# How to stay secure online
# cyberaware.gov.uk

For: Chesterton / Bicester Community Resilience Group
On: 15th February 2023 – **(This is the summary document)**

Delivered by: Mr Mark Godsland  CISMP
TVP/SEROCU: Police Cyber Security Advisor

This information is exempt under the freedom of Information Act 2000(FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to **ncscinfoleg@ncsc.gov.uk.**

All material is UK Crown copyright ©.

# Summary of what to expect in the coming slides

A ‘High Level’ over view of the current, risks from the perspective of the wider community. (Individuals) All content is taken from the National Cyber Security Centre or NFIB/ NCA / CoLP/ ICO

**Cyber Aware, looking at their top tips to protect yourselves and stay secure online**

**Data Breaches**

**Phishing (Examples of current COVID-19, Vaccination Scams and other scams)**

**Reporting of suspicious websites, emails & text messages**

How and where to report Fraud and Cyber Crime.

Summary and signposting to further advice, guidance and information.

Note. All content correct as of 15th February 2023



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

National Cyber Security Centre
a part of GCHQ

Cyber Aware

Cyber Aware is the government's national campaign on cyber security.

It is led by the National Cyber Security Centre (NCSC) and delivered in partnership with the Cabinet Office, Home Office and the Department for Digital, Culture, Media & Sport (DCMS).

The campaign is designed to empower and enable the public to better understand how to stay secure online and to take practical steps to help do so.

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

# Cyber Aware

https://www.ncsc.gov.uk/cyberaware/home

National Cyber Security Centre
a part of GCHQ

Cyber Aware

**Take your email security to another level**
Your email is where you keep your most personal and financial information.

If a hacker accesses your email, they could access your other online accounts using the 'forgot password' feature (which often sends you an email) access personal or business information and use this to scam you or people you know.

**This guide outlines the Cyber Aware top tips and advice on how to**:

- Protect your **accounts** **(How to guides are listed in each of the tips, via web links in blue)**
- Protect your **devices** and **data / information**

ACTION REQUIRED

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

# Strong passwords

***What to avoid?***

National Cyber Security Centre
a part of GCHQ

Cyber Aware

Top 10 Most Common Passwords
**(ones to avoid)**

123456
123456789
Qwerty
Password
12345
Qwerty123
1q2w3e
12345678
111111
1234567890

## TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

| 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 | Instantly | Instantly | Instantly |
| 6 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 7 | Instantly | Instantly | 2 secs | 7 secs | 31 secs |
| 8 | Instantly | Instantly | 2 mins | 7 mins | 39 mins |
| 9 | Instantly | 10 secs | 1 hour | 7 hours | 2 days |
| 10 | Instantly | 4 mins | 3 days | 3 weeks | 5 months |
| 11 | Instantly | 2 hours | 5 months | 3 years | 34 years |
| 12 | 2 secs | 2 days | 24 years | 200 years | 3k years |
| 13 | 19 secs | 2 months | 1k years | 12k years | 202k years |
| 14 | 3 mins | 4 years | 64k years | 750k years | 16m years |
| 15 | 32 mins | 100 years | 3m years | 46m years | 1bn years |
| 16 | 5 hours | 3k years | 173m years | 3bn years | 92bn years |
| 17 | 2 days | 69k years | 9bn years | 179bn years | 7tn years |
| 18 | 3 weeks | 2m years | 467bn years | 11tn years | 438tn years |

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

# Action #1

# Use a strong and different password for your email using 3 random words

National Cyber Security Centre
a part of GCHQ

Cyber Aware

Your email password should be strong and different from all your other passwords. Combining 3 random words that each mean something to you is a great way to create a password that is easy to remember but hard to crack.

Do not use words that can be guessed (like your pet's name). You can include numbers and symbols if needed.

For example, “HippoPizzaRocket1”

ACTION REQUIRED

Action 1:
https://www.ncsc.gov.uk/cyberaware/home

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

# Action #2
# Turn on two-step verification (2SV)

National Cyber Security Centre
a part of GCHQ

Cyber Aware

2-Step Verification (2SV) gives you twice the protection so even if hackers have your password, they can't access your email.

2SV works by asking for more information to prove your identity. For example, getting a code sent to your phone when you sign in using a new device or change settings such as your password.

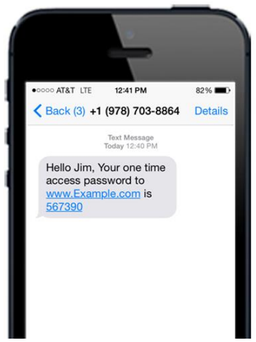
You **won't** be asked for this every time you check your email.

The how:
https://www.ncsc.gov.uk/cyberaware/home#section_4

More detailed information:
https://www.ncsc.gov.uk/guidance/setting-2-step-verification-2sv#section_5

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

# Examples of types of 2SV



- **Review your 2SV options**
- **Secure everything with 2SV:**
  - Email accounts
  - Social media
  - Any other online account

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

# Save your passwords in your browser or using password managers

National Cyber Security Centre
a part of GCHQ

Cyber Aware

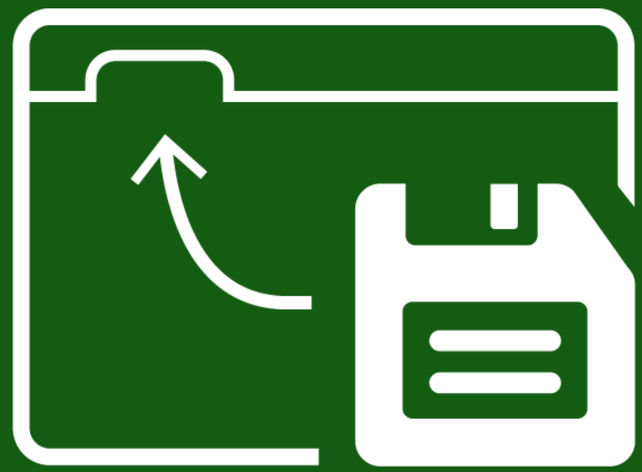
Using the same password for all your accounts makes you vulnerable - if that one password is stolen all your accounts can be accessed.

It's good practice to use different passwords for the accounts you care most about, but remembering lots of passwords can be difficult.

**Saving to your browser is quick, convenient and safer than re-using the same password.**

**Or use a password manager** which is an app on your phone, tablet or computer that stores your passwords securely, so you don't need to remember them all.

https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers



ACTION REQUIRED

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

# Backup up your data

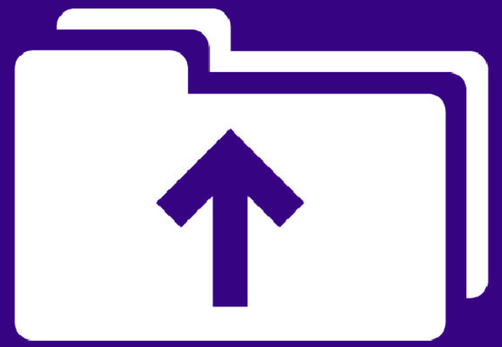
National Cyber Security Centre
a part of GCHQ

Cyber Aware

If your phone, tablet or laptop is hacked, your sensitive personal data could be lost, damaged or stolen.

Keep a copy of all your important information by backing it up.

You can back up all your data or only information that is important to you.



https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/always-back-up-your-most-important-data

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

# Update your devices

ACTION REQUIRED

National Cyber Security Centre
a part of GCHQ

Cyber Aware

Cyber criminals exploit weaknesses in software and apps to access your personal data. Providers continually work to fix these weaknesses, by releasing regular updates.

Using the latest versions of software, apps and operating system immediately improves your security.

Update regularly, or **set your phone or tablet to automatically update.**

That way you don't have to think about it.

https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home

https://www.ncsc.gov.uk/guidance/smart-security-cameras-using-them-safely-in-your-home

https://www.ncsc.gov.uk/cyberaware#action-5

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

# Cyber Action Plan Tool

For individuals or sole traders, where you can receive personalised advice on how to improve your online security

https://ncsc.gov.uk/news/consumer-cyber-action-plan…

**58%** of people are worried about their money being stolen online

**53%** are worried about having their personal details stolen online

**48%** are worried about their devices being infected by viruses or malware

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

# Data breaches:

guidance for individuals and families

National Cyber Security Centre
a part of GCHQ

Cyber Aware

**What is a data breach?**

A data breach occurs when information held by an organisation is stolen or accessed without authorisation.

Criminals can then use this information when creating phishing messages (such as emails and texts) so that they appear legitimate.

The message has been designed to make it sound like you're being individually targeted, when in reality the criminals are sending out millions of these scam messages. Criminals may even send messages pretending to be from an organisation that has suffered a recent data breach.

Even if your details are not stolen in the data breach, the criminals will exploit high profile breaches (whilst they are still fresh in people's minds) to try and trick people into clicking on scam messages.

Full guidance here: https://www.ncsc.gov.uk/guidance/data-breaches

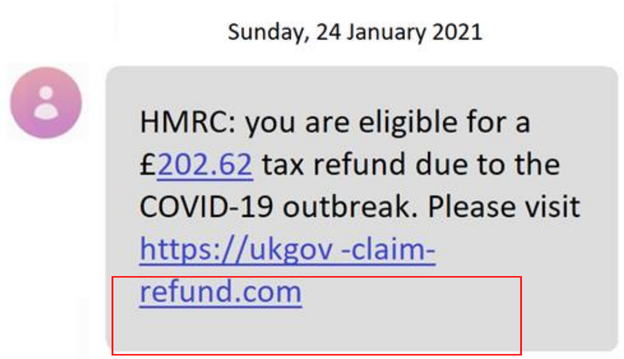
This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

National Cyber Security Centre
a part of GCHQ

Cyber Aware

Phishing attacks attempt to obtain your personal/private/financial information by email, text, phone and social media.

- **Are you expecting this communication? –** take a moment to think if this company/person would usually contact you.
- **Look at the senders address/phone number –** sometimes there may be slight spelling changes in email addresses. Always check the website for the correct email and phone number
- **Avoid clicking links –** even if you are 99% sure, avoid clicking on any links and visit websites directly through your browser.



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

# So how can we be tricked

National Cyber Security Centre
a part of GCHQ

Cyber Aware

Cyber criminals will use deceptive tactics to persuade, trick or lure you into believing that what you are reading is legitimate without questioning the source.

Sometimes we can be tricked into making impulsive decisions, as criminals use the following tactics:

**Urgency –** being put under a time limit, or being asked to provide information urgently, does not give us time to think about what is being asked of us.

**Authority –** we may receive a request from someone pertaining to be from an authoritative body, such as the police or bank, which we normally would not think to question.

**Trusted organisations –** if we receive a request from a ‘company’ or ‘person’ we frequently hear from or shop with, we may not feel to question the legitimacy of the request

**Reward** - it is easy to fall into a trap of winning a fantastic prize or amount of money. If it looks too good to be true, it probably is!

**Emotion –** we as people have emotive sides, which can be played upon in scams. Requests from ‘charities’ or ‘friends in need’ should always be double, or triple checked.

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

How to recognise and report emails, texts, websites, adverts or phone calls that you think are trying to scam you.

National Cyber Security Centre
a part of GCHQ

Cyber Aware

**PAGES**

**PAGE 1 OF 8**

- **Phishing: Spot and report scam emails, texts, websites and calls**
- Report a scam email
- Report a scam text
- Report a scam phone call
- Report a scam website
- Report a scam advert
- Phishing scams: If you've shared sensitive information
- How to spot a scam email, text message or call

https://www.ncsc.gov.uk/collection/phishing-scams

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

# Phishing Scams

## Reporting suspicious messages

National Cyber Security Centre
a part of GCHQ

Cyber Aware

If you are suspicious of an email, report it by forwarding it to:
**report@phishing.gov.uk**

Checking websites:
https://www.getsafeonline.org/checkawebsite

Report suspicious websites to:
https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-website

If you are suspicious of a text, report it by forwarding it to:
**7726**

Reporting of nuisance calls to the Information Commissioners Office:
https://ico.org.uk/make-a-complaint/nuisance-calls-and-messages/spam-texts-and-nuisance-calls/

ACTION REQUIRED

**Reported an email to the NCSC?**

- seek to block the address the email came from
- work with hosting companies to remove links to malicious websites
- raise awareness of commonly reported suspicious emails and methods used (via partners)

**Thank you for your continued support.**

**As of January 2023 the NCSC has received over:**

**17m** reported scams

**Which has resulted in:**

**114k** scams being removed across 209,500 urls

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

# If you have responded in any way to suspicious emails and Text messages

National Cyber Security Centre
a part of GCHQ | Cyber Aware

**Banking details?** - Contact your bank, let them know.

**Account has been hacked?** - Refer to the NCSC's guidance on recovering a hacked account.

**Occurred on a work laptop or phone?** - Contact your IT department.

**If you opened a link on your computer?** - Open your antivirus (AV) software if you have it, and run a full scan. Allow your antivirus software to clean up any problems it finds.

**Given out your password?** - Change the passwords on any of your accounts which use the same password.

**Lost money?** - Tell your bank and report it as a crime to Action Fraud

Citizens Advice's Scams Action service, visit www.citizensadvice.org.uk

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

**Reporting of Fraud / Cyber Crime**
https://www.actionfraud.police.uk/guide-to-reporting

National Cyber Security Centre
a part of GCHQ

Cyber Aware

# Action Fraud customer channels

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

## Social Media

Help and advice.
How to protect against fraud.
News and alerts.
Real time fraud intelligence.

## 0300 123 2040

Report fraud and cyber crime.
Help, support and advice.

## 24/7 Live cyber

Specialist line for business, charities or organisations suffering live cyber attacks

## Report 24/7 & Web Chat

**www.actionfraud.police.uk**
Secure online reporting.
News and Alerts.
Advice on avoiding the latest scams.

National Fraud and Cyber Crime Reporting Centre

2,000+ calls per day
250+ web chats per day

Cifas Data
UK Finance

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

# Summary of guidance for individuals
# Aim: To have an understanding of and have a behavioural change toward:

**Cyber Aware** has all of the above information in greater detail and with help sections: https://www.ncsc.gov.uk/cyberaware/home

**Report Suspicious Emails to**: report@phishing.gov.uk **Report Suspicious texts**, by forwarding them to **7726**

**Report Suspicious websites**: https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-website

**Reporting of Fraud / Cyber Crime – Action Fraud**: https://www.actionfraud.police.uk/guide-to-reporting

**Additional Cyber Security guidance**: https://www.ncsc.gov.uk/section/information-for/individuals-families

**From our Regional Pages:** https://serocu.police.uk/individuals/

**Be also aware of door step, romance, computer service, get rich quick fraud & other rogue trader offences.**
**"Too good to be true? Then Yes it's a Scam!!"**

**Advice and support from Citizens Advice's Scams Action service**: https://www.citizensadvice.org.uk/

**Reporting of nuisance calls to the Information Commissioners Office:**
https://ico.org.uk/make-a-complaint/nuisance-calls-and-messages/spam-texts-and-nuisance-calls/

National Cyber Security Centre
a part of GCHQ
Cyber Aware

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

south east
Regional Organised Crime Unit

National Cyber Security Centre
a part of GCHQ

Cyber Aware

**Thank you for this opportunity to have presented the above content to you**

Get the latest information and reports from the **National Cyber Security Centre, Action Fraud and TVP**

- Cyber Alerts & Advisories: www.ncsc.gov.uk/index/alerts-and-advisories
- Thames Valley Alerts: https://www.thamesvalleyalert.co.uk/
- Action Fraud Alerts: https://www.actionfraud.police.uk/sign-up-for-action-fraud-alert
- TVP dedicated Cyber / Fraud twitter account: @TVPCyber_Fraud

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION