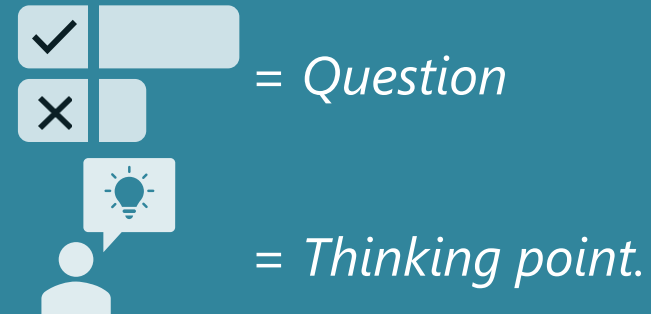


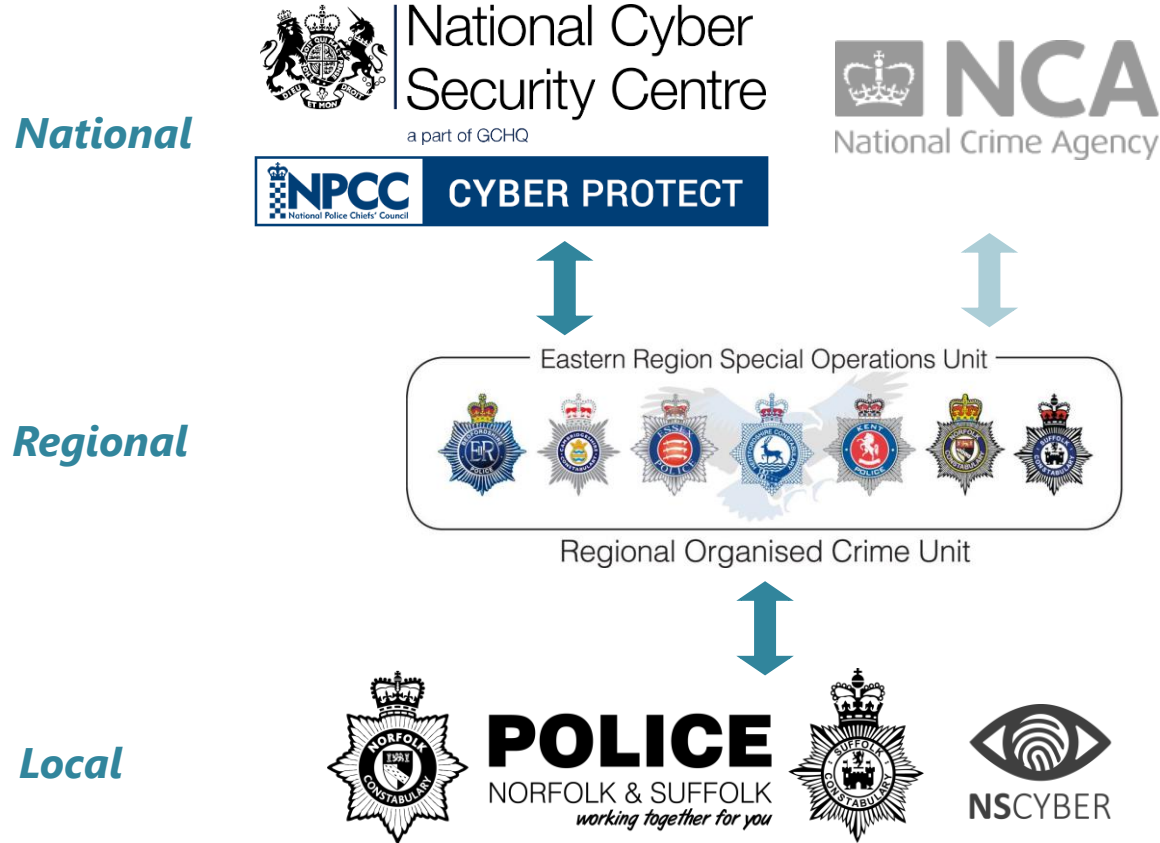
Protecting yourself and others from cybercrime and scams

Cyber Security Advisor - John Greenwood

John.Greenwood@Suffolk.police.uk



National Cyber Security Strategy



Cyber *dependent* crimes

- Pursue – Investigation
- **Protect** - Increase Defence
- *CHOICES* - Stop Involvement
- **Prepare** - Increase Resilience

Cyber Enabled

- 'traditional crimes', which can be increased in their scale or efficiency by use of computers / ICT
- *Fraud / Credit card theft*
- *Investment Scams*
- *Romance Scams*

Cyber Dependent

- Offences that can only be committed using a computer / ICT
- *Malware (viruses, ransomware)*
- *Hacking*



National Cyber
Security Centre

a part of GCHQ

- The NCSC is the single point of contact for individuals and organisations of all sizes in relation to cyber security



FILTERS

Use the following to filter the dashboard elements to a specific type of crime, crime code, grouped category, region, Police Force, date or type of victim.

Cyber Crime

No Filter Selected

Grouped Crime Category

No Filter Selected

Region

Eastern

Police Force

Norfolk

Filter by year

2020

Manual data selector

Type of Victim

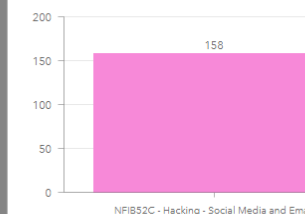
No filter selected Individual Organisation

NUMBER OF REPORTS

316

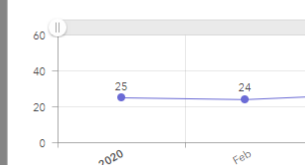
Last update: a few seconds ago

TOP 5 REPORTED CRIME CODES



MONTHLY REPORTING VOLUMES

If you hover over the data points, the month will show



Start to filter data if no data is appearing

REPORTED LOSSES

£53.6K

Last update: a few seconds ago

Norfolk Stats...

NFIB Fraud and Cyber Crime Dashboard - 13 months of data

FILTERS

Use the following to filter the dashboard elements to a specific type of crime, crime code, grouped category, region, Police Force, date or type of victim.

Fraud

No Filter Selected

Grouped Crime Category

No Filter Selected

Region

Eastern

Police Force

Norfolk

Filter by year

2020

Manual data selector

1/1/2020

12/31/2020

Type of Victim

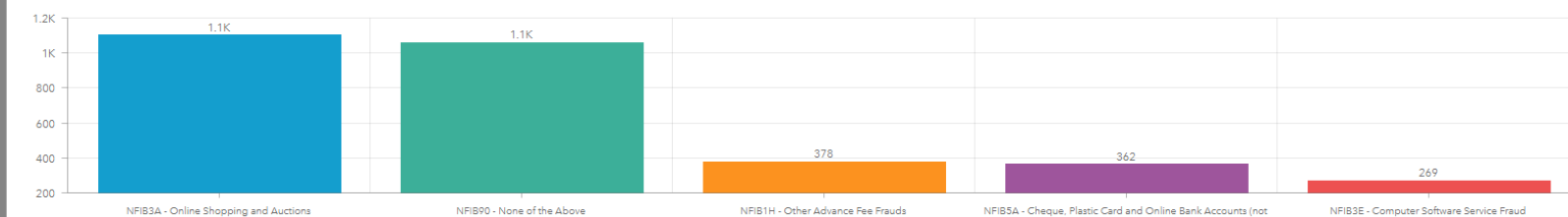
No filter selected Individual Organisation

NUMBER OF REPORTS

4,302

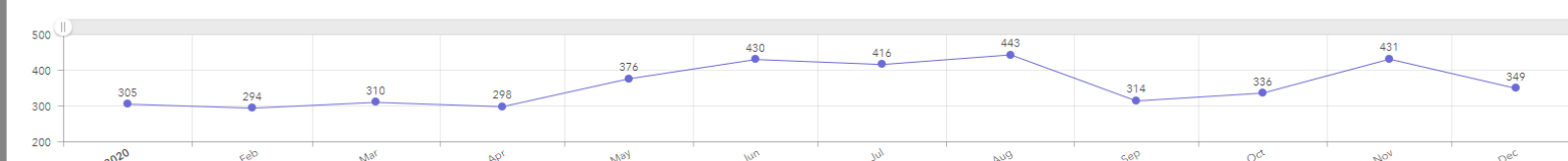
Last update: a few seconds ago

TOP 5 REPORTED CRIME CODES



MONTHLY REPORTING VOLUMES

If you hover over the data points, the month will show in the American date format currently. Use the slide bar at the top of the chart to zoom in and out.



Start to filter data if no data is appearing

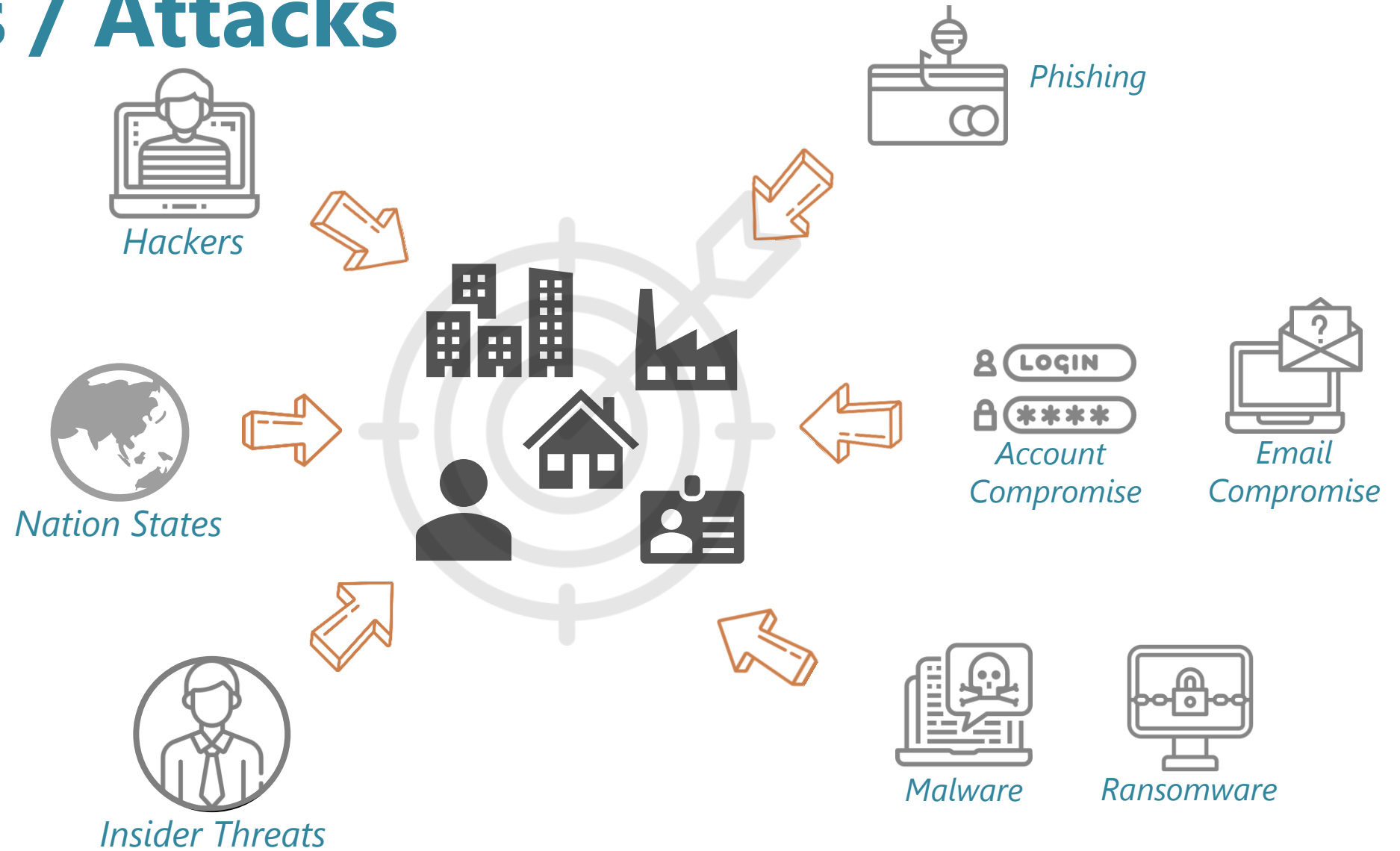
Last update: a few seconds ago



PROTECTIVE SERVICES | CYBER, INTELLIGENCE AND SERIOUS CRIME



Attackers / Attacks





- Phishing
- Account/ service compromise



STAPLETON
ROAD S.W.

JOHN DEAN
020 8677 8835

The walker wyatt coffee shop

coffee



Take Control Of Your Online Presence

- Avoid posting specific information about your organisation or role
- What does your social media say about you?
- Check your privacy settings on social media
- Register for data breach notifications '--have i been pwned?'
- Do you need location data enabled?
- Google yourself

Social engineering

- Attackers attempt to trick users into doing 'the wrong thing'

"98% of cyber attacks rely on social engineering." [2021 Cyber Trends PurpleSec](#)

"Criminals don't hack in, they log in." Detective Inspector David Parkin (ret)

Phishing



SMShing



Vishing



Phishing - General



- Disguise themselves as a trustworthy entity
 - Aim is to make the user click a bad link or give away sensitive information
-
- *Could contain legitimate links*
 - *Image of text to trick filters*
 - *Email addresses / web domains with typos are used*
 - *Link to fake site which is used to harvest details*
- *Sense of urgency / threats*
 - *Link to cloud documents*
 - *Numbers can be spoofed*
 - *Could come from a friend / colleague*



Have you received a phishing email to your email account this year?



In April (2020) Google (1.5 billion users) blocked 100 million phishing emails per day, a fifth of which related to COVID-19. ([BBC](#))



Whaling

- Targets high-level decision makers

Could be from:

- *compromised internal account*

Potentially followed up with call

Spear phishing

- Personalised to their targets

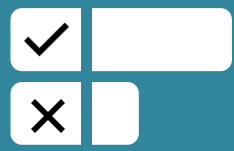
Targeted

Research Required

Personalised so more believable

Phishing

- Emails sent en masse





If a website has a padlock in the URL bar
is it trustworthy?



secure.accountinforming.com ×
Your connection to this site is private.


Permissions **Connection**

 The identity of this website has been verified by GeoTrust DV SSL CA - G4. No Certificate Transparency information was supplied by the server.
[Certificate information](#)

 Your connection to secure.accountinforming.com is encrypted using a modern cipher suite.

The connection uses TLS 1.2.

The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_RSA as the key exchange mechanism.

 **Site information**
You have never visited this site before today.

[What do these mean?](#)



Log in to your account

Email address

Password

Log In

[Forgot your email address or password?](#)

Sign Up for Free

All in one pay.

Pick a card, any card, or bank account. It's your money, you choose how to spend it.

Simple. And no hidden costs.

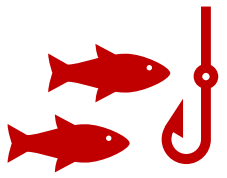
It's free to sign up for a PayPal account, and we don't charge you a transaction fee when you buy something, no matter how you choose to pay.

[About Us](#) | [Contact Us](#) | [Fees](#) | [Merchant Services](#) | [Worldwide](#)

[Privacy](#) | [Our Blog](#) | [Jobs](#) | [Legal Agreements](#) | [eBay](#)

Copyright © 1999-2015 PayPal. All rights reserved.
Consumer advisory- PayPal Pte. Ltd., the holder of PayPal's stored value facility, does not require the approval of the Monetary Authority of Singapore. Users are advised to read the Terms and Conditions carefully.

Reel or Phish..



[Account-Deactivation]



Microsoft Fix <mx-59545445435@protection.office-365.com>

Tuesday, August 21, 2018 at 1:18 AM

[Show Details](#)

Office-365

Hi Sales

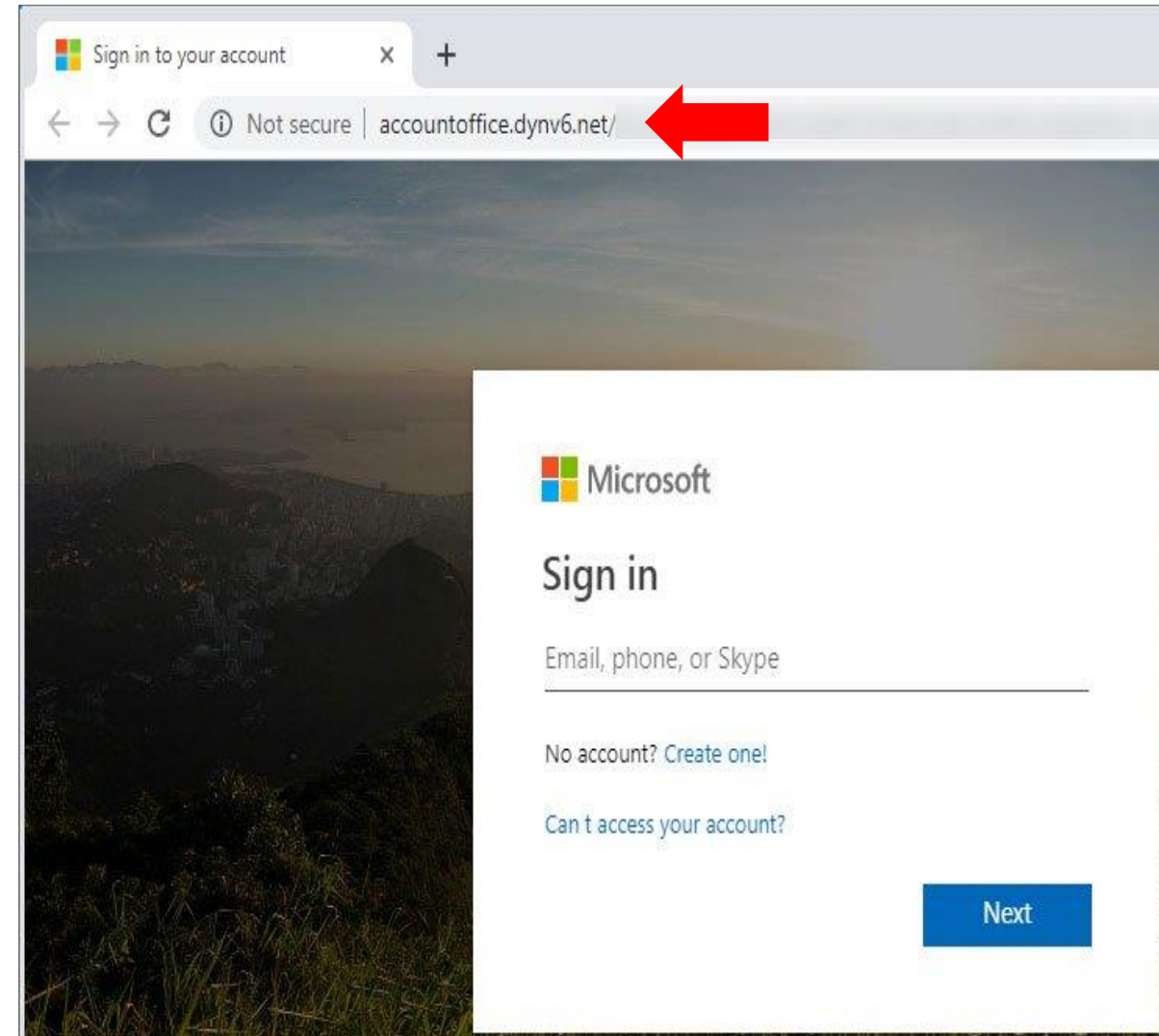
Your account of [redacted] .com will be disconnected from sending or receiving mails from other users. because you failed to resolve errors on your mail.

You need to resolve the errors or your account will be disconnected from [redacted] .com.
Follow the instruction below to resolve now.

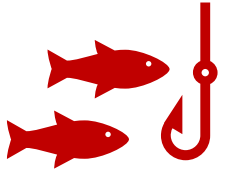
[RESOLVE ISSUE NOW](#)

Regards,
Microsoft Security Team

This notification was sent to [redacted] .com of Microsoft.com.



Reel or Phish..



NHS: We have identified that you are eligible to apply for your vaccine. For more information and to apply, follow here : uk-application-form.com



Carlisle ex-police officer 'devastated' by £3k Royal Mail scam

🕒 7 April

He had fallen prey to a scam text message that claimed a parcel was awaiting delivery.

Royal Mail has confirmed it would never send such a text message.

Victims receive a text purporting to be from the company which reads: "Your Royal Mail parcel is awaiting delivery. Please confirm the settlement of 1.99 (GBP) on the following link".

The message then links to a website mocked up to look like an official site.

The page requests personal and payment details, which fraudsters use to steal the victim's identity or target them with further scams.

Techniques ➔

Criminal Gain ➔

➔ **SMShing**

➔ **Trusted company, FOMO**

➔ **Phishing**

➔ **£1.99**
➔ **Personal data**

Text Message
Today 08:41

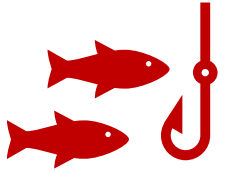
Royal Mail: Your package has a £2.99 shipping fee, to pay this now visit royalmail-redelivery.support. Actions will be taken if you do not pay this fee



Phishing – Tips for users



- Validate the other parties authenticity
- Check email addresses
- Hover over links to see where they go
- Visit sites via known URL's
- Forward to the Suspicious Email Reporting Service – report@phishing.gov.uk
- Text messages can be reported by forwarding to 7726



Vishing Call [02.03.21]

- Pretending to be BT Openreach
- Automated recording: *problems on your line, will be disconnected press 1 to speak to an agent....*
- Gave a 'technical' reason & said that my account had been hacked
- Asked what I used the internet for (prompted banking, PayPal etc)
- Took me to a website (pchelpme.us) then asked me to enter a code and this allowed them to run support software which allowed remote access
- **Aim:** To steal credentials / money



Do you / your organisation reuse passwords?

superman

password1

abc123

football

111111

monkey

qwerty1234

123456

password

qwerty

liverpool

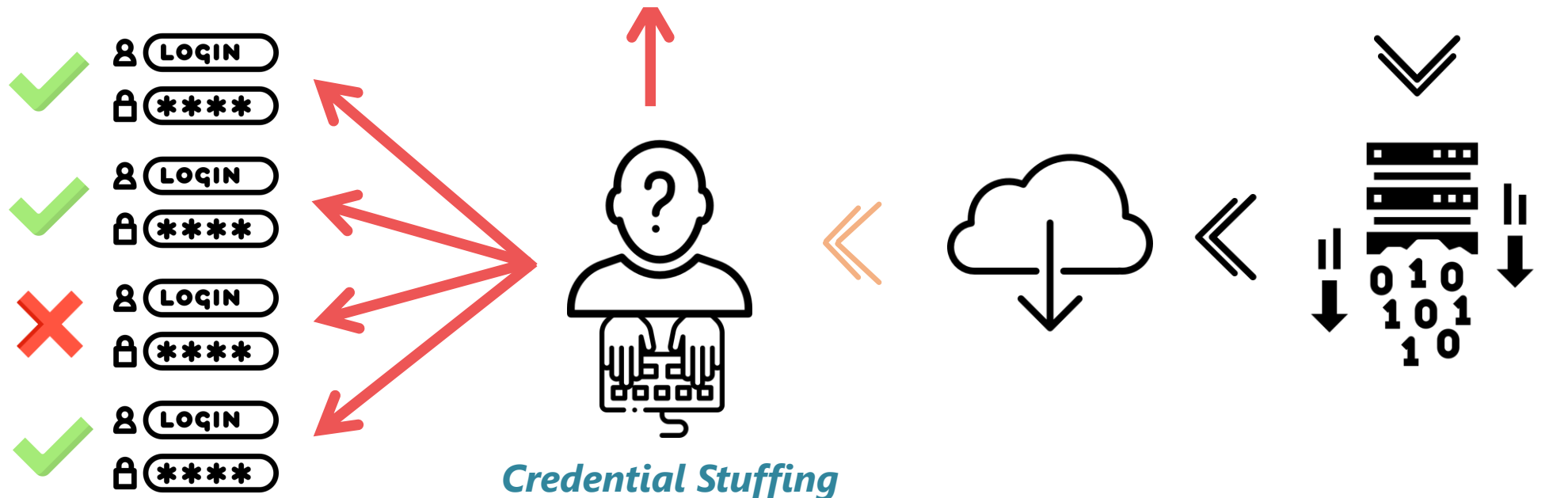
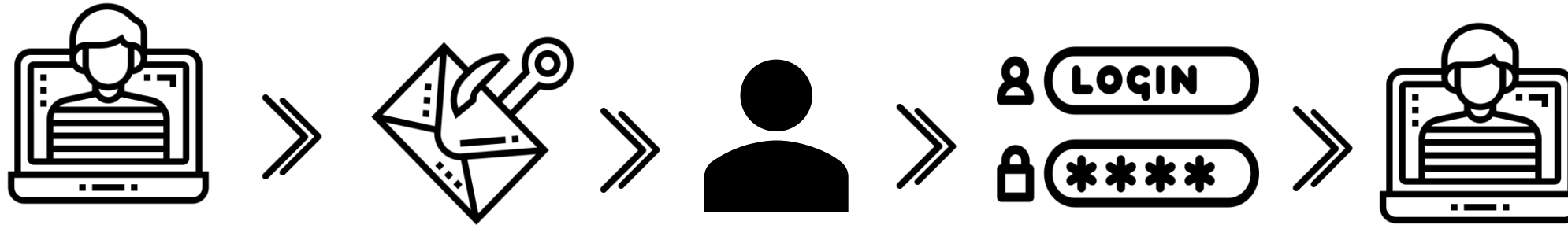
qwerty123

1q2w3e4r5t



Account compromise example

'--have i been pwned?





Have your details ever been in a data breach?

*You can check using
www.haveibeenpwned.com*

*65% of people reuse passwords
across multiple sites.
(Google 2019)*

The screenshot shows the homepage of the 'have i been pwned?' website. At the top, there is a navigation bar with links: Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main heading is 'have i been pwned?' in a large, rounded box. Below it, a subheading says 'Check if your email or phone is in a data breach'. There is a search input field with the placeholder text 'email or phone (international format)' and a button labeled 'pwned?'. Below the search field, there is a section for 'Generate secure, unique passwords for every account' with a link to 'Learn more at 1Password.com'. The main content area displays statistics: 521 pwned websites, 11,145,906,797 pwned accounts, 114,031 pastes, and 199,732,579 paste accounts. Below this, there are two sections: 'Largest breaches' and 'Recently added breaches'. The 'Largest breaches' section lists: Collection #1 accounts (772,904,991), Verifications.io accounts (763,117,241), Onliner Spambot accounts (711,477,622), Data Enrichment Exposure From PDL Customer accounts (622,161,052), Exploit.In accounts (593,427,119), and Facebook accounts (509,458,528). The 'Recently added breaches' section lists: Facebook accounts (509,458,528), Unverified Data Source accounts (11,498,146), Carding Mafia accounts (297,744), WeLeakInfo accounts (11,788), Liker accounts (465,141), Travel Oklahoma accounts (637,279), and Gab accounts (66,521).



World's Biggest Data Breaches & Hacks

Selected events over 30,000 records

UPDATED: Apr 2021

size: records lost

filter



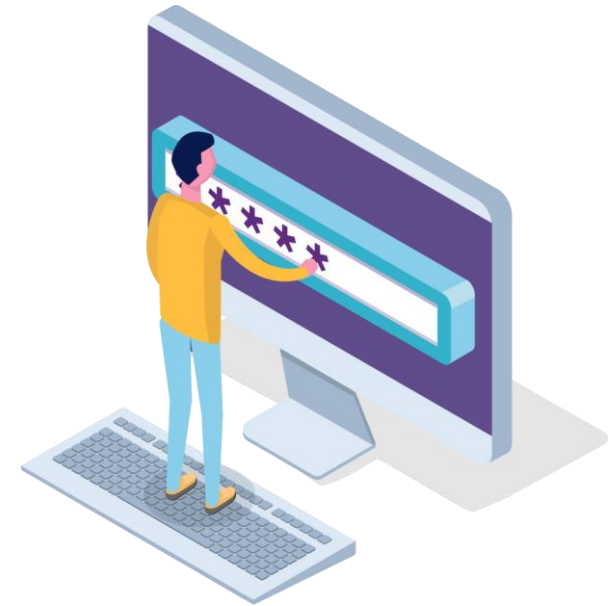
Top Tips



**PROTECT
YOUR EMAIL**



- ✓ Use strong, separate passwords
 - ✓ THREE RANDOM WORDS - Then add complexity, numbers and special characters
- ✓ Use a password manager / save passwords in browser
- ✓ Use two-factor authentication (2FA)



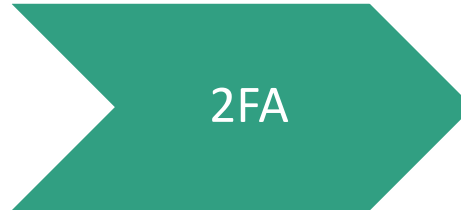
2 Factor Authentication (aka multi-factor, 2FA)



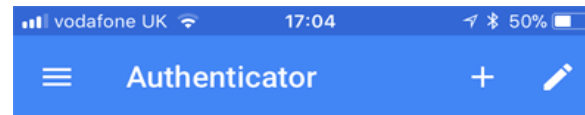
**Something
you know**

TreeChairFish67^

*Cash Point
example*



**Something
you have**



571 208



**If both correct
then access
granted**





Do you use 2FA for your email?



13% of people use the same password for all their accounts. ([Google 2019](#))



More Top Tips



- ✓ Update your devices
 - ✓ Use anti-virus
 - ✓ Backup your most important data
 - Test these backups
- } *(set to auto update)*

The Computer Misuse Act (1990)

Section	Offence	Example	Prison Sentence
1	Unauthorised access to computer material.	Without them knowing, you shoulder surf a friend and use their password to access their account.	Up to 2 years
2	Unauthorised access with intent to commit or facilitate commission of further offences.	Without their permission, you access a friends phone and transfer money from their account.	Up to 5 years
3	Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer.	Use a booter tool to kick someone off an online game.	Up to 10 years
3ZA	Unauthorised acts causing, or creating risk of serious damage.	Hack into a government system undermining national security.	Up to 14 years, if serious risk or actual harm – up to life
3A	Making, supplying or obtaining articles for use in another CMA offence.	Downloaded malware to put on a school computer to gain remote access. You didn't event get to use it.	Up to 2 years

Scams are Fraud - Fraud is the most commonly experienced crime in the UK

- Fraud costs the UK economy £5-£10 Billion a year
- 53% of people over 65 have been targeted by scams
- Statistics indicate that the average scam victim has lost over £3000
- Only 5% of scams are reported

Postal scams

Fake lotteries and prize draws, investment offers, inheritance windfalls.

Telephone scams

Pretending to be a trusted institution, may have some information to make credible, recorded messages.

Doorstep scams

Selling goods and services often poor quality or non existent.

Online scams

Disguised as known company – bank, Paypal, Google Email offers embedded links or attachments.

Fraud

- COVID (vaccine, fines, payments)
- Investment Scams
- Romance Scams
- Courier Fraud
- TV Licencing
- Council Tax reduction
- Tech support scams

Phone



Mobile



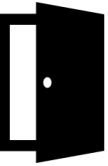
Internet



Letter Box



Doorstep



STOP

CHALLENGE

PROTECT

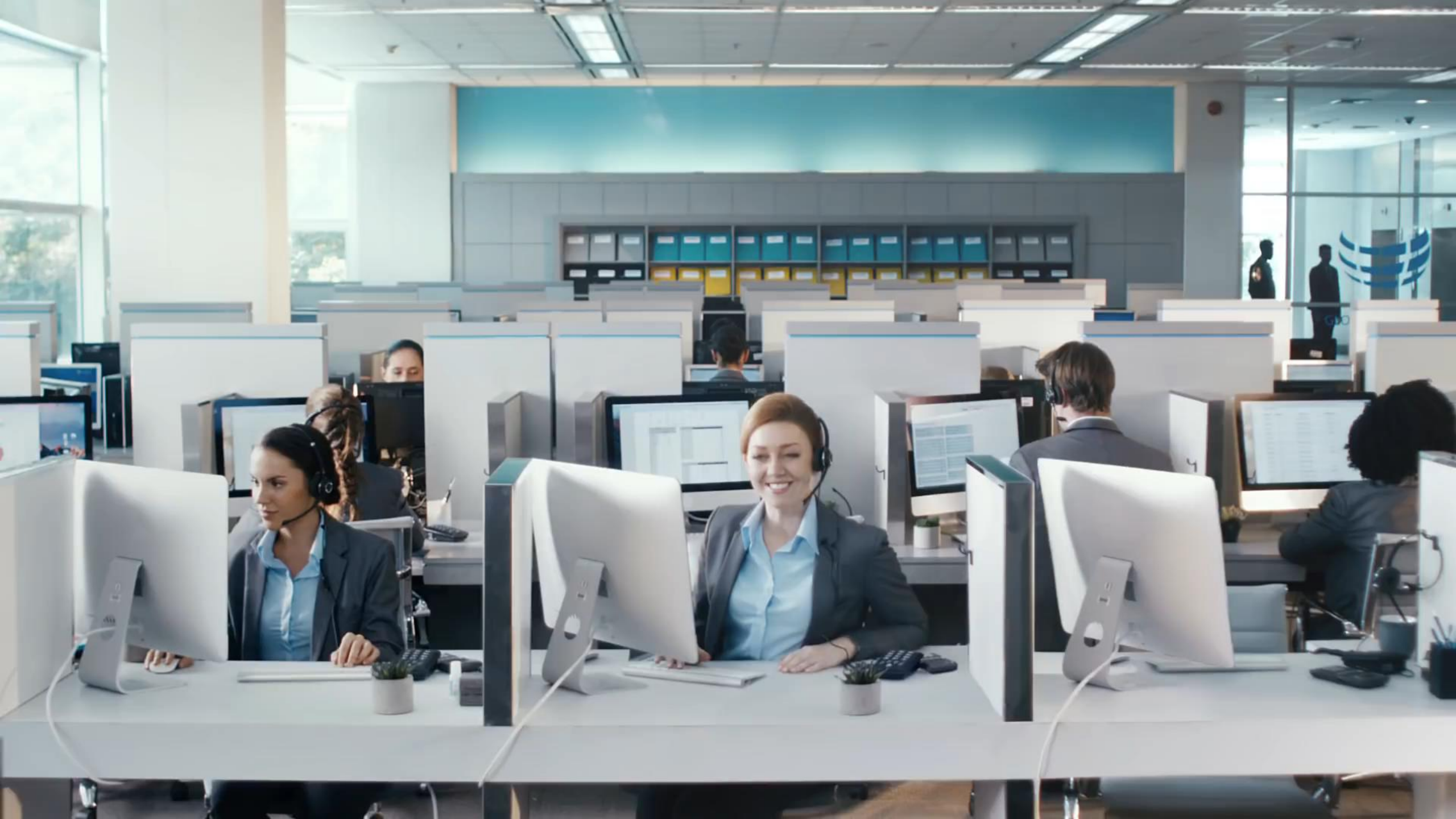


ARE YOU SCAM-SAVVY?



Thinks to look out for: C.A.U.S.E.D

- **C**urrent - Criminals often exploit current news, big events or specific times of year (CENSUS, Tax)
- **A**uthority - Is the message claiming to be from someone official?
- **U**rgent - Are you told you have a limited time to respond
- **S**carcity - Is the message offering something in short supply / to good to be true.
- **E**motion - Does the message make you panic, fearful, hopeful or curious
- **D**ata - They may have some information about you



Things to know



- Bank / police will never call you to ask you to verify your personal details / PIN
- Use contact details you can trust
- Phone numbers can be faked
- If you need to call someone back to check, take five; fraudsters can keep your landline 'open' for a short period of time after you hang up

What to look for in others



Postal Scams

- Making regular trips to Post office
- Lots of Junk Mail
- Lots of Stamps
- Cheque books
- unnecessary products or free gifts in house



Telephone Scams

- Receive lots of Phone calls
- Make regular Payments
- SMS messages
- Talking about new 'Friends'
- Talk about Helpful caller



Doorstep Scams

- Poor quality
- Unnecessary work
- Fearful
- Pressure
- Cash withdrawals



Online Scams

- Suspicious emails
- Final demands
- Refunds
- New Online relationships
- Payments being made
- Asking about bitcoins or other cryptocurrency

FREE

NS Cyber as a resource

- Deliver Cyber Protect message & training
- Signpost and offer general cyber support and advice
- Cyber Basics Review - in line with [Cyber Essentials](#)
- Sponsors for [CiSP](#) – (Cyber Security Information Sharing Partnership) joint industry and government knowledge initiative
- Lego Decisions and Disruptions roleplaying game - to raise awareness of the importance of cyber security

If you are a victim

Action Fraud 24/7
live cyber attacks

- Report to Action Fraud
- Keep copies of / photos of:
 - ✓ Logs (server / access / email)
 - ✓ Email headers
 - ✓ Any related documents
 - ✓ Keep forwarding rules





National Cyber
Security Centre
a part of GCHQ

ncsc.gov.uk



cyberaware.gov.uk

REPORT

Action Fraud

National Fraud & Cyber Crime Reporting Centre

 actionfraud.police.uk 

ALSO FOR **NEWS & ALERTS**

Enable 2FA

Authy.org



haveibeenpwned.com



www.getsafeonline.org



TO STOP FRAUD™

takefive-stopfraud.org.uk



friendsagainstscams.org.uk





As a result of this presentation will you be reviewing your cyber security?



CyberProtect@Norfolk.police.uk



@NSCyberCrime



norfolk.police.uk/advice/cybercrime



smartsurvey.co.uk/s/Individual-NorfolkSuffolk2021

