRC is that starting point, with our free of charge membership, to get businesses started on their cyber resilience journey.

43% of SMBs lack any type of Cyber Resilience Plan

1 Small Business in the UK is successfully hacked every 19 seconds

Hackers target **VULNERABILITIES** not organisation size

4 in 10 SMEs say they would struggle to recover from data loss.

1 in 4 SMEs admit they wouldn't be able to recover any data.

41% of UK consumers claim they will never return to a business after a data breach

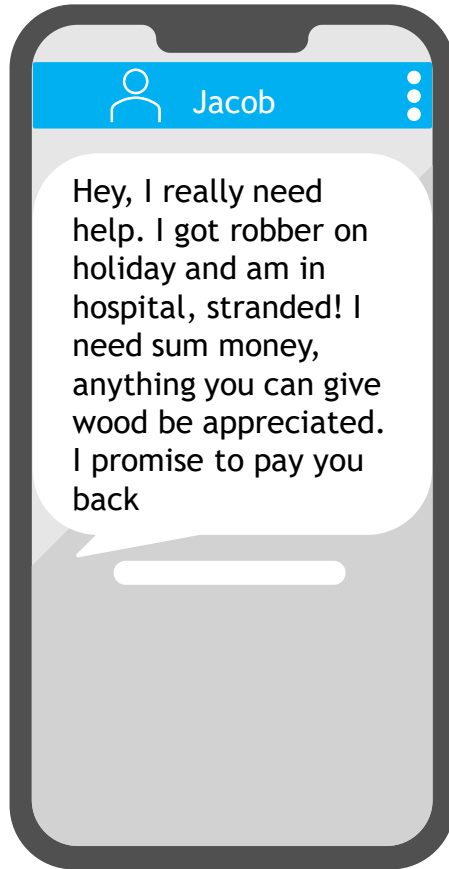
Local Threats

Hacking - Social
media and
email

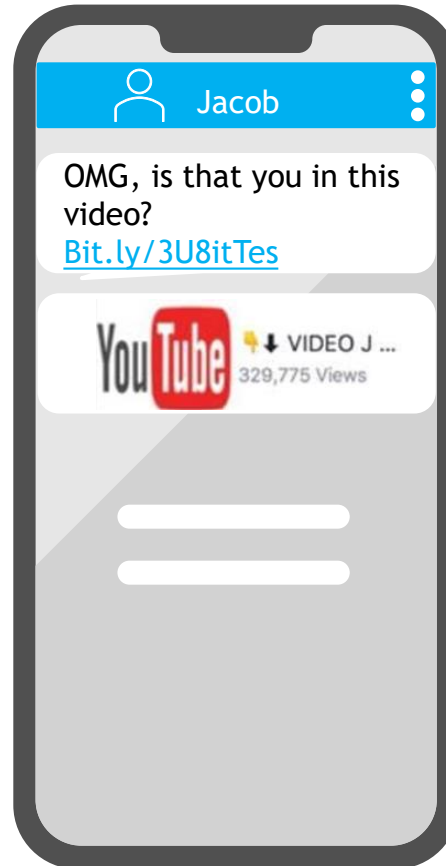
Business Email
Compromise

Phishing / Social
Engineering /
Impersonation

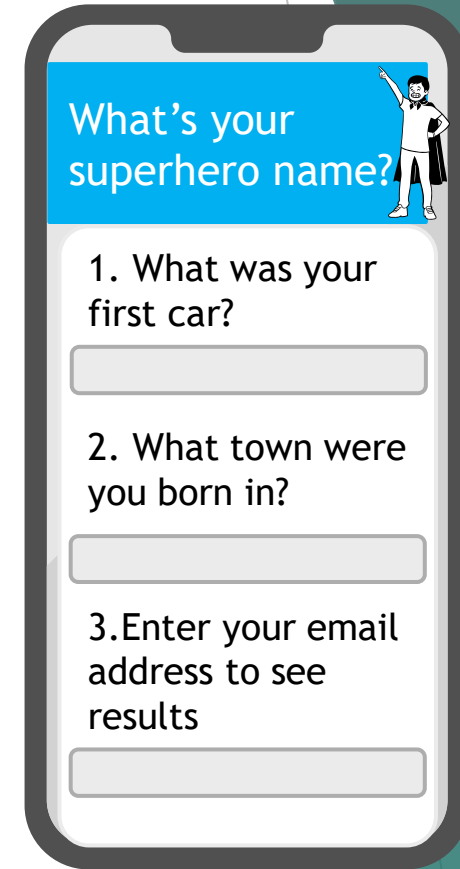
Social media examples



I need help!



Click bait

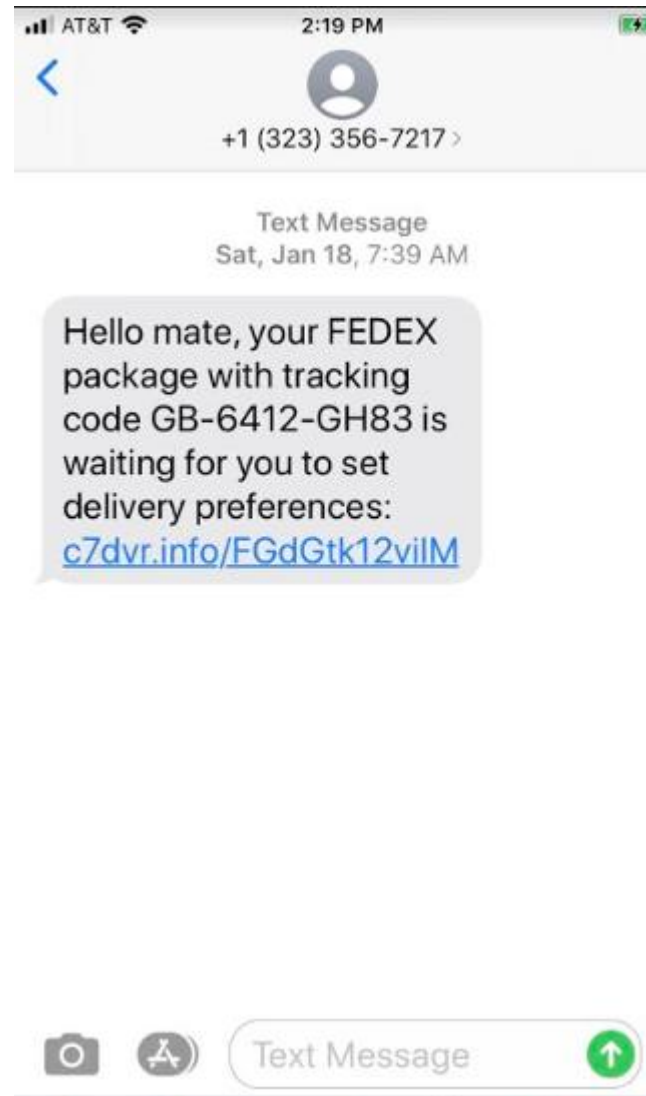


Quizzes

Smishing example

HSBC: A payment was attempted from a NEW DEVICE on 27/07 at 14:27PM. If this was NOT you, please visit:
<https://hsbc.co.uk.securitykpi.com/hsbc>

There is an update on your parcel. Item stopped due to unpaid customs fee. Follow the instructions here: [z\)\)0yT4ScvT](https://z))0yT4ScvT)



Vishing example



Ways to spot a phish

Designed to get you to do something

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

Things to check for

- ▶ Grammar and spelling
- ▶ Email address
- ▶ Hypertext - review url before clicking
- ▶ Go to legitimate site and check information rather than clicking a link
- ▶ Confirm information with person using different communication method
- ▶ Is it too good to be true?

Protocol

https://ecrcentre.co.uk/news

Domain

Directory

http://ecrcentre.co.uk/news

What can you do to protect you and your family?

Use Strong Passwords

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

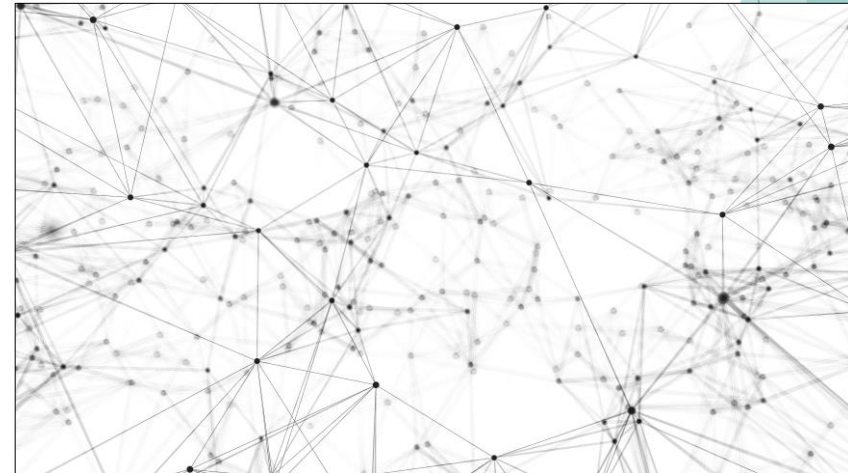
The stronger your password, the more protected your system will be.

Passwords = digital key - what type of key do you want?



What does a strong password look like?

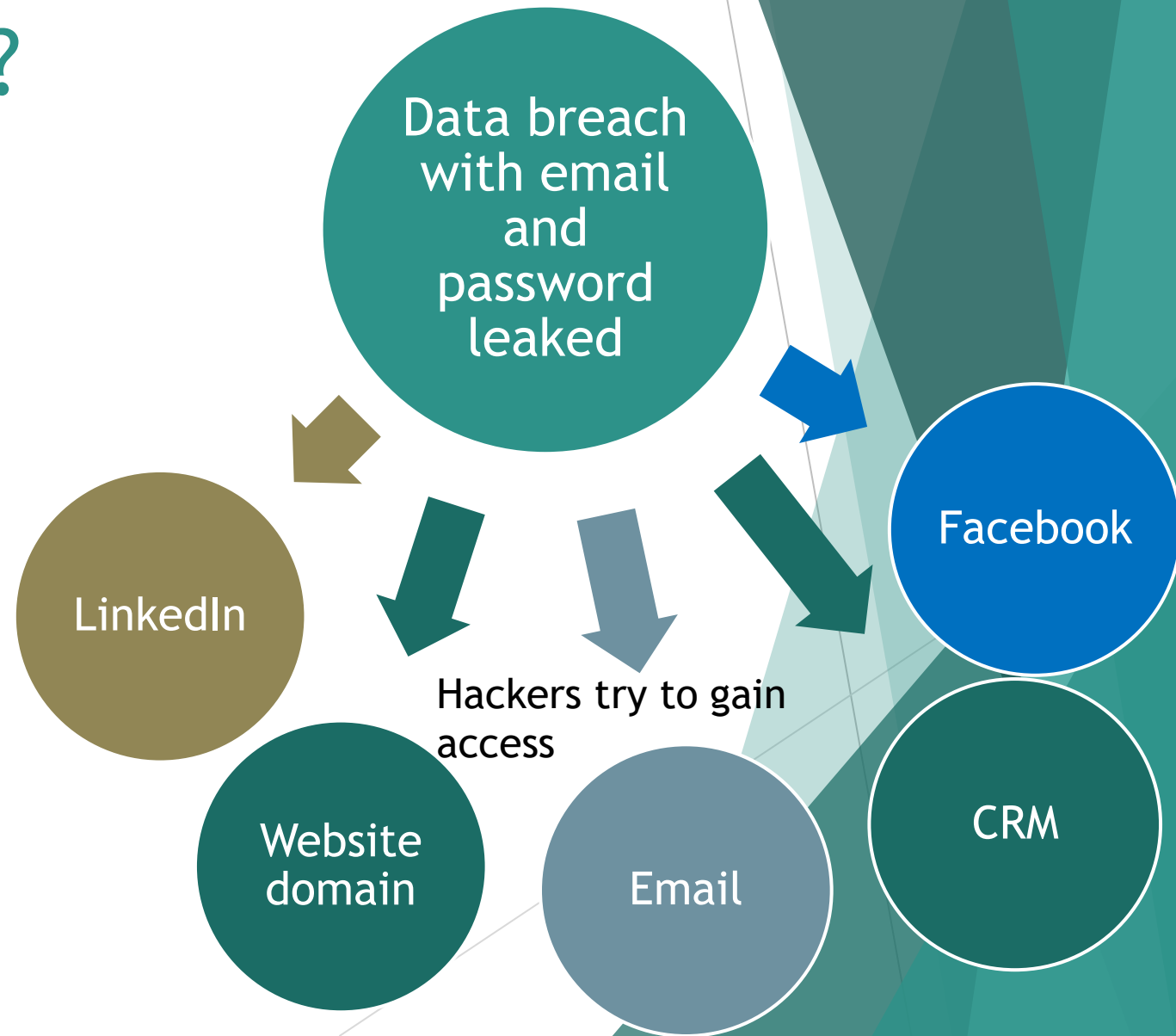
Un**i**q**u**e and **C**O**m**P**l**e**x**!



Why is using the same passwords problem?

A lot of people use the **same password** for all their accounts and use work details for personal accounts.

If their password is leaked in a data breach, then criminals can use that information to try and **gain access to all other accounts**.



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

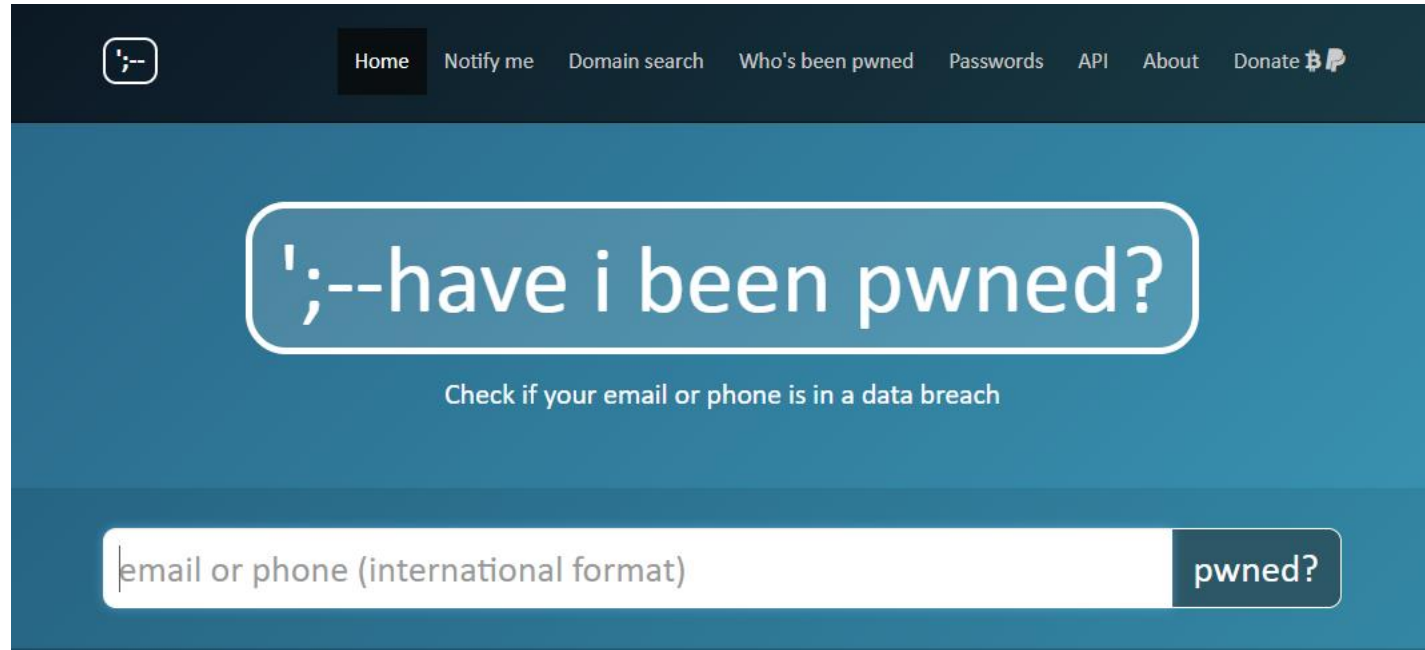
Add special characters and numbers

- ESCAPED100smashed!TREE

What is your
current

▶ compromise?

www.haveibeenpwned.com



The screenshot shows the homepage of the website. At the top, there is a dark navigation bar with a logo on the left and several menu items: Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate with a Bitcoin icon. The main content area has a blue background. In the center, there is a large white rounded rectangle containing the text ';--have i been pwned?'. Below this, a smaller line of text reads 'Check if your email or phone is in a data breach'. At the bottom, there is a search input field with the placeholder text 'email or phone (international format)' and a dark button labeled 'pwned?' to its right.

Home Notify me Domain search Who's been pwned Passwords API About Donate ₿

';--have i been pwned?

Check if your email or phone is in a data breach

email or phone (international format) pwned?

Enable 2FA (2 Factor Authentication)

(aka Multi-Factor
Authentication or 2 Step
Verification)



Passwords can only provide so much protection for your accounts.



Your password could be stolen via:

- Data Breach
- Using malware from your phone, tablet or laptop, or
- You could be tricked into revealing them (via phishing)



2FA prevents access to your accounts because they don't have

- the “something you have” or
- the “something you are”

What is 2FA/2SV or MFA?

Two Factor Authentication / Two Step Verification - you provide two pieces of information to prove who you are

Multi-Factor Authentication - you provide two or more pieces of information

Types of Information

Knowledge

Something you know

Password

Possession

Something you have

Authenticator code

Inherence

Something you are

Biometrics

What should
you do?

Identify and set up 2FA/MFA on all your important
accounts

Email

Social media

Any financial, banking or investment accounts

Apple ID and Google Play

Gaming accounts

Retails shopping accounts

Subscription accounts

Password and Identity management accounts

Government accounts

Why do I need 2FA on my email address?



Enter your email and we'll send you a link to reset your password.

Reset Password

Create your 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.

**For sole traders & small
businesses**

Takes 3-5 mins

[Start now](#)

For individuals & families

Takes 3-5 mins

[Start now](#)

Understand your current cyber resilience

<https://www.ncsc.gov.uk/cyberaware/actionplan>

How the ECRC can help?



CRC Membership

Free community for businesses

Provides members with:

- ▶ Access to national **guidance** on cyber resilience, free online **resources** and **toolkits**, **affordable services**
- ▶ Regular updates from the ECRC team including the latest information about **emerging threats** in our region.
- ▶ **Contact** from a member of the ECRC to discuss your current cyber resilience and discuss areas to consider.
- ▶ A “**little steps**” journey - receive one email a week about one cyber resilience consideration.



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.

[Find Out More](#)



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.

[Find Out More](#)



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.

[Find Out More](#)



Knowledge & Protection

- We coordinate cyber risk and protection information between policing and business
- We help business understand what's relevant to them
- We help you access NCSC free resources

[HOW WE DO IT](#)



Membership

- We provide regular e-updates
- We deliver affordable testing and training services
- We are a place to find trusted and accredited suppliers

[HOW WE DO IT](#)



Skills & Talent

- We provide real world experience for emerging university cyber talent
- We develop real world commercial skills for students
- We provide transferrable skills opportunity for veterans

[HOW WE DO IT](#)



Security Policy Review

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

[Find Out More](#)



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.

[Find Out More](#)



Partner Resource Support

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

[Find Out More](#)



Remember



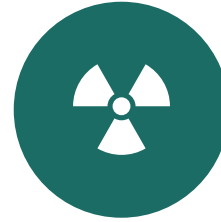
DON'T USE THE
SAME PASSWORD
ACROSS MULTIPLE
ACCOUNTS



MAKE YOUR
PASSWORDS
COMPLEX - USE 3
RANDOM WORDS
OR A PASSWORD
MANAGER



ENABLE 2FA ON
ANY IMPORTANT
ACCOUNT
ESPECIALLY EMAIL
AND SOCIAL MEDIA



VISIT -
HAVEIBEENPWNED
.COM



DO THE NCSC
ACTION PLAN

Thank you for listening

Any questions?

DI Fiona Bail - Fiona.bail@ecrcentre.co.uk

<https://www.ecrcentre.co.uk>

<https://www.linkedin.com/company/the-cyber-resilience-centre-for-the-east>

<https://twitter.com/EasternCRC>

Links

Reporting a suspicious website - <https://www.ncsc.gov.uk/section/about-this-website/report-scam-website>.

Reporting a suspicious email - forward to report@phishing.gov.uk

Reporting a suspicious text message – send to 7726

Check your compromise – www.haveibeenpwned.com

Cyber Action Plan - www.ncsc.gov.uk/cyberaware/actionplan