National Cyber Security Centre
a part of GCHQ

Cyber security:
Practical Tips for Protecting Your Organisation Online

Organisational Cyber Security

Every organisation needs to look after its data as well as manage the risks of using online services, and so **everyone needs to follow some basic principles of good cyber security as outlined in the cards.**

Organisation owners and employees need to be aware that cyber security is a management and assurance issue. After all, poor cyber hygiene could affect an organisations ability to function, its reputation and legal obligations to keep personal data safe.

*Cyber security is about protecting the **devices** we all use and the service we access online – both at home and work – from theft and damage.*

*It's also about preventing unauthorised access to the vast amounts of **personal information** we store on these devices and online.*

Why Cyber Security Matters

An increasing number of organisations are being seriously impacted by cyber incidents: perhaps a phishing attempt to steal money and passwords, or a ransomware attack that encrypts files preventing access. But why?

- **Many cyber incidents are untargeted.**
  They can affect any organisation that doesn't have basic levels of protection.

- **Organisations hold plenty of sensitive information.**
  For example, organisation records, customer payment information, personal details, and passwords. All this must be kept safe and confidential.

- **Cyber criminals want to make money.**
  They understand that an organisation's information is often sufficiently important to that organisation and that they might be prepared to pay a ransom to get it back.

Who is behind cyber attacks?

Online criminals

Are really good at identifying what can be monetised, for example stealing and selling sensitive data, or holding systems and information to ransom.

Hackers

Individuals with varying degrees of expertise, often acting in an untargeted way – perhaps to test their own skills or cause disruption for the sake of it.

Malicious insiders

Use their access to an organisation's data or networks to conduct malicious activity, such as stealing sensitive information to share with competitors.

Honest Mistakes

Sometimes staff, with the best intentions just make a mistake, for example by emailing something sensitive to the wrong email address.

What are the top threats to organisations?

Ransomware
Malicious software that makes data or systems unusable until the victim makes a payment.

Phishing
Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit fake website.

Virus
Programs which can self-replicate and are designed to infect legitimate software programs or systems.
A form of malware.

Insider Risks
The potential for damage to be done maliciously or inadvertently by a legitimate user with privileged access to systems, networks or data.

Be Cyber Aware

- **Create separate password for your organisation-critical accounts.**
  Your accounts include sensitive information about your customers, your organisation and financial information. If your accounts are not secure, your organisation could be at risk of a cyber incident.

- **Create strong passwords using three random words.**
  Weak passwords can be hacked in seconds. The longer and moreunusual your password is, the stronger it becomes and the harder it is to hack.

- **Save your passwords in your browser.**It is good practice to use different passwords for the accounts you care most about. Of course, remembering lots of passwords can be difficult, but if you save them in your browser then you don't have to.

Cyber Aware

cyberaware.gov.uk

Cyber Aware is the government's advice on how to stay secure online.

- **Turn on 2-step verification (2SV) for your email**
  2-step verification (2SV) gives you twice the protection so even if cyber criminals have your password, they can't access your email.
  2SV works by asking for more information to prove your identity. For example, getting a code sent to your phone when you sign in using a new device or change settings such as your password.
  You **won't** be asked for this every time you check your email.

- **Keep your organisation device up to date**
  Make sure all your devices have the latest software updates to reduce the risk of a cyber incidents. This will ensure that all your devices include the latest security.

- **Back up important organisation data and key contacts**
  By backing up your data, your organisation can continue operating even if you suffer a cyber incident. Backups can include paper copies, removable media or backed up to the cloud.

https://cyberaware.gov.uk/

Preparing for a cyber incident

While implementing good security controls is important, there is no such thing as perfect security.

All organisations are at risk of a potential cyber incident, so it is vital you prepare your response and plan your recovery in the event of a cyber incident.

What can you do to prepare for an incident?

- **Identify critical electronic information**
  Such as contact details, emails calendars, and essential documents. Also identify the key systems and resources to keep your organisation running.

- **Make a regular back up of essential information**
  Regularly test that the backup is working to ensure you can restore information from it.

- **Make a list of the key partners that you use to run your organisation**
  This will aid your response in the event of an incident and will enable you to keep your organisation active offline or in the event of unavailable systems.
  e.g. supplier contact numbers, IT support number.

- **Make an incident plan** and keep it safe so you can use it if your equipment is stolen or damaged by a cyber incident.

See our full guide for more information on how to prepare and plan.

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

Reporting an incident

What is an incident?
A cyber incident is an unauthorised access (or attempted access) to an organisation's IT systems. These may be malicious attacks (such ransomware or phishing attacks), or could be accidental incidents (such as damage from fire/flood/theft).

Reporting
If your organisation suffers a cyber incident or is affected by fraud (e.g. money lost a result of a phishing email or your IT systems are compromised), report it to **Action Fraud** by calling 0300 123 2040 or go to **www.actionfraud.police.uk** or in Scotland through Police Scotland's 101 call centre.

If you have received an email which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS): **report@phishing.gov.uk**

Moving your organisation from the physical to the digital.

If you are moving or currently running your organisation online this will present new risks, by placing more reliance on digital technologies such as web hosting, credit card processing, and productivity tools like email, video and chat. Having good relationship with your IT service provider(s) will help massively with this.

If you are talking directly with your supplier or you are in charge of your own IT, the following points will help you ensure that security is at the forefront of any new service you decide to use.

- **Patching & Updates**
  Ask your providers how often they patch the services you use, and check any contracts or SLAs to ensure that patching is included.

- **Backups**
  What sort of backup arrangements are in place and how often are these tested? You should know how often your data is backed up, where it is stored, and who has access to it.

- **Access:**
  Is your data (and the data of others which you have responsibility for) being properly protected? Are you able to put 2FA in place to limit access to your data and services?

- **Logs**
  Are logs being kept for security purposes? Logging can play a vital role in diagnosing any problems. Logs will also prove invaluable when responding to and recovering from security incidents.

- **Response** What will happen if things go wrong? Service providers should operate on the presumption that they will be attacked. It should be clear how and when they will engage with you during a security incident.

Find out more:

https://www.ncsc.gov.uk/guidance/moving-business-from-physical-to-digital

You will find all this advice and guidance and more on our website:

- **Small Business Guide**
  How to improve your cyber security; affordable, actionable advice for organisations.
  https://www.ncsc.gov.uk/smallbusiness

- **Small Charities Guide**
  How to improve cyber security within your charity - quickly, easily and at low cost.
  https://www.ncsc.gov.uk/collection/charity

- **Response & Recovery Guide**
  Guidance that helps small to medium sized organisations prepare their response to and plan their recovery from a cyber incident.
  https://www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery

- **Top Tips for Staff**
  The NCSC's e-learning package 'Top Tips for Staff' can be completed online, or built into your own training platform. It has been deliberately designed for a non-technical audience with tips that complement any existing policies and procedures
  https://www.ncsc.gov.uk/training/top-tips-for-staff-scorm-v2/scormcontent/index.html#/

- **Exercise in a Box**
  A free online tool which helps organisations find out how resilient they are to cyber-attacks and practise their response in a safe environment
  https://www.ncsc.gov.uk/information/exercise-in-a-box

- **Cyber Essentials**
  Cyber Essentials government backed certification scheme helps you to guard against the most common cyber threats and demonstrate your commitment to cyber security.
  https://www.ncsc.gov.uk/cyberessentials/overview

- **Home working**
  How to make sure your organisation is prepared for an increase in home working, and advice on spotting coronavirus (COVID-19) scam emails
  https://www.ncsc.gov.uk/guidance/home-working

- **Ten Steps to Cyber Security**
  Take things a little further: breaks down the task of defending networks into ten essential components.
  10 steps to cyber security - NCSC.GOV.UK

- **Video Conferencing**
  Guidance to help you to choose, configure and deploy video conferencing services such as Zoom and Skype within your organisation
  https://www.ncsc.gov.uk/guidance/video-conferencing-services-security-guidance-organisations

- **Moving your organisation from physical to digital**
  Security questions to ask your IT service providers when running your organisation online
  https://www.ncsc.gov.uk/guidance/moving-business-from-physical-to-digital

- **Cyber Security for Small Organisations**
  The NCSC's e-learning package 'Cyber Security for Small Organisations' can be completed online, or built into your own training platform. The e-learning will take you through all the actions needed to take to reduce the likelihood of becoming a victim of the most common cyber attacks
  https://www.ncsc.gov.uk/training/cyber-security-for-small-organisations-scorm-v2/scormcontent/index.html#/

Small Organisations Newsletter

If you would like to receive regular advice and updates from us you can sign up to our monthly newsletter created specifically for small organisations who are looking for up to date information and advice on cyber security.

You can subscribe at:
https://ncsc-production.microsoftcrmportals.com/subscribe/