HM Government

Switching the public and small businesses on to cyber security and fraud

A cyber crime and fraud communications toolkit for Law Enforcement

Version 2.0 | February 2018

CYBER AWARE

TAKE FIVE TO STOP FRAUD™

Contents

This toolkit has been designed as an interactive document. It can be read in full or you can scroll straight to relevant sections. Clicking on one of the highlighted 'live links' anywhere in the toolkit will take you straight to where you can find more detail on that subject.

A joined up approach to tackling the UK cyber and fraud threat

Aims of this toolkit

Scale of the cyber and fraud threat

Navigating the communications landscape

Aims of this communications toolkit

Cyber crime can affect anyone, regardless of age, gender, job or location. It's one of the fastest growing crimes in the UK and as we let more and more digital technology into our lives, the threat keeps growing.

Law enforcement is a vital partner in helping the Government deliver these messages to the public and organisations in your local community.

This toolkit is designed to provide you with the right tools and resources to deliver impactful and consistent communications on cyber crime and fraud whether you are in a corporate communications teams or a police officer in operations.

Just as the cyber threat is changing all the time, so this toolkit will evolve over time to incorporate changing messages and new examples of good practice.

It should be noted that the toolkit is intended to cover cyber-enabled and dependent crime and not cyber-facilitated crime such as online harassment or bullying, child sexual exploitation or radicalisation and terrorism.

In 2016, the government set out its approach to securing the UK against the cyber threat in the National Cyber Security Strategy. A core element of this is delivering a step change in public and organisational behaviour towards cyber security.

Key to its success is to:

Repeatedly deliver co-ordinated communications

that educate and motivate the public to change the behaviours that put them at greater risk

Harness 'trusted voices'

to increase the credibility, relevance and reach of the easy and actionable advice which will better protect people from the cyber threat.

Scale of the cyber threat

Why is cyber crime a threat?

- **Cyber crime is significant and one of the biggest criminal threats to the UK**, with an estimated cost of billions of pounds each year. It is everybody's responsibility, although action can be hampered by a lack of personal responsibility and a poor understanding of the threat.
- For many people and organisations affected by cyber crime, **the impact goes far beyond just the immediate financial and reputational costs.**
- **Most cyber criminals exploit basic security vulnerabilities and human vulnerabilities**, as seen in the numerous data breaches that come to light each year[1].
- **The rise of internet connected devices gives attackers more opportunity**. With more interconnected devices such as home appliances and driverless cars, the public is increasingly exposed to new threats to their security.
- **Under-reporting of cyber crime continues to obscure understanding** of its true scale, cost and impact on victims.

How is cyber crime a threat?

- **This threat is varied and adaptable**; ranging from mass, opportunistic, low-tech attacks on individual members of the public and organisations which merely exploit human vulnerabilities, to highly sophisticated and persistent attacks involving bespoke malware designed to compromise specific targets, usually large organisations or government systems.
- The most technically competent **cyber crime offenders are increasingly moving away from individuals towards targeting businesses and payment systems** drawn by the prospect of greater financial rewards[1].
- **Ransomware attacks are increasingly prevalent.**
- **2017 was punctuated by cyber attacks on a scale and boldness not seen before.** This included the largest recorded cyber heist, the largest DDoS attack and the biggest data breach ever being revealed[2].

1 NCA National Strategic Assessment of Serious and Organised Crime 2017
2 NCSC/NCA – The Threat to UK Business report 2016/2017

Scale of the cyber threat

More needs to be done to help ensure the public and small businesses are aware of the current threats to help them take responsibility to protect themselves against the threat. Consistently communicating the simple, protective behaviours outlined here will help bridge the gap between awareness, action and, importantly, encourage the reporting of crime.

1.6 million **cyber crime incidents** in the past year[1]

£1,380 was the **average loss** for small firms[2]

46% of UK businesses identified at least one **cyber security breach** or attack in the last 12 months[2]

89% of small business victims also saw an **impact on their reputation** after an incident – the impact is not just financial[3]

But the threat is not being acted on

27% **feel they are too small to be targets**

27% of small to medium sized enterprises believe they are 'too small' to be of interest to cyber criminals[4]

48% **don't follow software and app updates cyber advice**

Only 52% of people are following HMG's advice on installing the latest software and app updates[5]

For more information

about the cyber threat or for news on the latest cyber incidents, visit:

ncsc.gov.uk/index/report
twitter.com/ncsc (@NCSC)
nationalcrimeagency.gov.uk/news
nationalcrimeagency.gov.uk/publications
twitter.com/NCA_UK (@NCA_UK)
twitter.com/CyberProtectUK (@cyberprotectUK)
actionfraud.police.uk/news

1 ONS, Crime Survey for England and Wales 2017
2 The Government's 2017 Cyber Security Breaches Survey
3 Small Business Reputation research – RICU and KPMG (2016)
4 The Government's 2017 Cyber Security Breaches Survey
5 National Cyber Security Tracker, 2016

Scale of the fraud threat

Why is fraud a threat?

Fraud is the most prevalent crime in the UK. In 2016 there were 1.8 million cases of card fraud with losses of £768 million across payment cards, remote banking and cheque fraud (FFA UK 2016 data).

Banking & corporate fraud (such as mandate fraud, mortgage fraud and procurement fraud) are considered the biggest threats to the private sector, due to the increasing frequency of reports of high losses.

How is fraud a threat?

Fraud is when trickery is used to gain a dishonest advantage, which is often financial, over another person. Fraud can be committed against individuals or businesses and technology is a key enabler.

The most common types include: Identity crime, Individual fraud, Corporate fraud, Online fraud, Advanced fee fraud, Fraud against the tax & benefit system, Intellectual property crime.

There are many words used to describe fraud: scam, con, swindle, extortion, sham, double-cross, hoax, cheat, ploy, ruse, hoodwink, confidence trick. An A-Z of fraud can be found here.

To avoid direct bank intervention, fraudsters are increasingly using social engineering tools, particularly vishing (obtaining information by phone) and smishing (obtaining information by SMS text message) to gain customer information that will enable them to commit fraud.

Data obtained during security breaches continues to be a key enabler of fraud against the individual, and can be used to commit fraud directly, or add authenticity to a fraudulent approach.

For more information

actionfraud.police.uk/news
twitter.com/actionfrauduk (@ActionFraudUK)
twitter.com/CyberProtectUK (@cyberprotectUK)

The City of London Police are currently investigating **estimated financial losses** of around **£600 million**

3.3 million **fraud incidents** in the past year[1]

70% of fraud is **cyber enabled**

3x more money lost to cyber criminals on average for men than women[2]

£2,354 average loss for **men**

£809 average loss for **women**

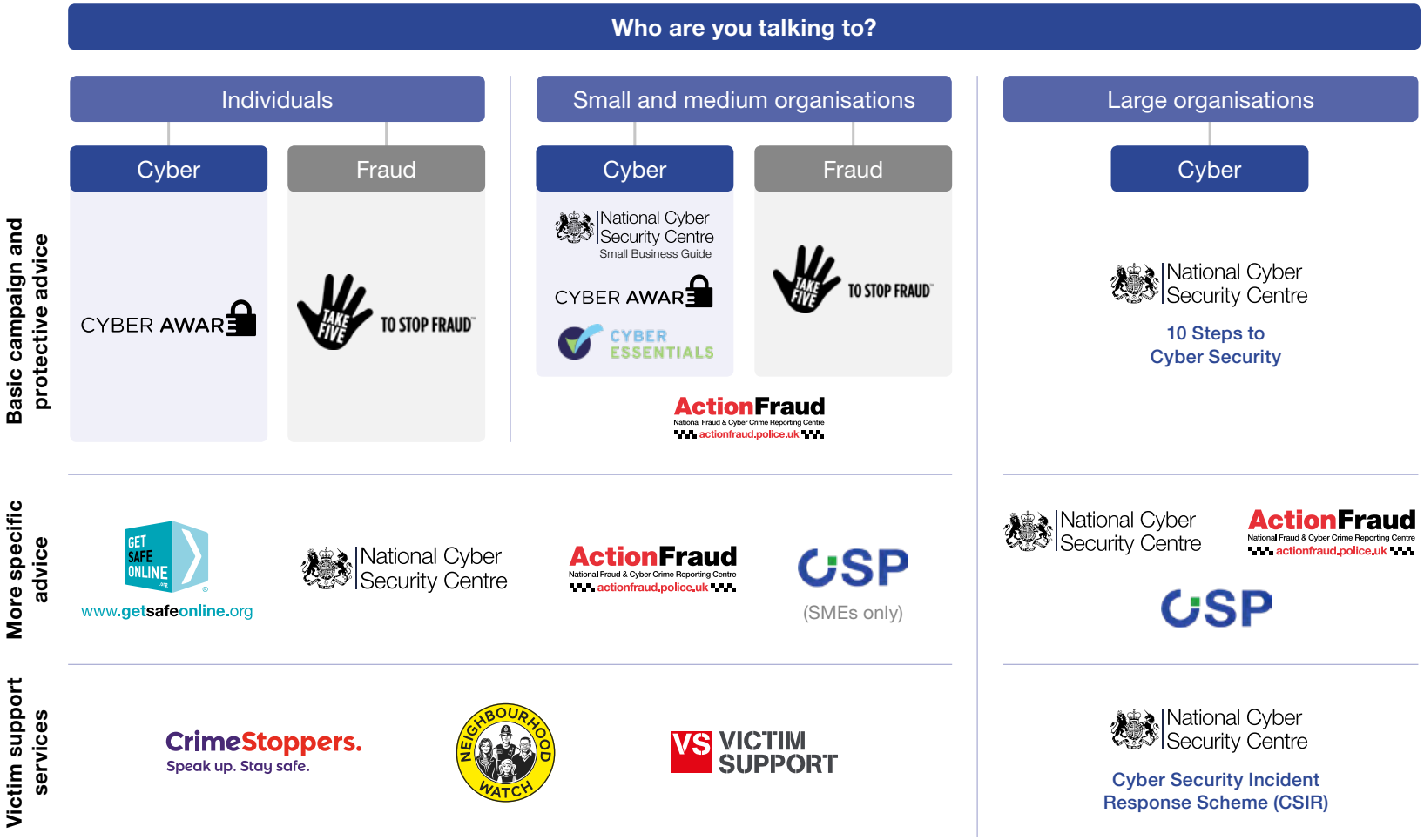
1 ONS, Crime Survey for England and Wales 2017
2 City of London Police, Economic and Cyber Crime Prevention Centre (ECPC)

The cyber crime and fraud fighting landscape: what advice to give to which audiences and when

The Cyber Aware, Cyber Essentials and Take Five – To Stop Fraud umbrella brands provide Government's agreed basic level advice and should form the foundation of, and be signposted to, from all your communications activity so that we can better provide the public and organisations with greater clarity on the actions they should focus on. The diagram below aims to clarify which key campaigns/services to direct audiences towards depending on what you are trying to achieve.

Reactive communications: In response to specific incidents you should first signpost to the NCSC or Action Fraud and then monitor for updates.

Always encourage the reporting of potential incidences of cyber crime and fraud to **ACTION FRAUD.** Click here for more information.



Key messages

The two brands

What the advice says

Two brands, one goal

Research tells us that the public and many small organisations often see cyber crime and fraud as a single issue.

Because of this, two complementary Government, industry and NCSC-backed 'umbrella' brands providing official and consistent advice have been developed:

CYBER AWARE

Cyber Aware has been developed with the National Cyber Security Centre and provides the simplest, technical advice for the public and micro businesses to help protect themselves against the cyber threat.

Visit cyberaware.gov.uk

TAKE FIVE TO STOP FRAUD

Take Five, a partnership between UK Finance and the Government, advises the public on how to protect themselves from preventable financial fraud (including email deception and phone-based scams) and offline fraud.

Visit takefive-stopfraud.org.uk

Collectively these brands provide the most important basic advice that the public and micro businesses need to put in place to best protect them from the threat and this advice should be the foundation in your own local communications.

For more detailed advice for small businesses, please use the NCSC's Small Business Guide.

"Very few people would leave their front door unlocked or windows open when they went out. Encouraging people to be Cyber Aware is the equivalent of the check list of things we go through to make our house secure when we go out. Take Five is the equivalent of putting a chain on your door and being sure about who's knocking before you let them in. Together they ensure you won't get any unwanted visitors."

- **T/Commander Dave Clark**, City of London Police and National Co-ordinator for Economic Crime

What the advice says

When speaking to the public and small organisations about how they can protect themselves against cyber crime and fraud, there are a number of key messages that you should seek to provide. These messages are applicable for one-off presentations, a communications campaign or following an incident.

Cyber Crime

Priority messages

- Install the latest software and app updates
- Use a strong, separate password for your email account

Secondary messages

- Secure your tablet or smartphone with a screen lock
- Always back-up your most important data
- Don't use public Wi-Fi to transfer sensitive information such as card details
- Use two-factor authentication for your most important accounts

For the public

- Don't 'jailbreak' or 'root' your smartphone – mainly relevant for the younger audience
- Beware of fake websites

Cyber-enabled Fraud

(E.g. phishing – where messages can be drawn from both brands)

- Never automatically click on a link in an unexpected email or text
- Install the latest software and app updates
- Use a strong, separate password for your email account
- Beware of fake websites

Fraud

Take Five empowers people to confidently challenge uninvited and potentially fraudulent approaches with a simple principle/message: 'My money? My info? I don't think so!'

Requests to move money

A genuine bank or organisation will never contact you out of the blue to ask for your PIN, full password or to move money to another account. Only give out your personal or financial details to use a service that you have given your consent to, that you trust and that you are expecting to be contacted by.

Clicking on links/files

Don't be tricked into giving a fraudster access to your personal or financial details. Never automatically click on a link in an unexpected email or text.

Personal information

Always question uninvited approaches in case it's a scam. Instead, contact the company directly using a known email or phone number.

Always encourage potential victims to report fraud and cyber crimes to Action Fraud

A range of free materials are available to download and/or order for each campaign, from posters to pull up banners.
Click here for further information. For more detailed advice for small businesses, please use the **NCSC's Small Business Guide.**.

Communication insights

What drives people to be more or less cyber secure

Understanding your local audiences: Segmentation

Hitting the target: what makes people change their cyber security behaviour?

We need to make the UK think about cyber security and fraud prevention measures as second nature – the same as locking your doors and windows when you leave the house.

But that's easier said than done if a person doesn't think getting hacked is as much of a crime as getting burgled.

The only way to really change behaviours around the risks of online criminality is through consistency and repetition of message, delivered at relevant points and through trusted voices.

What can help get the cyber secure and fraud message across?

- Awareness of – and engagement with – cyber security and fraud – and the simple things individuals can do to protect themselves is increasing
- Internet use is prevalent, with each click on a web page offering opportunities to flag up cyber secure messages
- It's not just about losing money - people are motivated by the risk to their identity, privacy and future career prospects
- Individuals and organisations expect to hear this advice from all trusted sources, including Government and law enforcement.

Why people don't take cyber security and fraud messages on board

People don't understand how cyber crime happens, so they're unlikely to engage with it. Cyber security and fraud prevention is often perceived to be the responsibility of other people.

"Before you even realise it the bank will just give you your money back. You don't really have to even worry about it"

Cyber crime and fraud aren't 'real crimes' – they're not physical and it's something that happens to 'other people'

"You'd have to be full on paranoid to worry about it [cyber crime]"

Cyber crime isn't something to worry about – it's perceived to have very few consequences and limited personal impact

"If the experts can't even agree what I need to do, then how am I supposed to know?

Being cyber secure is seen as time consuming, confusing and complex – people think there's nothing more they can do to protect themselves

1 Insights are drawn from qualitative research done by Britain Thinks for RICU since 2014; gathered through focus groups with both the public and small businesses.

Understanding your local audience: Segmentation

Segmentation is simply a term used in marketing to describe the process of dividing potential customers/users into groups – or segments – based on different characteristics.

This can be anything from people's age, to where they live or what car they drive. It allows different types of communication to be developed and 'targeted' at specific groups.

The 'Public Interventions Model' (more commonly referred to as the 'SOC Segmentation') is a piece of research carried out by the Home Office that identifies and separates groups within the UK general public by their susceptibility to becoming victims of fraud, financial and cyber crime.

It breaks the groups down into:

- **Who** they are (age, gender, address etc.)
- **What** makes them at-risk (attitudes, behaviours, experience of crime)
- **How** to reach them (location, trusted partners, communications channels)

To see all the segment groups at a glance, click here.

Knowing the profile of your local community and being able to break it down into different groups sharing common traits can help you identify vulnerable groups.

Click here for ideas on how to put this into practice and a case study of how the segmentation tool has been used in practice.

Fraud victim profile data for your force area, which effectively paints a picture of your local force area's potential vulnerability, is contained in the quarterly profiles sent to your force's special point of contact (SPOC) by the City of London Police's National Fraud Intelligence Bureau.

The raw data feeding into these quarterly force profiles can be accessed via POLKA – for more information or to find out who your force's SPOC is please contact

NFIBoutputs@cityoflondon.pnn.police.uk

Communications tools, tactics & tips

Communications campaigns come in all shapes and sizes, depending on a range of factors, from your desired outcome to the amount of time and money at your disposal.

Your force's communications team is the best first port of call for campaign advice and to keep them updated on your plans. This section helps police officers to set out some of the different ways you can communicate as well as some top tips from communications experts.

This section includes:

- Running a successful campaign
- Events
- Using the internet and social media
- Evaluation
- Working with the press and media

Running a successful campaign

Good campaigns are based on good planning – whatever the scale. There are a few basic steps worth following in any campaign:

Set specific objectives

What is the issue and what are you trying to achieve? E.g. to make residents in [enter location] more resilient against the cyber threat by making sure they have a strong and separate password for their email by [enter date].

Refine your target audience

Who are the most vulnerable and what are their characteristics? (Use the Segmentation tool to help you identify this) E.g. 25 to 45 year old residents in the [enter location] local area who are online and vulnerable to cyber crime.

Tailor your messages

Use the approved messages in this toolkit for the core advice. Think of a communications 'hook' to make the advice relevant and engage the audience. E.g. in [enter location] are more likely to experience [enter threat type] than elsewhere. Use local case studies to bring the issue to life if you can.

Choose your channels

How does your target audience receive their information? E.g. Use the segmentation data to see that 25-45 year olds use social media, read the local paper and trust information from you, voluntary sector organisations and local banks. So, use social media, local press and community events with voluntary organisations, such as Age UK and local businesses/banks.

Set your targets

Identify ways to track the effectiveness of your activity and identify how you will gather this information, such as unique links that enable the tracking of visits to websites. E.g. deliver 10 Facebook and 10 Twitter posts, achieving 100 'likes' or 're-shares' across the campaign period.

Plan your campaign delivery

Set a realistic timeline for developing each of the stages above, highlighting key milestones for approvals and launch. Seek advice from your corporate communications colleagues as there could be quick wins – ideally leave 3-4 weeks to plan your campaign where possible, especially if multiple approvals are needed.

Evaluate your activity

Review whether you achieved your targets, and what went well/not well so you can factor any learnings into your next campaign.

Close the loop

Thank your local supporters and share your successes on social media.

Click here for examples of how other Government departments have run successful campaigns

We're looking to review this document regularly, so please inform us of your successful campaigns at cyberaware@homeoffice.x.gsi.gov.uk and we may include them in the future as examples of best practice.

Using the internet and social media

Using social media is a really effective and economic way of increasing the reach of your campaign, providing hooks for partners to support and to get real-time feedback from your audience(s).

Planning and writing social media content

1. **Map out when you will post during your campaign**
   Flag any external events that might spark further interest in or conflict with your campaign aims
2. **Agree frequency of posts**
   It's generally considered good practice to post around twice a day on Twitter, once a day on Facebook
3. **Work out how you're going to reply to comments**
   Consult your existing moderation policy or create one to deal with any abusive or inappropriate comments
4. **Tailor your content for the channel**
   Twitter is more reactive and fast-paced, whereas Facebook can accommodate longer, more reflective posts
5. **Get to know your audience by asking open-ended questions**
   It helps boost engagement in your posts
6. **Use Hashtags which are relevant to your topic**
   Bring your content to a wider audience
7. **Try to avoid 'naked' posts**
   Each post should include a picture or video
8. **Use calendar hooks to boost engagement**
   Link your content to things that are happening in the 'real world' e.g. Mother's Day
9. **Always sense check your images**
   Are you showing the inside of your office with sensitive material in view?
10. **Get the right permissions for the images you use**
    E.g. has anyone featured given consent to be photographed and for the image to be used in this way?

Click here to see a template social media schedule with top tips

Using the internet and social media

Top Twitter tips

Automatically schedule posts
using Hootsuite

Check post length
using Microsoft Word's 'character count' function to keep to the 280 character limit

Click here to see a template Twitter schedule with top tips

Top website tips

Direct signposting
Consider signposting directly to cyber security advice from your website home page

Consider your audience's journey
Link social media, leaflets, posters to the relevant page on your website so the journey makes sense for your audience

Click here to see a template Facebook schedule with top tips

Working with press, media and local partners

Media organisations are bombarded with press releases, so it pays to spend time getting yours right so that it will stand out from the crowd. Ensure that your force's Communications Team are the first port of call when contacting the media.

Writing a compelling press release

Always try to find a 'hook' – something that will make it newsworthy. Think about whether your event or issue is the 'first', the 'biggest', the 100th or whether it is linked to another newsworthy event, or national campaign.

Answer the four Ws in your press release: what, when, where and why.

Useful examples

Click here for an example of a press release written for Cyber Aware's Think Random campaign.

Top tips for getting your press release noticed

Regional journalists are primarily concerned with news taking place within the patch they cover, so ensure the connection to their area is clear by including:

- **the city/region name** throughout: email subject line, headline and body copy
- quotations from, and offers of interviews with, **local spokespeople** in your press release where possible
- **regionalised statistics** and relevant case studies where possible.

Issue the press release around 9am and follow up on the phone from around 9.30am to 12pm. By the afternoon journalists will generally be too busy to speak to you.

When speaking to broadcast media, emphasise the availability of spokespeople for interview.

Top tips for developing local partnerships

- **Map your potential local partners** by thinking about how the campaign is relevant to them and if they are a good channel to your target audience
- Carry out some **due diligence checks** to make sure the partner organisation is a good fit for your communications
- Approach with a **small ask** in the first instance (e.g. a re-Tweet on social media) then once you have a foot in the door, it will be easier to ask for more
- There's **no 'one size fits all'** way of partnering – really think about why the organisation you are approaching is a particular fit with the campaign
- Contact partners with **plenty of notice** before you want them to do something and then follow up closer to the time with further information.

Events

Face to face meetings and events are amongst the most powerful ways to engage with local communities. A well-run event can give you the opportunity to understand your audiences better and improve the way you communicate with different groups and communities.

Don't forget, a range of free materials are available to download and order to help you promote Cyber Aware and Take Five.

Top tips for running local events

Get there early to set up and scope the lay of the land

Pick an area that's in the sight line of people as they arrive

Use pull up banners, posters, leaflets so it's **clear what your stall is about** on first approach

Think as well about the audience you are trying to attract. Think about **using tablets for surveys** or displaying advice – how age appropriate are the materials on your stall?

Make friends with the people on stalls surrounding you as they can recommend that participants also visit your stand

Ensure you've got **enough people manning your stand** to allow for breaks and can talk to as many people as possible

Don't forget your business cards or handouts so people can find more information afterwards

Try to ask **feedback questions** to understand what the visitors have taken away.

Evaluation

Evaluating campaign activity of any size is vital. It allows you to report successes, learn from what did or didn't work and allows you to constantly improve.

Build evaluation in

from the very beginning, with regular checks as the campaign progresses so you know you're on target

Set SMART objectives

Specific, Measurable, Achievable, Realistic, Time bound – which you can measure and track. E.g. a % increase in enquiries by [enter date] as a result of your campaign

Use existing data

if you have it as a 'baseline' from which you can then track from to identify shifts and trends

Use multiple methodologies and sources

Draw on quantitative (numbers and statistics) and qualitative (longer form answers) information

---

Split out your metrics

Using this model:

Inputs

what specific activity went into the campaign

e.g. cost of leaflets

Outputs

what was delivered

e.g. 2 events and 500 leaflets distributed

Outtakes

what did the audience think or do to make that decision

e.g. the number of people who clicked on your social media posts

Outcomes

the impact of your activity on the ultimate objective

e.g. x% people saying they would adopt the behaviours as a result of the activity measured through feedback forms at the event

For more information, view the GCS Evaluation Framework **here**

Communications campaign examples

Almost all communications activity can be scaled up and down depending on resources. Here are some examples, where bronze is a basic campaign and gold involves more planning and effort but should deliver better results.

	Bronze	Silver	Gold
Social media	Re-tweet someone else's message (e.g. Cyber Aware, Take Five) so your audience see it too. Add a line explaining why this is of interest to your audience	Create a simple schedule of your own posts, adding imagery and hashtags across all your social channels. Signpost to your website page. Co-ordinate with other local forces to deliver the same messages	Create a social media schedule that builds on the insights in a press release. Drip feed the contents over multiple posts across the campaign time period. Track responses and re-tweet positive ones to add momentum
Web content	Include signposts to other campaigns using agreed, consistent advice, e.g. Cyberaware.gov.uk	Add a content page on your website with the messaging and signpost appropriately for more information	Add content to your website which includes the press release, signposting and promote this on the website homepage
Events & supporting materials		Run a local street event in a high footfall area using standard leaflets or other collateral	Run a series of local events with both the public and small businesses. Use bespoke collateral that is co-branded with your force's logo and local messaging
Local partnerships		Reach out to local councils, business networks, community groups for them to support your activity on their own social media	Ask the same local partners to support on other channels (e.g. distributing your leaflets, joint events)
Press engagement		Reach out to local papers to offer top tips/advice articles	Gather local insight to write a press release. Use a local case study if possible. Use spokespeople – both from the local force and the case study if possible

Click here to see best practice examples from other campaigns

Cyber Aware campaign materials

Cyber Aware materials to order

How to order

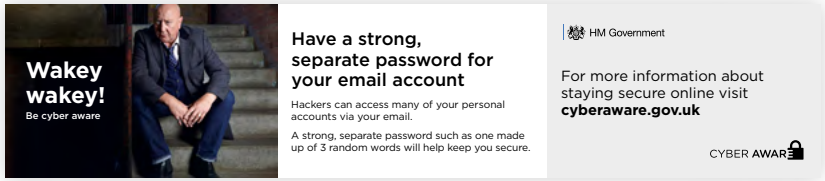
Cyber Aware campaign materials

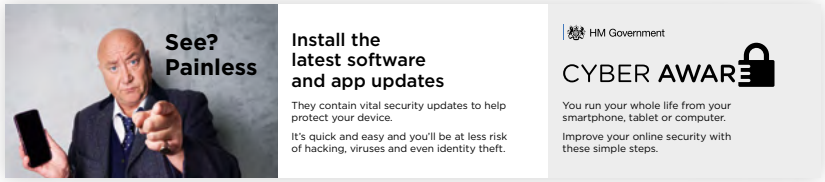
There are a range of materials you can use to promote Cyber Aware and cyber security advice locally, from leaflets to digital banners.

Each type has a name and code to use if you want to order them. They are also all free to download at cyberaware.gov.uk/toolkit Please only order materials as and when you require them.

Bespoke sizes will not be supplied unless in exceptional circumstances. Cyber Aware posters, leaflets, z-cards and pull up banners can all be co-branded with a police force's own logo.

Poster Available in A3 #001A3 or A4 #001A4



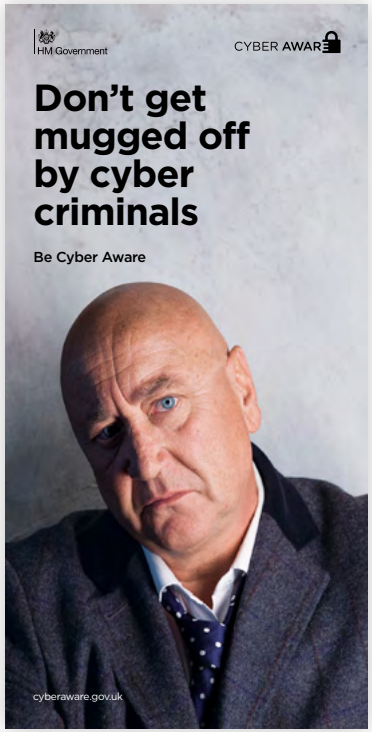


Credit card sized handout #002

A5 leaflet #003

Cyber Aware campaign materials

MPU online banner #004



Pull up banner #006

Skyscraper online banner #007

Email signature #005

How to order

1. Identify the assets you require
Posters, leaflets, z-cards, pull-up banners etc.

2. Complete the order form
Stating the product code, description, quantity you require, and whether you wish this to be co-branded with your organisation's own logo

3. Email the completed order form
Along with your organisation's logo to **cyberaware@homeoffice.x.gsi.gov.uk** for any co-branded materials

- Orders should take up to **15 working days** to process upon receipt of your order form and delivered to the specified address
- For bespoke artwork, urgent orders or questions, please email on cyberaware@homeoffice.x.gsi.gov.uk
- Please order the quantity of materials only when you require them. **Order quantities will be limited** to 300 each of leaflets, posters and z-cards per year per asset for each force and one pull up banner
- All artwork will be supplied to each force to enable future local print runs
- All logos for co-branding will need to be provided in **EPS file format**, these can be obtained from your corporate communications team.

Signposting

1. Take Five
2. Action Fraud/National Fraud Intelligence Bureau (NFIB)
3. The National Cyber Security Centre
4. Cyber Essentials
5. Get Safe Online
6. Neighbourhood Watch
7. Crimestoppers
8. Victim Support

Take Five

As the national campaign offering advice to help the public protect themselves from preventable financial fraud, Take Five offers a range of resources for local police forces to use free of charge.

A new toolkit is available on the Take Five website containing key messages and calls to action which can be woven into your ongoing media work

What's on offer?

- Advice leaflets
- Posters
- Videos
- Digital content for sharing on social media
- PR templates
- Take Five logos and more

Simply visit the Take Five website, takefive-stopfraud.org.uk and download what you need.

Officers are encouraged to use the materials as they are or rebadge them to include their own force's logo. There is no need to request approval all we ask is that you include the Take Five logo. Printing costs will need to be met by your own force/region.

For more information

Tony Blake, Senior Fraud Prevention Officer
Dedicated Card and Payment Crime Unit

T 0207 709 6629 (Office) 07919 166576 (Mobile)
E tony.blake@dcpcu.pnn.police.uk

facebook.com/takefivestopfraud
twitter.com/takefive (@TakeFive)

Leaflet

Web banner

Logos

Posters

Action Fraud/National Fraud Intelligence Bureau (NFIB)

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

Action Fraud is the single point of contact within the UK for reporting all fraud and cyber related crime.

It has an online reporting system and a UK based call centre staffed by experienced call handlers. There's a 24 hour web chat facility on the website, where you can chat online direct with an advisor.

It also operates a 24-hour hotline for businesses, charities and organisations that are suffering a live cyber dependant attack. All you have to do is call 0300 123 2040 and select '9'. This is a unique number for these organisations so that the report can be taken and triaged immediately.

Reports taken by call centre staff are then passed onto the NFIB, which reviews the crime report and makes a decision as to whether there are any leads that would result in a successful criminal investigation. They then make a decision on who within the UK should investigate the crime, whether this would be the local police force, a regional cyber crime unit or the National Crime Agency.

What's on offer?

- Alerts issued by the NFIB on emerging threats and trends - to receive alerts, please click on actionfraudalert.co.uk
- Campaign resources (including social media posts and infographics) on different cyber crime and fraud types at actionfraud.police.uk/resources
- Twitter and Facebook feeds with shareable digital content
- City of London Police have built a free and publicly accessible website - frauddefencetest.com - using the same question matrix as the segmentation's self-assessment tool. This can be used in your own communications for people to complete and obtain tailored Protect advice specific to their segment.

Please continue to encourage the public and small businesses in your communications to report any incidents to Action Fraud.

For more information

actionfraud.police.uk
twitter.com/actionfrauduk (@ActionFraudUK)

Telephone: 0300 123 2040

The National Cyber Security Centre (NCSC)

National Cyber Security Centre
a part of GCHQ

The National Cyber Security Centre is the UK's authority on cyber security and is a part of GCHQ.

It was set up to help protect the UK's critical services from cyber attacks, manage major incidents, and improve the underlying security of the UK Internet through technological improvement and advice to citizens and organisations.

It works together with UK organisations, businesses and individuals to provide authoritative and coherent cyber security advice and cyber incident management, underpinned by world class research and innovation.

NCSC recognises that, despite all efforts to reduce risks and enhance security, incidents will happen. When they do, the NCSC will provide effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future.

NCSC works closely with a national network of police cyber security advisors, based in Regional Organised Crime Units, to deliver our advice coherently and consistently to businesses and individuals.

The Cyber Security Information Sharing Partnership, CiSP, is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK businesses.

When advising small businesses on how to be more cyber secure, please use the Small Business Guide, viewable on page 40. When advising small charities on how to be more cyber secure, please use the Small Charity Guide, available on the NCSC website.

For more information

For **urgent enquiries** phone 0300 020 0964.
For **general enquiries**, use the contact form found at ncsc.gov.uk/contact

Your regional police cyber security advisor can be contacted through your ROCU.

Download the **NCSC Small Business Guide** here

Password guidance for Small Businesses here

Bring Your Own Device guide here

NCSC Cyber Security Incident Response Scheme (CSIR) guide here

twitter.com/ncsc (@NCSC)

Cyber Essentials

Cyber Essentials is a certification scheme designed by the NCSC. The vast majority of cyber attacks exploit basic weaknesses in IT systems, which can easily be fixed. Cyber Essentials helps your organisation guard against the most common cyber threats and demonstrate your commitment to cyber security.

The Government recommends all businesses and organisations that rely on the Internet adopt this scheme, as a minimum. It provides businesses of all sizes with clarity on good, basic cyber security practices that can help companies better protect themselves against the most common cyber threats.

Applying for a Cyber Essentials certificate and displaying the badge provides independent assurance you have correctly implemented basic cyber security protections. It also allows you to bid for Government contracts.

The technical controls set out in Cyber Essentials form part of the broader set of cyber security measures set out in the Ten Steps to Cyber Security guidance.

Visit the website to (a) obtain advice on the 5 technical controls and (b) see how to can get certified.

For more information

Download 10 Steps to Cyber Security

For more information, visit cyberessentials.ncsc.gov.uk

Get Safe Online

www.getsafeonline.org

Get Safe Online is a not-for-profit, public/private sector partnership which exists with the sole aim of helping to keep the UK public and small businesses safe whilst on the internet.

It provides a respected media mouthpiece on ongoing and topical issues and actively contributes to a number of official forums and committees. It is well versed in researching, setting up and manning road shows and regional public advice events and works with a wide range of organisations to deliver resources to their employees and customers alike.

Get Safe Online supports a growing cohort of police forces in providing the information/advice and resources to enable them to deliver outreach activity within their generic and targeted communities across a broad spectrum of topics in depth.

Police Cyber Protect

Police Cyber Protect is an innovative multi-channel programme developed by Get Safe Online working with a number of police forces, The National Police Chiefs' Council and the City of London Police.

Get Safe Online's online content is offered as a self-service facility, providing the tools and support you need to engage both online and face-to-face with the public and SMEs in your area with high-profile live events, plus the starting point to produce hard-hitting, informative online and offline communications resources.

Key benefits include:

- A ready-to-go, proven resource
- A major contribution to your PROTECT strategy
- Lower expense and resource than setting up from scratch
- Fits in the context of your existing communications and infrastructure – can be customised and scaled

For more information

Maria Booker
Director of Police Programme and Events,
Get Safe Online

E maria.booker@getsafeonline.org

Visit getsafeonline.org

twitter.com/GetSafeOnline (@GetSafeOnline)

Neighbourhood Watch

A strong relationship between Neighbourhood Watch and the police at a local, force and national level is vital to reduce crime and keep people safe in their communities.

The network distributes campaign material in relation to cyber, fraud and vulnerability to Force Area Associations for them to use in their own local campaigns. It also uses its social networks and its community messaging tool to promote and share partner information and fraud awareness messages across a network of supporters.

Resources for police forces to draw on include:

- Relevant articles regularly published in a bi-monthly newsletter and distributed to a network of around 330,000 people
- Links to relevant toolkits and resources on the website for network supporters to use locally to support their own activity and campaigns.

For more information

E enquiries@ourwatch.org.uk
T 0116 402 6111

Visit ourwatch.org.uk to find out more

twitter.com/N_watch (@N_Watch)
facebook.com/ourwatch

Crimestoppers

CrimeStoppers.
Speak up. Stay safe.

Every year Crimestoppers helps to stop thousands of crimes.

Crimestoppers is an independent charity that gives people the power to speak up to stop crime, 100% anonymously – whoever they are, wherever they're from, by phone and online, 24/7, 365 days a year. There's no police contact, no witness statements and no courts.

How Crimestoppers can help:

The charity works in partnership with every police force and law enforcement agency in the UK. Every day it sends forces the valuable information it receives anonymously from the public.

Crimestoppers is aware that some people will not, or cannot, talk directly to the police so it works to complement police intelligence, giving the public the power to speak up to stop crime, 100% anonymously.

There is a wide range of resources available, from targeted campaigns to generic marketing materials.

For more information

E cst@crimestoppers-uk.org
T 020 8835 3700

Visit crimestoppers-uk.org to find out more

twitter.com/CrimestoppersUK (@CrimestoppersUK)

Victim Support

Victim Support is an independent charity helping victims of crime across England and Wales.

Victim Support helps thousands of victims of fraud each year. The charity knows from its experience that the impact of this crime can be far reaching. There is not only a financial impact, but the stress caused can have long term effects on people's health.

Victims of fraud can be left feeling angry and ashamed and often blame themselves, but this can happen to anyone.

Victim Support provides free specialist, emotional and practical help to victims of fraud, for as long as needed, whether or not the incident has been reported to the police.

Victims of any type of fraud can refer themselves confidentially through Victim Support's 24/7 support line on 0808 16 89 111.

Victim Support works closely with Police and Crime Commissioners, who in some areas provide specialist services to support victims of cyber crime.

For more information:

24/7 Support line: 0808 16 89 111
Victim Support Press Office: 020 7268 0202

victimsupport.org.uk

facebook.com/victimsupport
twitter.com/VictimSupport (@VictimSupport)

Annex

In collaboration with law enforcement this toolkit has been produced by the Research, Information and Communications Unit (RICU) in the Home Office, who deliver Cyber Aware and jointly deliver with UK Finance - Take Five.

It's also been made possible thanks to contributions from the UK's leading authorities on protecting the public from the growing threat of cyber crime:

- **The National Cyber Security Centre** (NCSC); who are the authoritative voice for UK cyber security, set up to help protect the UK's critical services from cyber attacks, manage major incidents and improve the underlying security of the UK Internet
- **National Cyber Crime Unit** (NCCU), a part of the National Crime Agency (NCA), leads the UK's response to cyber crime, supports partners with specialist capabilities and coordinates the national response to the most serious of cyber crime threats
- **City of London Police** (CoLP), which holds the national police portfolio for Economic Crime and Cyber PROTECT. Visit **cityoflondon.police.uk**
- **Action Fraud**, the UK's national fraud and cyber crime reporting centre. Visit **actionfraud.police.uk**

With additional thanks for input from:

- The Department for Digital, Culture Media and Sports
- The Home Office
- ROCU Protect Network
- Cambridge, Durham, Lancashire, South Wales, Staffordshire, Thames Valley & West Midlands Police Forces
- UK Finance
- Get Safe Online
- Neighbourhood Watch
- Victim Support
- Crimestoppers

Full Cyber Aware advice set with accompanying explanations and further guidance

PRIORITY MESSAGES – USE THESE FIRST

Install the latest software and app updates

- They contain **vital security updates** which help protect your device from viruses and hackers
- Security updates are designed to fix weaknesses in software and apps which could be used by hackers to attack your device and steal your identity. **Installing them as soon as possible helps to keep your device secure**
- You can choose to **install updates at night when you are asleep** and your device is plugged in or set your mobile or tablet to automatically update your apps when you are connected to Wi-Fi and an update is available
- You can also set laptops and desktops to **automatically install software updates** when an update is available.

Use a strong, separate password for your email account

- **Hackers can use your email to access many of your personal accounts**, by asking for your password to be reset, and find out personal information, such as your bank details, address or date of birth, leaving you vulnerable to identity theft or fraud
- Having **strong, separate passwords for your most important accounts** means that if hackers steal your password for one of your less important accounts, they can't use it to access your most important ones
- A good way to create a strong and memorable password is to **use three random words**. Number and symbols can still be used if needed, for example 3redhousemonkeys27!
- Use words which are memorable to you, but **not easy for other people to guess**
- **Hackers know many of the simple substitutions we use**, for example 'Pa55word!' may follow the rules of using letters and symbols, but is easy for hackers to guess
- When available you should use **two-factor authentication** on your email account. It gives it an extra layer of security, as it means your account can only be accessed on a device that you have already registered. When you first log-in with a new device you are asked to complete a second step after entering your password, such as providing your fingerprint or entering a unique code which has been sent to your phone.

Full Cyber Aware advice set with accompanying explanations and further guidance

SECONDARY MESSAGES

Secure your tablet or smartphone with a screen lock

- Give your device an extra layer of security by **setting it to lock when you aren't using it**
- **Screen locks provide an extra layer of security** to your device, as each time you want to unlock it or turn it on, you will need to enter a PIN, pattern, password or fingerprint. This means if someone gets hold of your device they can't access the data on your device without entering your password, pattern, PIN or fingerprint
- **Don't use '1,2,3,4' or an 'L' shaped pattern** which are easy for other people to guess.

Don't use public Wi-Fi to transfer sensitive information such as card details

- Hackers can set-up fake wi-fi hotspots, which might enable them to intercept sensitive information you are transferring online.

Always back-up your most important data

- **Safeguard your most important data** such as your photos and key documents by backing them up to an external hard drive or a cloud-based storage system
- If your device is infected by a virus, malicious software (malware) or accessed by a hacker, **your data may be damaged, deleted or held to ransom by ransomware**, which means you won't be able to access it. Backing up your data means you have another copy of it, which you can access
- Malware or ransomware can infect external hard drives which are connected to your device. Make sure that the external hard drive you are using to back-up your data is not permanently connected to the device you are backing up either physically or over a local network connection.

Full Cyber Aware advice set with accompanying explanations and further guidance

Beware of fake websites

- Cyber criminals can **set up fake websites** to try and get you to share sensitive information, such as your bank account details or passwords, or download malware (malicious software) which can infect your device and damage or delete the data you have on it
- Always **check that the website address of the site you are using is correct**. Cyber criminals can create fake website addresses which look very similar to the real website address, for example by misspelling the name of the company. Wherever possible type the address of the website directly into the browser yourself or search for the website using a search engine
- A website **can still be a fake website if it has a padlock and/or 'https' in the address bar**. These simply mean data is encrypted when transferred over the internet, not that the website itself is trustworthy.

Never click on suspicious links or attachments

- **Beware of suspicious emails**. Even if they seem to come from a company or person you know, contact them by other means to check they are genuine
- An **email address can be faked**. If the message is unexpected or unusual, even if an email appears to be from someone or a company you know, contact the sender directly via another method and check that they have sent it to you
- **Never respond** to messages that ask for your **personal or financial details**
- If you **suspect the email is a scam** don't reply to the sender, as this will let them know that your email address is active and will lead to you receiving more spam emails
- **Flag the email as spam** with your email provider and delete it. Your email provider will use this information to help them reduce the number of spam emails which are received.

Don't 'jailbreak' or 'root' your smartphone

(Young & risky audience only)

- Jailbreaking or rooting turns off software restrictions placed by the manufacturer, allowing you to download and install apps which aren't available through official app stores
- However, turning off the software restrictions leaves your phone **vulnerable to malicious software or applications** (malware), which can infect your phone and damage or delete the data you have on it
- Jailbreaking will also **invalidate your phone's warranty** and mean that you will no longer receive software updates, which often contain security updates designed to fix weaknesses in software and apps which could be used by hackers to attack your device.

For more detailed advice for small businesses, please use the NCSC's Small Business Guide.

NCSC – Cyber Security Small Business Guide

National Cyber Security Centre
a part of GCHQ

Cyber Security
Small Business Guide

This advice has been produced to help small businesses protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/smallbusiness** .

Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

- **Identify what needs to be backed up.** Normally this will comprise documents, photos, emails, contacts, and calendars, kept in a few common folders. Make backing up part of your everyday business.
- **Ensure the device containing your backup is *not* permanently connected** to the device holding the original copy, neither physically nor over a local network.
- **Consider backing up to the cloud.** This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

- **Switch on PIN/password protection/fingerprint recognition** for mobile devices.
- Configure devices so that when lost or stolen they can be **tracked**, **remotely wiped** or **remotely locked**.
- Keep your **devices** (and all **installed apps**) **up to date**, using the '**automatically update**' option if available.
- When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs**.
- **Replace devices that are no longer supported by manufacturers** with up-to-date alternatives.

Preventing malware damage

You can protect your organisation from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

- **Use antivirus** software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.
- **Patch all software and firmware** by promptly applying the latest software updates provided by manufacturers and vendors. Use the '**automatically update**' option where available.
- **Control access to removable media** such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.
- **Switch on your firewall** (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

- Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges**. This will reduce the impact of successful phishing attacks.
- **Scan for malware** and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).
- Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

- Make sure all laptops, MACs and PCs **use encryption products** that require a password to boot. Switch on **password/ PIN protection** or **fingerprint recognition** for mobile devices.
- **Use two factor authentication (2FA)** for important websites like banking and email, if you're given the option.
- **Avoid using predictable passwords** (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).
- **If you forget your password** (or you think somebody else knows it), tell your IT department as soon as you can.
- **Change** the manufacturers' default passwords that devices are issued with, before they are distributed to staff.
- **Provide secure storage** so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.
- **Consider using a password manager**, but only for your less important websites and accounts where there would be no real permanent damage if the password was stolen.

For more information go to www.ncsc.gov.uk @ncsc

To view the infographic, visit **ncsc.gov.uk/guidance/cyber-security-small-business-guide-infographic**

Segmentation

The table below summarises the Serious and Organised Crime Segmentation groups with associated characteristics.

	Segment	Size (% pop)	Personality	Protection	Gender	Social Group	Age	Household companion	Highest qualification	Internet use
A	**Already protected**	13%	Considered Suspicious Prepared	High - offline High - online High - financial	F	n/a	30-49 55-69	Partner, Partner & Children	School leavers, professional qualifications	Daily and less
B	**Online novice**	9%	Disorganised Fatalistic Technophobe	High - offline Low - online High - financial	F	DE	65+	Alone, Partner	None	Very rarely online
C1	**Trusting**	15%	Trusting Easily swayed Non-confrontational	Medium - offline Medium - online Medium - financial	F	n/a	n/a	Partner, Children, Extended family	n/a	Daily
C2	**Unconcerned & somewhat protected**	18%	Risk taking Impetuous Morally ambiguous	Medium - offline Medium - online Medium - financial	M	n/a	16-44	Parents	School leavers	Throughout the day
C3	**Relatively savvy**	20%	Not impetuous Willing to challenge Ethical	Medium - offline High - online Medium - financial	M+F	A	n/a	n/a	Graduate Postgraduate	n/a
D1	**Unsuspecting & unprotected**	8%	Not considered Non-confrontational Easily swayed	Low - offline Low - online Low - financial	M+F	n/a	16-29	Parents, Siblings, Extended family	A Levels Graduate	Throughout the day
D2	**Unconcerned & unprotected**	9%	Morally ambiguous Confrontational Risk taking	Low - offline Low - online Low - financial	M+F	AB	16-29	Parents	A Levels Postgraduate	n/a
E	**Unaware**	7%	Fatalistic Non-confrontational	Medium - offline Low - online Medium - financial	F	DE	70+	Alone, Partner, Children & Extended family	None	Never online

Click here for more information

Segmentation – ideas on how to use it

Depending on your ultimate communications goal, the below table gives you an idea of how you could use segmentation to deliver different types of cyber and fraud education campaigns:

Bronze	Silver	Gold
Identify the segments and crime vulnerabilities that are prevalent in your local force area	Look at your local Action Fraud demographic and crime type data to identify links with the segmentation groups that victims might be in	Create maps of local areas of your most vulnerable groups, or groups you wish to target using access to your force's Mosaic licence and data (if this is available)
Working with your Regional Organised Crime Unit (ROCU) and corporate communication team, build a simple campaign, such as handing out Cyber Aware co-branded leaflets in your local areas where D2s live - those 'unconcerned and unprotected' about cyber crime	From this and their contact details consider follow-up resource appropriate initiatives like an email 'mail merge', phone call or house visit to the most vulnerable groups, signposting to Cyber Aware and Take Five for more information	Have Officers/Staff, PCSOs, Cadets, Special Constables and volunteers deliver relevant advice leaflets to addresses highlighted by the local maps (e.g. Cyber Aware leaflets to postcodes where D2s live)
	Ask the public you engage with to work through the Public Interventions Model's dedicated self-assessment tool. Use frauddefencetest.com or contact cyberaware@homeoffice.x.gsi.gov.uk for more information on obtaining an offline version (if required)	Build on your awareness campaigns by working with local partners such as Age UK to set up or build segmentation into local targeted initiatives e.g. a 'cyber coffee morning' for the elderly residents or in-branch SME events at local banks
	Run bigger, integrated campaigns, such as running street clinics at high footfall areas in neighbourhoods with a high amount of vulnerable groups, and providing spokespeople for local press activity	Ask the same local partners to support on other channels (e.g. distributing your leaflets, joint events)
	Reach out to local papers to offer top tips/advice articles	Gather local insight to write a press release. Use a local case study if possible. Use spokespeople – both from the local force and the case study if possible

Segmentation - case studies

Serious and Organised Crime Segmentation Tool in practice – case study

Aylesbury, Thames Valley Police – Segment mapping

Due to the segmentation being matched against Mosaic[1] profiles in its research stage it is relatively easy to make broad judgements based on an area's Mosaic profile to match it with the corresponding segmentation group(s).

For example, in Aylesbury town centre in the Thames Valley Police area, vulnerable segment groups were mapped to postcode level using Mosaic profile matching.

These maps allowed local policing teams to **actively target tailored protective advice to addresses with potentially less protected and vulnerable residents,** including:

- A co-branded and bespoke localised Cyber Aware leaflet
- Tailored advice available to officers via an app which they could convey face-to-face whilst out 'door knocking'
- Local officers getting the public signed up to their local Neighbourhood Alert scheme as part of their existing events and meetings, so they would receive follow-up advice and local crime information.

Example Aerial view of 'D2 unconcerned and Unprotected', Aylesbury

1 Mosaic, provided by Experian is a cross-channel classification system. It helps understand consumers in detail by providing rich, accurate data and a robust methodology. It synthesizes over 850 million pieces of information to create an easy to understand segmentation that allocates 49 million individuals and 26 million households into one of 15 Groups and 66 detailed Types - experian.co.uk

Social media templates and top tips

Twitter posts

Twitter has a character limit of 280 characters so **some words will need to be shortened**

Using hashtags will help your post to **show up more frequently** in Twitter search

Videos tend to perform very well on social media so include these where you can

Date & time	Post	Image
22/2/17 09:00	2m Brits were victims of #cybercrime last year https://www.youtube.com/watch?v=b4WBnVDPRXw. Be #cyberaware. Find out how to stay secure: cyberaware.gov.uk	<insert link to Vox pop video – Main>
22/2/17 09.45	Only 32% of Brits follow Gov advice to use #3randomwords to create a strong password. Be #cyberaware https://www.youtube.com/watch?v=b4WBnVDPRXw	<insert link to Vox pop video – Main>
22/2/17 10:15	82% of households have double locks or deadlocks, but only 32% of Brits follow Gov advice to use #3randomwords to create a strong password	

Include stats where possible to add interest to your content

Ensure each post has a **call to action**

Every post should include a picture or video link where possible

Social media templates and top tips

Facebook posts

As with Twitter, videos, pictures or links **should be used for every post**

Date & time	Post	Image
22/2/17 09:00	2m Brits were a victim of cyber crime last year. Be Cyber Aware & find out how to stay secure at cyberaware.gov.uk https://www.youtube.com/watch?v=b4WBnVDPRXw	<insert link to vox pop video: Main>
22/2/17 13:00	Did you know 82% of households have double locks or deadlocks and 89% have window locks, but only 32% of Britons are following the Government's latest password advice to use three random words to create a strong password? Visit the Cyber Aware website for tips to keeping secure online: cyberaware.gov.uk	<insert link to Vox pop video – Main>

A Facebook post can be up to 63,206 characters long so there is **more room for longer posts**

Press release template and top tips

Page one

Add relevant logo in top left hand corner

In journalism and public relations, a news embargo or press embargo is a request or requirement that the information or news provided by that source not be published until a certain date.

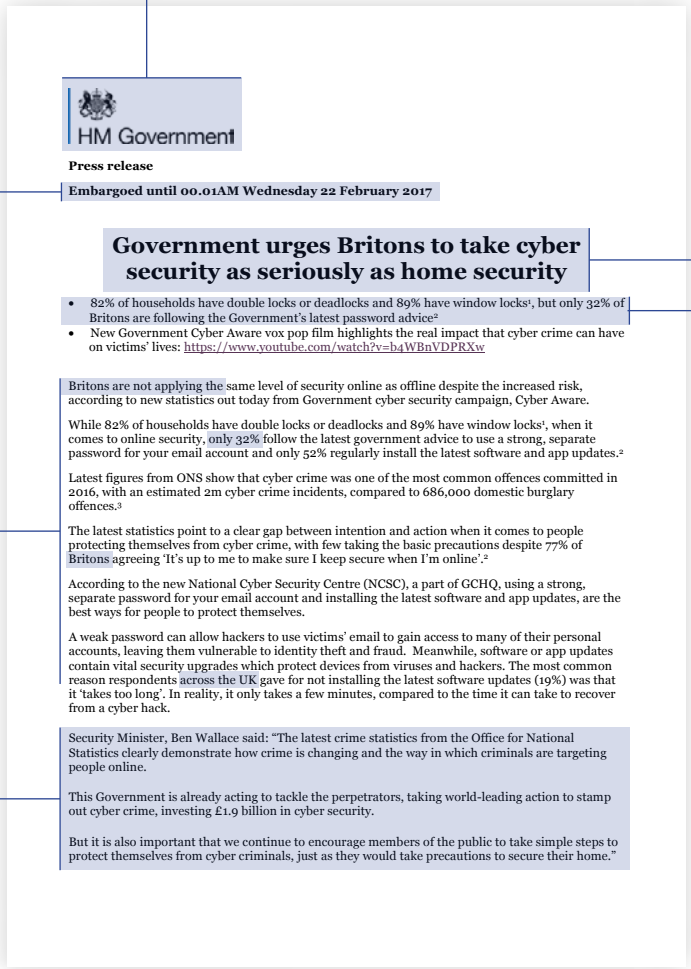
If your press release is embargoed, you should mention it here, **including the exact date and time the embargo is due to lift**

These would need to be **regionalised** for a regional release e.g.

'Mancunians are not applying the…'
'Only 32% of Mancunians follow...'

At this point in the press release you can include **quotes from relevant spokespeople**. If your release is a regional one we would suggest you include a quote from a regional spokesperson.

Quotes should sound as though a real person is speaking and **not include any jargon or technical language**. You should always reference the person's full name and job title



HM Government

Press release

Embargoed until 00.01AM Wednesday 22 February 2017

Government urges Britons to take cyber security as seriously as home security

- 82% of households have double locks or deadlocks and 89% have window locks[1], but only 32% of Britons are following the Government's latest password advice[2]
- New Government Cyber Aware vox pop film highlights the real impact that cyber crime can have on victims' lives: https://www.youtube.com/watch?v=b4WBnVDPRXw

Britons are not applying the same level of security online as offline despite the increased risk, according to new statistics out today from Government cyber security campaign, Cyber Aware.

While 82% of households have double locks or deadlocks and 89% have window locks[1], when it comes to online security, only 32% follow the latest government advice to use a strong, separate password for your email account and only 52% regularly install the latest software and app updates.[2]

Latest figures from ONS show that cyber crime was one of the most common offences committed in 2016, with an estimated 2m cyber crime incidents, compared to 686,000 domestic burglary offences.[3]

The latest statistics point to a clear gap between intention and action when it comes to people protecting themselves from cyber crime, with few taking the basic precautions despite 77% of Britons agreeing 'It's up to me to make sure I keep secure when I'm online'.[2]

According to the new National Cyber Security Centre (NCSC), a part of GCHQ, using a strong, separate password for your email account and installing the latest software and app updates, are the best ways for people to protect themselves.

A weak password can allow hackers to use victims' email to gain access to many of their personal accounts, leaving them vulnerable to identity theft and fraud. Meanwhile, software or app updates contain vital security upgrades which protect devices from viruses and hackers. The most common reason respondents across the UK gave for not installing the latest software updates (19%) was that it 'takes too long'. In reality, it only takes a few minutes, compared to the time it can take to recover from a cyber hack.

Security Minister, Ben Wallace said: "The latest crime statistics from the Office for National Statistics clearly demonstrate how crime is changing and the way in which criminals are targeting people online.

This Government is already acting to tackle the perpetrators, taking world-leading action to stamp out cyber crime, investing £1.9 billion in cyber security.

But it is also important that we continue to encourage members of the public to take simple steps to protect themselves from cyber criminals, just as they would take precautions to secure their home."

Make sure your headline is **succinct and clear** as this is your opportunity to pique the interest of the journalists reading it. They should be able to instantly understand what the story is about from reading your headline

Subheadings can add context to your headline and include additional information there wasn't space for in the headline.

If your story has a focus on stats then the headline can give the topline story and the **subheads can give the stats themselves**

Note

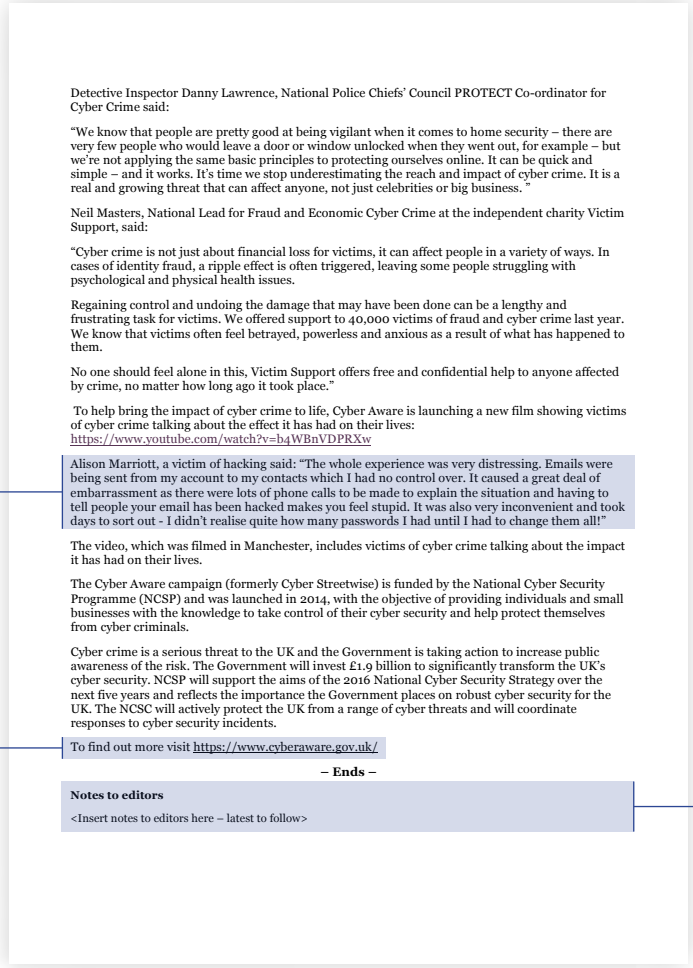
When writing regionalised releases it is important to **include a mention of that region** in the headline and email subject line so the regional journalists receiving it realise the story will be relevant to them.

Press release template and tips

Page two

If you have **case study quotes** available this is often a helpful way of bringing the story to life

Include a call to action / signpost by ensuring you've added a hyperlink



Detective Inspector Danny Lawrence, National Police Chiefs' Council PROTECT Co-ordinator for Cyber Crime said:

"We know that people are pretty good at being vigilant when it comes to home security – there are very few people who would leave a door or window unlocked when they went out, for example – but we're not applying the same basic principles to protecting ourselves online. It can be quick and simple – and it works. It's time we stop underestimating the reach and impact of cyber crime. It is a real and growing threat that can affect anyone, not just celebrities or big business. "

Neil Masters, National Lead for Fraud and Economic Cyber Crime at the independent charity Victim Support, said:

"Cyber crime is not just about financial loss for victims, it can affect people in a variety of ways. In cases of identity fraud, a ripple effect is often triggered, leaving some people struggling with psychological and physical health issues.

Regaining control and undoing the damage that may have been done can be a lengthy and frustrating task for victims. We offered support to 40,000 victims of fraud and cyber crime last year. We know that victims often feel betrayed, powerless and anxious as a result of what has happened to them.

No one should feel alone in this, Victim Support offers free and confidential help to anyone affected by crime, no matter how long ago it took place."

To help bring the impact of cyber crime to life, Cyber Aware is launching a new film showing victims of cyber crime talking about the effect it has had on their lives: https://www.youtube.com/watch?v=b4WBnVDPRXw

Alison Marriott, a victim of hacking said: "The whole experience was very distressing. Emails were being sent from my account to my contacts which I had no control over. It caused a great deal of embarrassment as there were lots of phone calls to be made to explain the situation and having to tell people your email has been hacked makes you feel stupid. It was also very inconvenient and took days to sort out - I didn't realise quite how many passwords I had until I had to change them all!"

The video, which was filmed in Manchester, includes victims of cyber crime talking about the impact it has had on their lives.

The Cyber Aware campaign (formerly Cyber Streetwise) is funded by the National Cyber Security Programme (NCSP) and was launched in 2014, with the objective of providing individuals and small businesses with the knowledge to take control of their cyber security and help protect themselves from cyber criminals.

Cyber crime is a serious threat to the UK and the Government is taking action to increase public awareness of the risk. The Government will invest £1.9 billion to significantly transform the UK's cyber security. NCSP will support the aims of the 2016 National Cyber Security Strategy over the next five years and reflects the importance the Government places on robust cyber security for the UK. The NCSC will actively protect the UK from a range of cyber threats and will coordinate responses to cyber security incidents.

To find out more visit https://www.cyberaware.gov.uk/

– Ends –

Notes to editors

<Insert notes to editors here – latest to follow>

In notes to editors include:

- Information on any **stats references**

- Details for the **main point of contact** (email and telephone)

- **More information** on the campaign

Best practice examples

Here are some examples of successful campaigns that have delivered real impact:

Social media

Cyber Aware's 'Three Random Word' campaign

- Consistent message brought to life with fun and engaging hooks
- Imagery to boost engagement
- Schedule developed and shared in advance for partners to support

Events and collateral

Get Safe Online's community event

- High impact co-branded collateral
- Knowledgeable staff answering questions
- Consistent advice across all materials
- Surveys done via feedback forms to track awareness and behavioural shifts

Best practice examples

Here are some examples of successful campaigns that have delivered real impact:

Website content

- Consistent content and messaging but framed in the partner's own words

Local press engagement

- Using a local angle and local media contacts
- Consistent messaging made relevant to the target audience
- Local spokesperson

Contact details

For more information, or to contribute to the toolkit in the future, please get in touch using the details provided below.

Please follow these links to our Twitter and Facebook feeds:

twitter.com/cyberawaregov (@CyberAwareGov)

facebook.com/cyberawaregov

For press enquiries, please contact the Home Office Press Office on **020 7035 3535**

For any other queries, email cyberaware@homeoffice.x.gsi.gov.uk

HM Government

CYBER AWARE

TAKE FIVE TO STOP FRAUD™