nwcrc.co.uk

Cyber Security Guide

For Small Businesses.

THE
CYBER
RESILIENCE
CENTRE
FOR THE NORTH WEST

Affordable, professional cyber security services for your business.

What is Cyber Security?

THE CYBER RESILIENCE CENTRE FOR THE NORTH WEST

Cyber security is how individuals and organisations reduce the risk of becoming victims of a cyber-attack or online crime.

Cyber security is designed 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 also prevents 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 is more important than ever to take steps to prevent cybercriminals from getting unauthorised access to our accounts, data, and devices.

Cybercrime takes many different forms. For example:

- **Ransomware**
- **Account compromise**
- **Business Email Compromise**

In this guide, we will provide straightforward advice on how to spot the signs of an attack, how you can protect your business and links to further free resources & support.

National Cyber Security Centre (NCSC)

The NCSC supports critical national infrastructure, the public sector, private industry, SMEs, and the general public. We will signpost to free NCSC materials in this guide where possible as a trusted source of support.

Ransomware

THE CYBER RESILIENCE CENTRE FOR THE NORTH WEST

Ransomware is a type of malicious software (malware) that prevents a user from accessing a computer or its stored data.

The computer itself may become locked, or its data might be stolen, deleted or encrypted. Some ransomware will also try to spread to other machines, 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 payment 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 avoid Ransomware

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

- Keep your operating system and apps up to date. Please don't put off applying updates; they contain patches that keep your device secure.
- Make sure your antivirus 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 protect from viruses.
- The NCSC's Mobile Device Guidance advises how you can achieve this across various platforms.

Ransomware

THE CYBER RESILIENCE CENTRE FOR THE NORTH WEST

If you've already been infected, please refer to the below guidance on mitigating malware:

- Large 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.
- Files encrypted by most ransomware typically cannot be decrypted by anyone other than the attacker.
- The No More Ransom Project, run in partnership with Europol, provides free decryption tools and other resources that may help.

SHOULD I PAY THE RANSOM?

Police and partners, including the NCSC, encourage 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 a criminal group.
- You're more likely to be targeted in the future.

EUROPOL

NO MORE RANSOM

Account Compromise

THE CYBER RESILIENCE CENTRE FOR THE NORTH WEST

Whether it's your email, social media or some other online service, many things can alert you that someone else is accessing your account.

Being locked out of the account indicates something has gone wrong, but the signs can be more subtle. Things to look for include logins or attempted logins from unknown locations or 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, the NCSC have a step-by-step guide to help you regain control and protect yourself against future attacks.

How to avoid account compromise.

- Use a strong and separate password for each of your online accounts
- Follow NCSC guidance by using three random words
- Use a password manager
- Save passwords to your internet browser.
- Turn on 2-factor authentication (2FA).

Business Email Compromise

THE CYBER RESILIENCE CENTRE FOR THE NORTH WEST

Business email compromise (BEC) is a 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, activated when opened.

Unlike standard phishing emails, which 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 threatens all organisations of all sizes and sectors, including non-profit organisations and charities.

What are the signs of business email compromise?

- Unsolicited email/phone call
- Pressure and a sense of urgency
- Unusual contact from a senior official
- Unusual request that contradicts internal processes
- Request for absolute confidentiality

What can I do to reduce the risk?

- You can protect your account with a strong password.
- Use 2-factor authentication (2FA).
- Review how you manage payment requests received by email to mitigate the risk of fraud.
- Check your email rules regularly
- Check for compromised accounts at haveibeenpwned.com

Back-ups

THE CYBER RESILIENCE CENTRE FOR THE NORTH WEST

Up-to-date backups are the most effective way to recover from a ransomware attack; please 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 works as expected.*

- Please ensure you create offline backups 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 payment likelihood.
- NCSC blog on 'Offline backups in an online world' provides additional practical advice for organisations.

- Make multiple copies of files using different backup solutions and storage locations.

- Please ensure your backup devices (such as external hard drives and USB sticks) are not permanently connected to your network.

- Please ensure your cloud service protects previous backup versions from being immediately deleted and allows you to restore them.

- You can scan backups for malware before you restore files. Ransomware may have infiltrated your network over time and replicated to backups before being discovered.

Reporting & Useful Resources

THE CYBER RESILIENCE CENTRE FOR THE NORTH WEST

How do I report a cybercrime?

If you are currently suffering a live cyber-attack, please immediately call Action Fraud on 0300 123 2040. This service is available 24 hours a day, seven days a week.

If not, you can also call the Police at any time on 101.

In an emergency, where there is a threat to life or a crime in progress, always phone 999.

Further resources (click the links below) :

- Sign up for the Free NWCRC Newsletter
- Cyber Incident Response Pack Template
- Cyber Security Checklists
- Cyber Security - Sector-based guidance
- Frequently Asked Questions about Remote Working

- Phishing attacks: dealing with suspicious emails
- A guide to recovering your hacked online accounts
- Business email compromise: dealing with targeted phishing emails

About Us

THE CYBER RESILIENCE CENTRE FOR THE NORTH WEST

The North West Cyber Resilience Centre is a police-led partnership which brings together the police, local government, academia and the business community.

As the trusted voice in cyber resilience, our vision is for every business to have access to the knowledge, skills and tools to help protect themselves from online crime

We achieve this by providing education, testing and training services delivered by our team of trusted professionals, seconded police officers and security consultants.

We have developed a number of membership packages specifically designed to help small businesses become more resilient to online crime.

We also provide a small range of affordable professional cyber security services to test your vulnerability to an attack and your ability to recover.

The NWCRC was established in 2019 as the first centre in the country and a pathfinder to the National Police Chief's Council and the Home Office.

We are proud to be a part of a national network of Cyber Resilience Centres supporting the Police in keeping our business communities safe.

Sign up for free membership

nwcrc.co.uk

Contact us

www.nwcrc.co.uk
info@nwcrc.co.uk
0161 706 0940

Address:
Manchester Technology Centre
Oxford Road
Manchester
M1 7ED

The North West Cyber Resilience Centre and north west police forces would like to thank the Scottish Business Resilience Centre for their assistance in the publication of this guide.

IN PARTNERSHIP WITH

nwcrc.co.uk