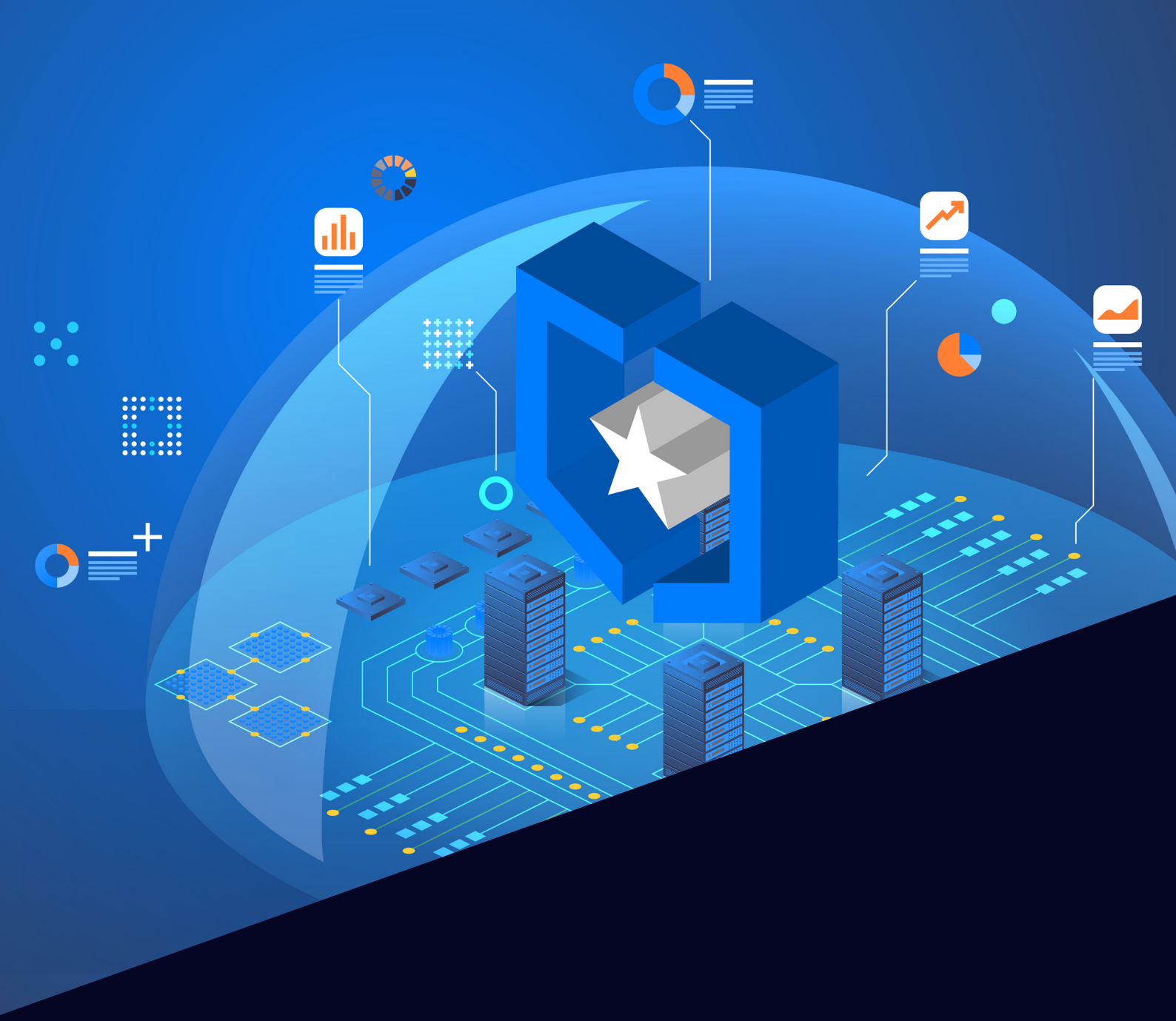


Cyber security advice:

Businesses and charities

IN PARTNERSHIP WITH

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Scottish Business Resilience Centre

What is Cyber security.

Cyber security is the means by which individuals and organisations reduce the risk of becoming victims of cyber-attack.

Cyber security's core function is to protect the devices we all use (smartphones, laptops, tablets and computers), and the services we access - both online and at work - from theft or damage. It's also about preventing unauthorised access to the vast amounts of personal information we store on these devices, and online.

From online banking and shopping, to email and social media, it's more important than ever to take steps that can prevent cyber criminals getting hold of our accounts, data, and devices.

Cyber crime takes many different forms. For example:

- Ransomware
- Account compromise
- Business Email Compromise
- Denial of Service Attack

Ransomware

Ransomware is a type of malicious software (malware) that prevents a user from accessing a computer or the data that is stored on it. The computer itself may become locked, or the data on it might be stolen, deleted or encrypted. Some ransomware will also try to spread to other machines on the network including any backup storage devices connected to the network.

Ransomware attacks are typically carried out using malware disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment. A popup message or note is left on the computer asking for a payment to be made in order to regain access to the data.

However, even if a payment is made, there is no guarantee that the computer or files will be decrypted.

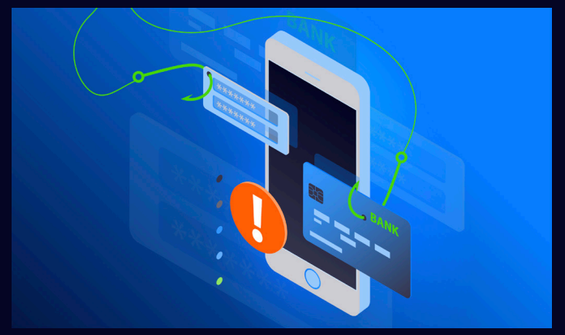
How to prevent Ransomware

The National Cyber Security Centre (NCSC) has published advice to assist individuals and businesses to mitigate malware and ransomware attacks.

Back-ups

Up-to-date backups are the most effective way of recovering from a ransomware attack, you should do the following.

- Make regular backups of your most important files - it will be different for every organisation - check that you know how to restore files from the backup, and regularly test that it is working as expected.
- Ensure you create offline backups that are kept separate, in a different location (ideally offsite), from your network and systems, or in a cloud service designed for this purpose, as ransomware actively targets backups to increase the likelihood of payment. NCSC blog on 'Offline backups in an online world' provides useful additional advice for organisations.
- Make multiple copies of files using different backup solutions and storage locations. You shouldn't rely on having two copies on a single removable drive, nor should you rely on multiple copies in a single cloud service.



- Make sure that the devices containing your backup (such as external hard drives and USB sticks) are not permanently connected to your network. Attackers will target connected backup devices and solutions to make recovery more difficult.
- You should ensure that your cloud service protects previous versions of the backup from being immediately deleted and allows you to restore to them. This will prevent both your live and backup data becoming inaccessible - cloud services often automatically synchronise immediately after your files have been replaced with encrypted copies.
- Ensure that backups are only connected to known clean devices before starting recovery.
- Scan backups for malware before you restore files. Ransomware may have infiltrated your network over a period of time, and replicated to backups before being discovered.
- Regularly patch products used for backup, so attackers cannot exploit any known vulnerabilities they might contain.

Protecting your data and devices

RANSOMWARE

The following steps will reduce the likelihood of your computer or device being infected with ransomware.

- Keep your operating system and software (apps) up to date. Don't put off applying updates, they contain patches that keep your device secure, including protection from ransomware and viruses.
- Make sure your antivirus product is turned on and up to date.
- Provide security education and awareness training to your staff.
- Avoid downloading unofficial apps. Only use official app stores (like Google Play or the Apple App Store), which provide protection from viruses.

The NCSC's Mobile Device Guidance provides advice on how to achieve this across a variety of platforms.

WHAT TO DO IF AFFECTED BY RANSOMWARE

The NCSC has produced guidance to help private and public sector organisations deal with the effects of malware (which includes ransomware). The guidance provides actions to help organisations prevent a malware infection, and also steps to take if you're already infected.

Following this guidance will reduce:

- the likelihood of becoming infected
- the spread of malware throughout your organisation
- the impact of the infection

MALWARE

If you've already been infected with malware, please refer to NCSC list of urgent steps to take:

- Smaller organisations should refer to the NCSC's Small Business Guide.
- Larger organisations / enterprises should refer to the NCSC's Mobile Device Guidance.
- For information about protecting your devices at home, please read NCSC guidance especially written for individuals and families.

The NCSC has jointly published an advisory: Technical Approaches to Uncovering and Remediating Malicious Activity, which provides more detailed information about remediation processes.

Files encrypted by most ransomware typically have no way of being decrypted by anyone other than the attacker. However, the No More Ransom Project provides a collection of decryption tools and other resources from the main anti-malware vendors, which may help.

SHOULD I PAY THE RANSOM?

Police Scotland and partners, including NCSC encourages individuals / organisations NOT TO PAY THE RANSOM. If you do pay the ransom:

- There is no guarantee that you will get access to your data or device.
- Your device will still be infected.
- You will be paying criminal group.
- You're more likely to be targeted in the future

We would advise anyone who thinks they may have been subject to a ransomware attack to contact Police Scotland via 101 (Non-emergency) or 999 (where there may be a threat to life or threat to national infrastructure). For further guidance please see the information at NCSC and No More Ransom.

ACCOUNT COMPROMISE

Whether it's your email, social media or some other type of online service, there are many things which can alert you to the fact that someone else is accessing your account.

Being locked out of the account is an obvious indication that something has gone wrong, but the signs can be more subtle. Things to look out for include logins or attempted logins from strange locations or at unusual times. Changes to your security settings and messages sent from your account that you don't recognise are also indications.

Once you realise your account has been hacked, NCSC have a step by step guide to help you regain control and protect yourself against future attacks.

BUSINESS EMAIL COMPROMISE

Business email compromise (BEC) is a form of phishing attack where a criminal attempts to trick a senior executive (or budget holder) into transferring funds, or revealing sensitive information. The criminals behind BEC send convincing-looking emails that might request unusual payments, or contain links to 'dodgy' websites. Some emails may contain viruses disguised as harmless attachments, which are activated when opened.

Unlike standard phishing emails that are sent out indiscriminately to millions of people, BEC attacks are crafted to appeal to specific individuals, and can be even harder to detect. BEC is a threat to all organisations of all sizes and across all sectors, including non-profit organisations and government.

What are the signs of BEC?

- Unsolicited email/phone call
- Pressure and a sense of urgency
- Direct contact from a senior official you are normally not in contact with
- Unusual request in contradiction with internal
- Request for absolute confidentiality
- Threats or unusual flattery/promises of reward

WHAT CAN I DO TO PREVENT THIS?

- Protect your account with a strong password. Remember, a strong password will consist of at least 3 random words, be longer than 12 characters and include numbers, symbols and capital letters. It will be unique to that account and not used for other accounts.
- Use 2-factor-authentication (2FA). This is sometimes called 2-factor verification and is an additional layer of security to prevent criminals accessing your account. Please see NCSC advice on setting up 2FA.
- Businesses should consider the way they manage payment requests received by e-mail to mitigate the risk of mandate fraud.
- Check your e-mail rules regularly to ensure you are the author of them.
- Check your account security history to ensure no unusual login activity is taking place.
- Check for compromised accounts at https://haveibeenpwned.com and remember to change any that have been compromised and register to receive notification of future data breaches involving your username(s).

DENIAL OF SERVICE ATTACKS

"Denial of service" or "DoS" describes the ultimate goal of a class of cyber-attacks designed to render a service inaccessible. The DoS attacks that most people have heard about are those launched against high profile websites, since these are frequently reported by the media. However, attacks on any type of system, including industrial control systems which support critical processes, can result in a denial of service.

When a website suffers a DoS attack, the apparent effect will depend on your perspective. For the average user, it appears that the site has simply stopped displaying content. For businesses, it could mean that the online systems they depend upon have ceased to respond. NCSC have guidance to help organisations understand and mitigate DoS attacks.

Reporting and useful sources

HOW DO I REPORT A CYBER CRIME?

You can report Cybercrime to Police Scotland by phoning 101 (non-emergency) or 999 (emergency).

USEFUL LINKS AND FURTHER INFORMATION

Cyber Scotland

Cyber Scotland is a single online resource for individuals and organisations across the public, private, and third sectors seeking information and support across a range of cyber security and resilience issues. Cyber Scotland is a collaborative partnership between Scottish Government, Police Scotland, NCSC, Scottish Business Resilience Centre, Highlands and Islands Enterprise, Scottish Enterprise, Scotland IS, Scottish Council for Voluntary Organisations, Young Scot, Skills Development Scotland, and Education Scotland.

National Cyber Security Centre (NCSC)

NCSC support the most critical organisations in the UK, the wider public sector, industry, SMEs as well as the general public. Please see below.

- NCSC Small Business Guide: NCSC guidance for small businesses provides cyber security advice for businesses, charities, clubs and schools with up to 250 employees. You're likely to fall into this category if you do not have a dedicated team internally to manage your cyber security.
- NCSC Business Guide: Cyber security advice for businesses, charities and critical national infrastructure with more than 250 employees.
- NCSC Public Sector Advice: Cyber security guidance for public sector organisations.

NCSC Infographics: The NCSC have produced infographics covering technical guidance for organisations and their staff to keep safe online. Please click on the following links to download them in pdf format.

OTHER USEFUL SOURCES

- Stay safe online: top tips for staff
- Protect devices from viruses and malware
- Phishing attacks: dealing with suspicious emails
- Using passwords to protect your devices and data
- Sextortion phishing scams: how to protect yourself
- A guide to recovering your hacked online accounts
- Video conferencing: using services securely
- Bring Your Own Device
- Homeworking: managing the cyber risks
- Business email compromise: dealing with targeted phishing emails

The full list of infographics is available at the NCSC website

- NCSC e-learning Training Package: The NCSC has produced a new e-learning training package: 'Stay Safe Online: Top Tips for Staff'. It's totally free, easy-to-use and takes less than 30 minutes to complete.
- NCSC Exercise in a Box: Exercise in a Box is an online tool from NCSC which helps organisations find out how resilient they are to cyber-attacks and practice their response in a safe environment.
- NCSC Cyber Action Plan Tool: National Cyber Security Centre (NCSC) have created the Cyber Action Plan tool to help micro businesses and sole traders securely navigate the increasingly digital landscape they operate in. To help increase their digital defence, micro businesses and sole traders are being invited to complete a short questionnaire that generates a personalised list of actions linked to the Cyber Aware behaviours.

ABOUT SBRC

The Sottish Business Resilience Centre (SBRC) is a respected voice in business resilience, bringing together the Scottish Government, Police Scotland, Scottish Fire & Rescue Service, and the Scottish business community.

The vision of SBRC is to become the catalyst that makes Scotland one of the safest and most resilient places to live, work, and do business, both on and offline.

It is the intention of SBRC that every Scottish organisation have the skills and knowledge to protect themselves against online attacks. We achieve this through the delivery of education and preventative training, as well as actively raising awareness of threats throughout the business community.

SBRC operates across three areas to offer a range of services and education, covering all aspects of business resilience and cyber security under the following areas:

- Community and Membership
- Prevent and Protect
- Skills and Education

INCIDENT RESPONSE HELPLINE

In partnership with Scottish Government and Police Scotland, SBRC have launched the UK's first cyber incident response helpline for the SME community and the third sector to help victims of cybercrime understand what support is immediately available to them and help them recover.

Businesses can reach the cyber incident helpline by calling **01786 437 472** weekdays 9am-5pm.The free helpline will help organisations confirm they have been the victim of an attack and, if so, provide expert guidance to get them back to secure operations.

SCOTTISH COUNCIL FOR VOLUNTARY ORGANISATIONS (SCVO)

The Scottish Council for Voluntary Organisations (SCVO) is the national membership organisation for the voluntary sector.

Cyber Essentials and people

What is Cyber Essentials?

Cyber Essentials (CE) is a simple but effective, Government backed scheme from the Nation Cyber Security Centre
(NCSC) that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber attacks.

Cyber attacks come in many shapes and sizes, but the vast majority are very basic in nature, carried out by relatively unskilled individuals. They're the digital equivalent of a thief trying your front door to see if it's unlocked. CE has been designed to prevent these attacks.

There are two levels of certification:

Cyber Essentials

The self-assessment option gives you protection against a wide variety of the most common cyber attacks. This is important because vulnerability to simple attacks can mark you out as target for more in-depth unwanted attention from cyber criminals and others.

Certification gives you peace of mind that your defences will protect against the vast majority of common cyber attacks simply because these attacks are looking for targets which do not have the Cyber Essentials technical controls in place.

Cyber Essentials shows you how to address those basics and prevent the most common attacks.

Cyber Essentials Plus

Cyber Essentials Plus still has the Cyber Essentials trademark simplicity of approach, and the protections you need to put in place are the same, but for Cyber Essentials Plus a hands-on technical verification is carried out.

NCSC's Cyber Essentials Partner the IASME consortium can help you to get certified.

There is also the Cyber Essentials readiness toolkit. Your responses to the questions in the toolkit helps create a personal action plan to help you move towards meeting the Cyber Essentials requirements.

The action plan includes links to specific guidance on how to meet the requirements.

Why should you get Cyber Essentials?

There's many benefits to becoming Cyber Essentials certified, here are just a few:

- Reassure customers that you are working to secure your IT against cyber attack
- Attract new business with the promise you have cyber security measures in place
- You have a clear picture of your organisation's cyber security level
- Some Government contracts require Cyber Essentials certification

Government contracts

If you would like to bid for government contracts which involve handling sensitive and personal information or the provision of certain technical products and services, you will require Cyber Essentials Certification.

Trusted partners

The Scottish Business Resilience Centre (SBRC) has worked with Cyber Essentials Certifying Bodies based and operating in Scotland to support organisations, both small and large, to focus on cyber hygiene and achieve Cyber Essentials or Cyber Essentials Plus.

This 'Trusted Partners' initiative, endorsed by Police Scotland, has developed into a network of independent companies focused on promoting continuous improvement in cyber resilience across all sectors in Scotland and supports the Scottish Government's Safe, Secure and Prosperous: A Cyber Resilience Strategy for Scotland.

Certifying Bodies are professional companies that have been licensed to deliver Cyber Essentials assessments and offer consultancy services to help organisations achieve the certification. On 1st April 2020, the IASME Consortium Ltd were selected by the National Cyber Security Centre to oversee Cyber Essentials within the UK and Certifying Bodies will now work in partnership with IASME to deliver the scheme.

Find out more about the Trusted Partners on the SBRC website.

TRUSTED PARTNER

Scottish Business Resilience Centre

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

CREATING A SECURE SCOTLAND FOR BUSINESS

Staff

Prevention is key and by ensuring your staff understand the potential dangers of cyber attack you can all help mitigate against this.

Make sure your staff know your company protocols and procedures and have good cyber hygiene - personal devices should not be plugged into work devices unnecessarily and all passwords should be unique - think three-random-words - and comply with your organisation's security policy.

It is often complacency or human error that allows hackers their opportunity so make sure your staff all know their responsibilities.

Scottish Business Resilience Centre

Oracle Campus
Blackness Road
Linlithgow
West Lothian
EH49 7LR

01786 447 441
enquiries@sbrcentre.co.uk
www.sbrcentre.co.uk
@SBRC_Scotland

IN PARTNERSHIP WITH

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

A Company Limited by guarantee and registered in Scotland
No. SC170241 | VAT Registration Number: 717 2746 27