National Cyber Security Centre
a part of GCHQ

Cyber Aware

Cyber Aware
Campaign Toolkit

February 2022

About
Cyber Aware

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.

The tone of the campaign is light-hearted with the aim of getting the attention of non-cyber enthusiasts and encourage them to take up two behaviours to best protect important accounts, particularly emails: basing passwords on 3-random words (3RW) and setting up 2-step verification (2SV).

Contents

National Cyber Security Centre
a part of GCHQ

Cyber Aware

National Cyber Security Centre
a part of GCHQ

Cyber Aware

#1 Top lines

Top lines

National Cyber Security Centre
a part of GCHQ
Cyber Aware

- As we all spend more time online, it becomes increasingly critical that we are aware of the different ways to stay secure. We all have social media and email accounts. If they are hacked, they can be used to break into other linked accounts.
- The prospect of having our email or social media accounts hacked is a worry for many and, unfortunately, it's a very real threat.
- Opportunistic criminals are taking advantage of people using digital devices more than ever before with scams that can lead to accounts being hacked.
- Since April 2020, members of the public have reported over 10.5 million suspicious emails to the UK's cyber experts, resulting in the take down of 76,000 online scams. However, there has also been a 161% increase in unauthorised access to personal information offences – including hacking – last year.
- Fortunately, securing our most important accounts begins with following two simple steps:
    - Use a password based on 3-random words (3RW)
    - Secure accounts by enabling 2-step verification (2SV)

National Cyber Security Centre
a part of GCHQ

Cyber Aware

2

#2 Protective behaviours

Protective behaviours

National Cyber Security Centre
a part of GCHQ | Cyber Aware

Devised by NCSC technical experts, the campaign centres around two practical steps that protect the public and micro businesses from the majority of preventable cyber incidents.

1. **Use a strong and different password for your email based on 3 random words** – 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 longer, more complex password that is easy to remember but hard to crack.

1. **Turn on 2-Step Verification (2SV) for your email** - 2-Step Verification (2SV) gives you twice the protection so even if cyber criminals 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.

National Cyber Security Centre
a part of GCHQ

Cyber Aware

3

#3 Audience

Audience

National Cyber Security Centre
a part of GCHQ | Cyber Aware

Our activity will target:

- Individuals who are most likely to be hit hardest by any financial loss – but with enough income to be reliant on technology for banking, shopping, schooling, etc.
- Micro businesses and sole traders who make up 95% of UK businesses (5.6m).

National Cyber Security Centre
a part of GCHQ

Cyber Aware

4

#4 Campaign timings

Campaign timings

National Cyber Security Centre
a part of GCHQ | Cyber Aware

- **Campaign launch (consumers)**

  14 March

- **Radio advertising campaign**

  14 March - 15 April

- **Digital billboard campaign**

  25 March – 24 April

- **Social media campaign**

  1 April - 15 May

The campaign will run across England, Wales, Scotland and Northern Ireland

National Cyber Security Centre
a part of GCHQ

Cyber Aware

#5 How to get involved

How to get involved

National Cyber Security Centre
a part of GCHQ | Cyber Aware

Our ask of you is to use your public and/or staff-facing channels to support the Cyber Aware campaign messaging.

Three ways in which partners can help:

1. **Social media:** Amplify, share or comment on campaign content via the NCSC Twitter and LinkedIn channels or by using the materials below.
2. **Internal communications**: Share the Cyber Aware messages with colleagues and workforces, using suggested copy below.
3. **Customer/service users:** Include a short article in newsletters, e-bulletins or customer channels, alerting audiences to the Cyber Aware advice and tools to help secure their most important online accounts.

We thank you in advance for your assistance in helping to make the UK the safest place to live and work online by encouraging your audiences, workforces, service users or customers the right tools to improve their cyber resilience.
We ask that the assets (graphics and films) should be used as supplied and not altered in any way.

If you would like to co-brand the assets with your own logo, please get in touch with us at brand@ncsc.gov.uk.

Continued on next page…

National Cyber Security Centre
a part of GCHQ

Cyber Aware

#6 Creative assets

Creative assets

National Cyber Security Centre
a part of GCHQ | Cyber Aware

Links to campaign assets, which include the following, can be found at the Cyber Aware campaign resource centre. This is being updated but will include

- Campaign film
- Social media assets
- Digital assets

These assets are for use by public sector partners who have received them directly from NCSC. The assets should be used as supplied and not altered in any way.

If you would like to co-brand the assets with your own logo, please get in touch with us. For terms and conditions, please refer to the NCSC website: Terms & conditions - NCSC.GOV.UK

National Cyber Security Centre
a part of GCHQ

Cyber Aware

7

#7 Suggested social media posts

Social media suggested posts

National Cyber Security Centre
a part of GCHQ

Cyber Aware

You can support the campaign on social media using #CyberAware and sharing or reposting social content from @NCSC.

Please use the Twitter handle @cyberawaregov or “Cyber Aware from the National Cyber Security Centre” on Facebook.

Tweet 1:

Change your email password.

It's the gateway to your digital life. If you're using the same password elsewhere, do something about it.

Pick #ThreeRandomWords. Really. Go for something weird. Make that password uncrackable.

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

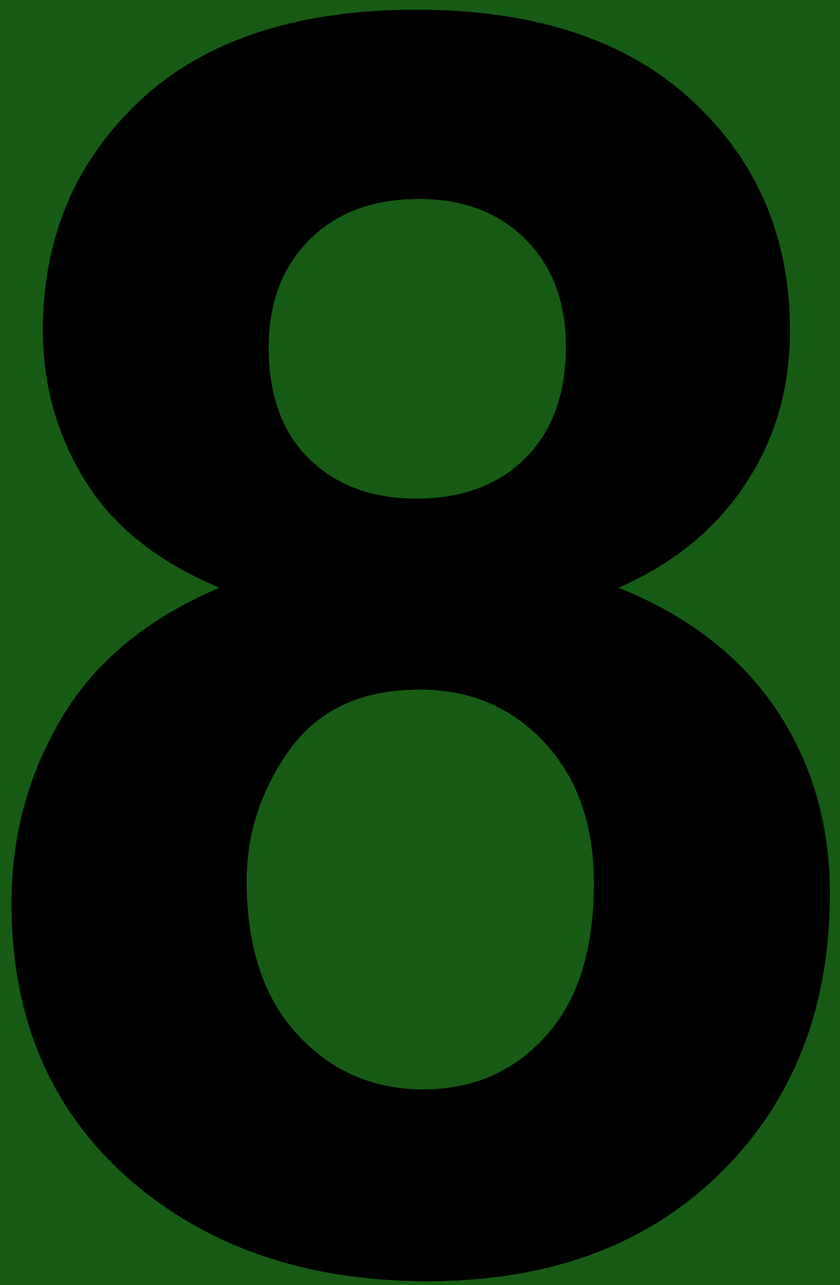
Tweet 2:

Turn on 2-Step Verification.

It's the thing where you prove you are who you say you are by using something like your thumb, face or phone to add another layer of security.

What do we want you to do? Turn it on.

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



National Cyber Security Centre
a part of GCHQ

Cyber Aware

#8 Suggested internal comms

Internal communications

National Cyber Security Centre
a part of GCHQ | Cyber Aware

This is a suggested form of words that can be edited to suit the tone of your organisation

- Since April 2020, members of the public have reported over 10.5 million suspicious emails to the UK's cyber experts, resulting in the take down of 76,000 online scams. However, there has been a161% increase in unauthorised access to personal information offences – including hacking – last year.

- Fortunately, securing our most important accounts begins with following two simple steps:

1. Use a password based on 3-random words (3RW)
2. Secure accounts by enabling 2-step verification (2SV)

- If you think this is familiar advice, it might be because you heard it played out on radio adverts or you may have seen it on billboards or your social media feeds.

- The advice comes direct from the UK's authority on cyber security – the National Cyber Security Centre (NCSC), a part of GCHQ.

- The NCSC has just launched its latest Cyber Aware campaign which provides actionable advice on defending digital assets against the very real threat of online scams and hacking.

- The Cyber Aware website gives clear instructions about how to set up 2-step verification (2SV), as well as guidance on passwords based on 3-random words (3RW). The aim is to protect all of us and make life even harder for the scammers.

- Using 3-random words (3RW) allows us to set passwords that are unique, strong, and easy to remember. Enabling 2-step verification (2SV) significantly decreases the likelihood of an account being hacked. It is simple and dramatically reduces risks, including financial losses.
- Stealing a password can be simple – stealing a password and a device used to authenticate a login is much harder.

- Now, you may think that this is not relevant to you since you have never been the victim of a scam. Or you may just find cyber security mystifying gobbledygook. That is understandable. And it is why the Cyber Aware advice has been set out in clear, easy to follow steps.

- As we all spend more time online, it becomes increasingly critical that we are aware of the different ways to stay secure. We all have social media and email accounts. If they are hacked, they can be used to break into other linked accounts.

- So, let's help ourselves and help each other to make the UK the safest place to live and work online. Follow the Cyber Aware advice by sorting our 2SV and 3RW today.

National Cyber Security Centre
a part of GCHQ

Cyber Aware

9

#9 Campaign background

Campaign Background

National Cyber Security Centre
a part of GCHQ | Cyber Aware

- Cyber Aware first launched in April 2020 with cyberaware.gov.uk and the Suspicious Email Reporting Service, alongside other reporting services for scam texts and websites.

- The Cyber Aware landing page provides direct links to the most common email providers, so visitors to the page can enact the changes there and then.

- The tone of the campaign is light-hearted with the aim of getting the attention of non-cyber enthusiasts and encourage them to take up two behaviours to best protect important accounts, particularly emails: basing passwords on 3-random words (3RW) and setting up 2-step verification (2SV).

- Using three random words allows people to set passwords that are unique, strong enough and easier to remember. Enabling two-step verification significantly decreases the likelihood of an account being hacked. Stealing a password can be simple – stealing a password and a device used to authenticate a login is much harder.

- The Cyber Aware campaign is delivered by the NCSC working alongside the Home Office, the Cabinet Office and the Department for Digital, Culture, Media, and Sport.