



SAFE, SECURE AND PROSPEROUS: A CYBER RESILIENCE STRATEGY FOR SCOTLAND

COMMUNICATIONS TOOLKIT



Overview

Introduction

How to communicate the key messages

Systems of basic and detailed advice and support

Trusted sources and key partners

- Police Scotland
- NCSC
- Take 5 & Get Safe Online

Cyber Essentials & CISP

Key messages to promote

Promoting key resources

Key contacts

Overview

The importance of cyber resilience in Scotland has never been greater. Digital technologies bring enormous opportunities but they also bring with them new threats and vulnerabilities that we must take decisive action to manage.

“[Safe, Secure and Prosperous: A Cyber Resilience Strategy for Scotland](#)” was published in 2015. It sets an ambition for Scotland to become a world leading nation in cyber resilience. The strategy is supported by a suite of action plans that have been developed and implemented to achieve our ambitions.

The action plans are as follows:

- [Economic Opportunity Action Plan](#): setting out actions to support Scotland’s business, enterprise and academic communities to mature into a thriving, coherent cyber security cluster.
- [Learning and Skills Action Plan](#): setting out actions to support the development of cyber resilient behaviours amongst our population, and to build a skilled and growing cyber security profession for Scotland.
- [Public Sector Action Plan](#): setting out actions to ensure that Scotland's public bodies have in place a common baseline of good cyber resilience practice.
- [Private Sector Action Plan](#): setting out a programme of work in partnership with Scotland's private sector to help raise fundamental levels of cyber resilience.
- [Third Sector Action Plan](#): setting out a detailed programme of work in partnership with Scotland's Third sector to help raise fundamental levels of cyber resilience.



COMMUNICATION TOOLKIT

Overview

Introduction

How to communicate the key messages

Systems of basic and detailed advice and support

Trusted sources and key partners

- Police Scotland
- NCSC
- Take 5 & Get Safe Online

Cyber Essentials & CISP

Key messages to promote

Promoting key resources

Key contacts

Introduction

We live in one of the most open digital societies in the world making us vulnerable to ever evolving cyber-attacks which seek to defraud, extort, steal information, damage or disrupt businesses. It's not a case of 'if' but 'when'. Cybercrime is significant and growing, and is one of the biggest threats to the UK that can cause both financial and reputational damage. More needs to be done to ensure individuals, public sector, private sector and third sector organisations are aware of current threats to help them take responsibility to protect themselves.



There is a wealth of well-intended advice and guidance available on cybercrime and cyber fraud, so much so that it can be very confusing. It is therefore important that cyber safe messages are communicated in the right way for different audiences and from an authoritative source.

By communicating the cyber basics effectively, we can support the development of a culture of cyber resilience and, at the same time, create the necessary conditions to ensure Scotland achieves its ambition of becoming a world-leading cyber resilient nation. The Scottish Government is clear it cannot achieve a strong, cyber-resilient Scotland on its own. We absolutely need the help of those who are better placed to talk to target audiences about cyber resilience. Consistently communicating the simple, protective behaviours outlined here will help bridge the gap between awareness, action and, importantly, encourage the reporting of crime.

This toolkit is designed to provide your communications team with the right tools and resources to deliver impactful and consistent communications from trusted sources.

COMMUNICATION TOOLKIT

Overview

Introduction

How to communicate the key messages

Systems of basic and detailed advice and support

Trusted sources and key partners

- Police Scotland
- NCSC
- Take 5 & Get Safe Online

Cyber Essentials & CISP

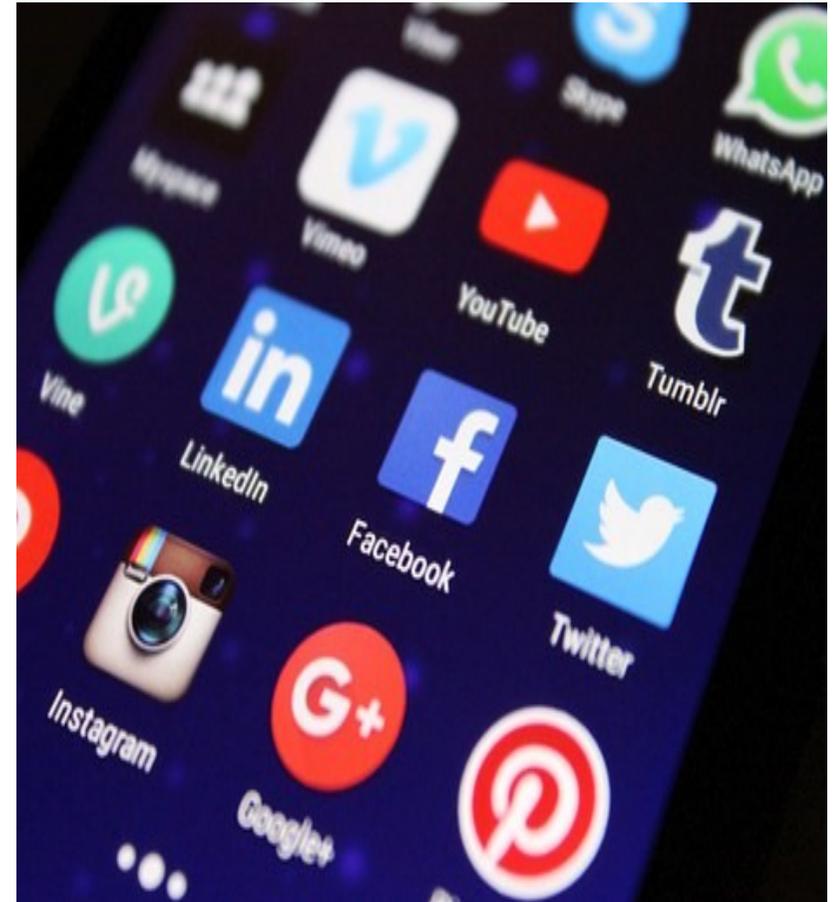
Key messages to promote

Promoting key resources

Key contacts

How to communicate the key messages

- Keep it simple and clear.
- Use hyperlinks to trusted sources for further information / trusted voices.
- Tailor your message to your audience.
- Repeat messages through different communications channels. E.g. Intranet, blog, twitter, email
- Be topical with your advice — e.g. holiday season (booking holidays etc).
- Use images to capture your audience's attention.
- Don't forget to add a hashtag as they can be an effective way for people to search for content which is specific to their original query.



COMMUNICATION
TOOLKIT

Overview

Introduction

How to communicate the key messages

Systems of basic and detailed advice and support

Trusted sources and key partners

- Police Scotland
- NCSC
- Take 5 & Get Safe Online

Cyber Essentials & CISP

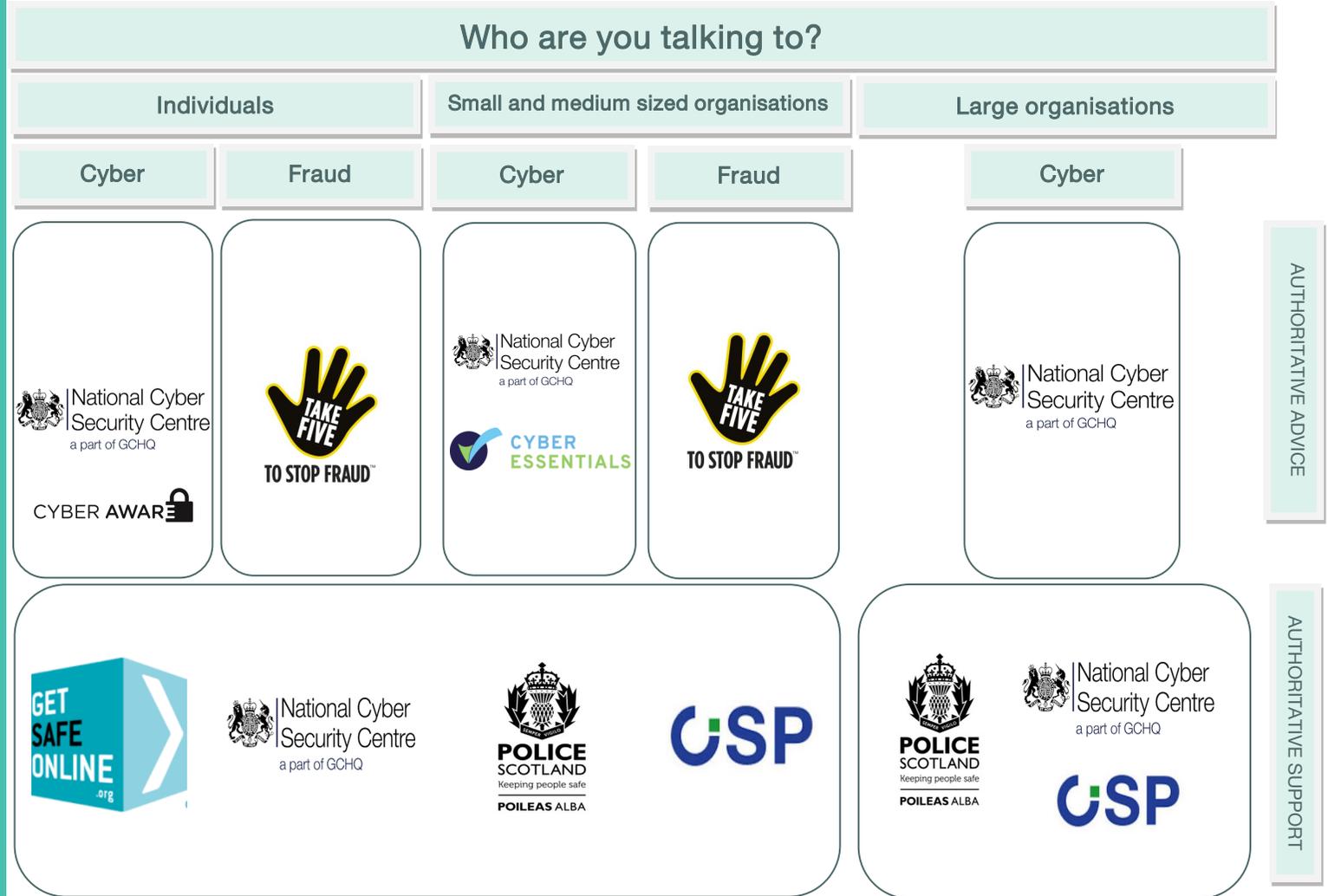
Key messages to promote

Promoting key resources

Key contacts

Systems of basic and detailed advice and support

This diagram aims to map the relevant campaigns/services to specific audiences and for specific purposes. (More information about these are on next page).



COMMUNICATION TOOLKIT

Overview

Introduction

How to communicate the key
messages

Systems of basic and detailed
advice and support

Trusted sources and key
partners

- Police Scotland
- NCSC
- Take 5 & Get Safe
Online

Cyber Essentials & CISP

Key messages to promote

Promoting key resources

Key contacts

Trusted sources and key partners



**POLICE
SCOTLAND**
Keeping people safe
POILEAS ALBA

Police Scotland's purpose is to improve the safety and wellbeing of people, places and communities in Scotland. Its focus is on Keeping People Safe which is at the heart of everything that it does.

The effects of cybercrime can be devastating, and victims can be reluctant to report incidents, often due to feeling embarrassed or unsure as to whether it is a crime, or indeed a police matter.

As part of Police Scotland's strategy to ensure all communities are better protected against the increasing cyber threat, its aim is to continue to engage with the public and its partners, across all sectors, encouraging the reporting of cybercrime which assists in the development and delivery of effective prevention and awareness programs.

Raising awareness and knowledge across all communities is crucial in tackling the cyber threat. Partnership working alongside Police Scotland's growing network of Web Constables across Scotland, ensures communities have increased resilience, capability and support to keep safe and secure in the online environment.

Key Messages to share more generally:

Please call **101** to report any crime.

For further advice visit the '**Keep Safe**' page of the Police Scotland website, or for information on how Police Scotland can support Prevention work in your area, please contact the Safer Communities department via 101 or the Contact Us section of the website – <https://www.scotland.police.uk/contact-us/>

COMMUNICATION

TOOLKIT

Overview

Introduction

How to communicate the key messages

Systems of basic and detailed advice and support

Trusted sources and key partners

- Police Scotland

- NCSC

- Take 5 & Get Safe

Online

Cyber Essentials & CISP

Key messages to promote

Promoting key resources

Key contacts

Trusted sources and key partners



National Cyber
Security Centre
a part of GCHQ

[National Cyber Security Centre](#) (NCSC) is the UK's authority on cyber security and is a part of GCHQ.

It provides a single point of contact for SMEs, charities, larger organisations, government agencies, the general public and departments. They work collaboratively with other law enforcement, defence, the UK's intelligence and security agencies and international partners.

The NCSC 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.

Key resources

[Top Tips For Staff](#)

[NCSC 10 Steps to Cyber Security](#)

[Cyber Security: Small Business Guide](#)

[Small Business Guide: Response & Recovery](#)

[Cyber Security: Small Charity Guide](#)

[Board toolkit](#)

[Password guidance: Simplifying your approach](#)

[Bring Your Own Device Guide](#)

[NCSC's CiSP](#)

COMMUNICATION TOOLKIT

Overview

Introduction

How to communicate the key messages

Systems of basic and detailed advice and support

Trusted sources and key partners

- Police Scotland
- NCSC
- **Take 5 & Get Safe Online**

Cyber Essentials & CISP

Key messages to promote

Promoting key resources

Key contacts

Trusted sources and key partners

Here are some authoritative sources where you can get useful advice and guidance.

[Cyber Aware](#) : Cyber Aware is the UK Government's campaign to help individuals and smaller organisations protect themselves online.



[Get Safe on Line](#): a free resource providing practical advice to individuals and businesses on how to protect themselves while online and using digital technologies.



[My Gov](#): The Scottish Government's site with advice on how to keep your business safe online.



Scottish Government
Riaghaltas na h-Alba
gov.scot

[Gov.scot](#) Scottish Government's policy on Cyber resilience.

[Take Five to Stop Fraud](#): a UK awareness campaign led by FFA UK (part of UK Finance), and delivered with and through a range of partners in the UK payments industry, financial services firms, law enforcement agencies, telecommunication providers, commercial, public and third sector.



COMMUNICATION TOOLKIT

Overview

Introduction

How to communicate the key
messages

Systems of basic and detailed
advice and support

Trusted sources and key
partners

- Police Scotland
- NCSC
- Take 5 & Get Safe
Online

Cyber Essentials & CISP

Key messages to promote

Promoting key resources

Key contacts

Cyber Essentials & CISP



[Cyber Essentials](#) is a Government-backed and industry-supported scheme that helps businesses protect themselves against the growing threat of cyber attacks and provides a clear statement of the basic controls organisations should have in place to protect them.

Key messages to share

- Cyber Essentials helps you to guard against the most common cyber threats.
- 5 steps to smarter security with Cyber Essentials .
- Demonstrate your commitment to cyber security with NCSC's Cyber Essentials.

<https://www.cyberessentials.ncsc.gov.uk/>



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 business.

Key messages to share

- Share cyber threat information in real time in a secure, confidential and dynamic environment with CISP

For more info

<https://www.ncsc.gov.uk/section/keep-up-to-date/cisp>

If you want further details or have a specific query about CISP then please email cisp@ncsc.gov.uk.

Overview

Introduction

How to communicate the key messages

Systems of basic and detailed advice and support

Trusted sources and key partners

- Police Scotland
- NCSC
- Take 5 & Get Safe Online

Cyber Essentials & CISP

Key messages to promote

Promoting key resources

Key contacts

Key messages to promote (1)

Below are some key social media materials for you to adapt and use as appropriate via social media channels.

Passwords

“Choose a strong separate password for each of your online accounts. Use the @NCSC method and choose three random words. #CyberAwareScotland”

“Screen locks—Always use a screen lock or password to protect your phones and tablets
#CyberAwareScotland”

“2FA is quick and simple way to add an extra layer of security to your online accounts. Find out how to turn on this feature here: <https://www.telesign.com/turnon2fa/> #CyberAwareScotland”

Phishing

“Do not click on links in posts, tweets or direct messages unless you are 100% certain that they are genuine and well-intentioned. #CyberAwareScotland”



Overview

Introduction

How to communicate the key
messages

Systems of basic and detailed
advice and support

Trusted sources and key
partners

- Police Scotland
- NCSC
- Take 5 & Get Safe
Online

Cyber Essentials & CISP

Key messages to promote

Promoting key resources

Key contacts

Key messages to promote (2)

Below are some key social media materials for you to adapt and use as appropriate via social media channels.

Phishing

“Have you ever received an email from someone claiming to be your bank? Always question uninvited approaches and never give out personal or financial details #CyberAwareScotland”

Always have a Back-Up

“Information held on your computer could be irreplaceable. Backing up your data often will ensure that you have more than one copy and could recover data quickly. #CyberAwareScotland”

Wi-Fi Hotspots

“Cyber criminals can set up Wi-Fi hotspots enabling them to intercept and steal the data you send online. Never send confidential or financial information over unfamiliar Wi-Fi. #CyberAwareScotland”



Overview

Introduction

How to communicate the key messages

Systems of basic and detailed advice and support

Trusted sources and key partners

- Police Scotland
- NCSC
- Take 5 & Get Safe Online

Cyber Essentials & CISP

Key messages to promote

Promoting key resources

Key contacts

Key messages to promote (3)

Below are some key social media materials for you to adapt and use as appropriate via social media channels.

Install software and application updates

“Cyber criminals use weaknesses in software and apps to attack your devices. Installing updates will help keep your devices secure. #CyberAwareScotland”

Reporting

“If you become a victim of cybercrime, you can report this to @policescotland by visiting a station or calling 101 (non-emergency) <https://www.scotland.police.uk/contact-us/report-cybercrime> #CyberAwareScotland”

Stay safe online

“Check out @NCSC top cyber tips for staying safe online. <https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online> #CyberAwareScotland”



Overview

Introduction

How to communicate the key messages

Systems of basic and detailed advice and support

Trusted sources and key partners

- Police Scotland
- NCSC
- Take 5 & Get Safe Online

Cyber Essentials & CISP

Key messages to promote

Promoting key resources

Key contacts

Promoting key resources (1)

Below are some messages to use on social media to promote key resources

Top Tips For Staff

Regardless of the size or type of organisation you work for, it's important to understand why you might be vulnerable to cyber attack, and how to defend yourself.

Check out @NCSC top tips #CyberAwareScotland

<https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available>

NCSC 10 Steps to Cyber Security

When dealing with the practicalities of cyber security it's extremely useful to understand what exactly you're protecting against. Find out more on @NCSC 10 steps you should make with cyber security

#CyberAwareScotland <https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security>

Cyber Security: Small Business Guide

Cyber security needn't be a daunting challenge for small business owners. Following the five quick and easy steps outlined in the guide below could save time, money and even your business' reputation.

<https://www.ncsc.gov.uk/collection/small-business-guide> #CyberAwareScotland



Overview

Introduction

How to communicate the key messages

Systems of basic and detailed advice and support

Trusted sources and key partners

- Police Scotland
- NCSC
- Take 5 & Get Safe Online

Cyber Essentials & CISP

Key messages to promote

Promoting key resources

Key contacts

Promoting key resources (2)

Below are some messages to use on social media to promote key resources

Small Business Guide: Response & Recovery

Find out how to prepare your response and plan your recovery to a cyber incident.

<https://www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery>

#CyberAwareScotland

Cyber Security: Small Charity Guide

Feel better-armed to face the challenges that come with such rapid technological advancement and protect your organisation from cyber crime.

<https://www.ncsc.gov.uk/collection/charity>

#CyberAwareScotland

Board toolkit

Cyber security is central to the health and resilience of an organisation. Cyber Security needs to be discussed at board level. Find out how you can make this happen

<https://www.ncsc.gov.uk/collection/board-toolkit>

#CyberAwareScotland



COMMUNICATION TOOLKIT

Overview

Introduction

How to communicate the key messages

Systems of basic and detailed advice and support

Trusted sources and key partners

- Police Scotland
- NCSC
- Take 5 & Get Safe
Online

Cyber Essentials & CISP

Key messages to promote

Promoting key resources

Key contacts

Key contacts

Below are some key contacts to follow on social media and blogs.

Who to follow on Twitter:

Scottish Government Cyber Resilience Unit [@CyberResScot](https://twitter.com/CyberResScot)

National Cyber Security Centre [@NCSC](https://twitter.com/NCSC)

Police Scotland [@policescotland](https://twitter.com/policescotland)

Cyber Aware [@cyberawaregov](https://twitter.com/cyberawaregov)

Get Safe Online [@GetSafeOnline](https://twitter.com/GetSafeOnline)

Take Five [@TakeFive](https://twitter.com/TakeFive)

Please follow these Blog feeds:

<https://blogs.gov.scot/cyber-resilience/>

<https://www.ncsc.gov.uk/section/keep-up-to-date/all-blogs>

For any other queries, email: cyberresilience@gov.scot