Back to the Office

Cyber Security Guidance

THE CYBER RESILIENCE CENTRE FOR THE NORTH WEST

CONTENTS

1. Introduction
2. Passwords
3. Cloud Security
4. Software Updates
5. Working from Home Policy
6. Security Awareness Training
7. Office Checklist
8. More Resources

BACK TO THE OFFICE

Cyber Security Guidance

If your staff are heading back to the office in the coming days and week; you should remember to reinforce the cyber security basics.

After a prolonged period of being out from the office (holidays, Christmas, Easter, etc), it's important that we all ensure that our networks and devices are all secure.

Revisit Old Passwords

We all have old passwords and accounts that need updating. Don't forget to revisit any old passwords and attempt to change those which are most at-risk.

Review any passwords that are short, easily guessed or using a word or number unique to us. *Such as;* Date of Birth, Pet name, Maiden Name, Address etc.

You should also consider syncing any new passwords across your devices so that your credentials aren't out of sync and you lose access to any accounts.

How do I find old passwords?

Most browsers (Chrome, Safari, etc) will do the work for you. Go to your browser's settings and review all of your passwords. Some browsers such as Safari do the password review for you and flag a warning next to a weak or repeated password.

Safari > Preferences > Passwords
Chrome >Settings > Passwords

Cloud Security

When working remotely or in the office, there are few things more important than sharing work documents with colleagues.

Online file storage, syncing and sharing services like Google Drive, One Drive, and Dropbox play a huge role in allowing us to share things quickly and securely.

Cloud services mean we've all become more comfortable in using them for hosting servers on the cloud. This is similar to when you rent a car and you're responsible for looking after the rental vehicle.

Whilst these services provide access to all your important data — Word docs, PDFs, spreadsheets, photos, and any other digital assets — from wherever you are. **You need to keep reviewing your security settings and adjust these based on your staff/company's needs.**

Software Updates

Out-of-date software, apps, and operating systems contain weaknesses. This makes it easier to hack, especially if your employees aren't keeping them updated or if you have devices that have been sat unused in your office for a prolonged period.

It's important you make time to install any critical security updates to your OS and any other software. These updates may take several hours, so factor this into your return to work planning or even consider going in a few days early to make sure all devices are up to date. **Employees mustn't try to bypass any security updates when they get back behind in the office.**

Going forward make sure you turn on automatic updates for your devices and software that offer them. This means you do not have to remember to install updates each time.

Don't worry - most devices will send reminders on your phone or computer.

Working from Home Policy

Staff who were previously used to sharing an office are now much more comfortable working remotely.

Have you thought about making sure your teams can continue to collaborate securely?

Your organisation needs to be prepared now we're all transitioning into hybrid working patterns. Having all or large numbers of staff working from home is here to stay and the need to have a policy in place is vital.

Our business memberships come with cyber security policy and procedures templates (including a 'Working from Home Policy').

These policies have been designed by our Cyber Security Consultants to help you put the right measures in place. Your business should have a clear security strategy and can respond efficiently if a cyber incident should occur.

Security Awareness Training

The most effective way to secure yourself in the digital world is to educate yourself and your staff. **80% of breaches could be prevented by raising awareness amongst staff.**

Cyber defence needs education and routine checks similar to any other aspects of the business such as finances.

This doesn't have to be in-depth technical knowledge of how a cyber attack works. A simple overview of attack trends and general awareness will give you defensive measures - remember lack of knowledge is the attacker's advantage.

For example, if you learn how Phishing works and what are the objectives of a Phishing attack then you automatically have an extra defensive measure built-in within your organisation.

Try to roll out this education regime throughout your entire company.

Security Awareness Training

Train with the Cyber Resilience Centre today.

Our training is focused on those with little or no cybersecurity or technical knowledge and is delivered in small, succinct modules using real-world examples.

Security Awareness training is tailored to each company to provide the right level of skills and context for your business.

Our trainers are highly knowledgeable, personable and friendly and pride themselves on providing the right environment for your people to feel comfortable and to ask questions.

Request a quote or learn more today.
Email: info@nwcrc.co.uk

OFFICE CHECKLIST

- [ ] Create a backup of your data in the cloud
- [ ] Keep a separate offline backup updated
- [ ] Setup/Review your Cyber Incident Response Plan
- [ ] Enable two-factor authentication on your accounts
- [ ] Review privacy settings on your social accounts
- [ ] Review which devices your accounts are signed-in
- [ ] Keep your OS, apps and browsers updated
- [ ] Enable your anti-virus and firewall, check for updates and install
- [ ] Do you staff need to create a Bring Your Own Device (BYOD) Policy?
- [ ] Disable or remove any unused browser extensions
- [ ] Review your passwords & password manager
- [ ] Use a VPN on public wi-fi networks

More Resources

1. Small Business Guide to Cyber Security
2. Cyber Incident Response Plan
3. FAQ about Cyber Security
    a. FAQ about Cyber Essentials
    b. FAQ about Remote Working
4. How to secure your social media accounts

Sector Specific Guidance

Accountants

Charities

Construction

Education

Retail & eCommerce

THE
CYBER RESILIENCE CENTRE
FOR THE **NORTH WEST**