THE
CYBER
RESILIENCE
CENTRE
FOR GREATER MANCHESTER

2021 Security Checklist

info@cyberresiliencecentre.com

cyberresiliencecentre.com

THE CYBER RESILIENCE CENTRE FOR GREATER MANCHESTER

Security Checklist

1 - Revisit Old Passwords
2 - Enable Two-Factor Authentication
3 - Cyber Awareness Training
4 - Privacy Settings
5 - Working From Home

info@cyberresiliencecentre.com
cyberresiliencecentre.com

Revisit Old Passwords

Even those educated in cybersecurity still have old passwords and accounts that need updating. This means that we should all revisit our passwords and attempt to change those which are most at-risk.

These are the 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.

Although this can be time-consuming and needs preparation, it will give you improved peace of mind.

How do I find old passwords?

If you are using a password manager in your internet browser (Chrome, Safari, etc) then this most of the work is done 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. Make sure you review them all and change those at risk.

- **Safari** > Preferences > Passwords
- **Chrome** >Settings > Passwords

Factsheet:

For more advice on passphrases download our factsheet.

Two-Factor Authentication

Two-factor authentication (often shortened to 2FA) provides a way of 'double-checking' that you really are the person you are claiming to be when you're using online services, such as banking, email or social media. This could be a code that's sent to you by text message, or that's created by an app.

Why should I use 2FA?

Passwords can be stolen by cybercriminals, potentially giving them access to your online accounts. However, accounts that have been set up to use 2FA will require an extra check, so even if a criminal knows your password, they won't be able to access your accounts.

How do I set up 2FA?

Some online services will already have 2FA switched on. However, most don't, so you will need to switch it on yourself to give extra protection to your other online accounts, such as email, social media and cloud storage. If available, the option to switch on 2FA is usually found in the security settings of your account (where it may also be called 'two-step verification').

For more advice on two-factor authentication read this NCSC guide.

THE CYBER RESILIENCE CENTRE FOR GREATER MANCHESTER

Cyber Awareness Training

The most effective way to secure yourself in the digital world is to educate yourself and your staff.

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.

Train with the Cyber Resilience Centre

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

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

info@cyberresiliencecentre.com

cyberresiliencecentre.com

Privacy Settings

This is very important to avoid exposing unnecessary information about you or your company. Revisit your devices and social media account privacy settings and make sure these settings are in line with your company's security & device policies.

Privacy advice for Devices:

if you've just bought a new device, or haven't looked at your security settings for a while, you should take some time to make sure you're protected against the latest threats. Fortunately, most manufacturers provide easy-to-use guidance on how to secure your devices.

- Apple
- Google (Android)
- Samsung
- Microsoft

Privacy advice for Social Media:

- Facebook: basic privacy settings and tools
- Twitter: how to protect and unprotect your Tweets
- YouTube: privacy and safety
- Instagram: privacy settings and information
- LinkedIn: account and privacy settings overview

Working from home

Working from home can be daunting for people who haven't done it before, especially if it's a sudden decision. There are also practical considerations; staff who are used to sharing an office space will now be remote. Think about whether you need new services, or to just extend existing ones, so that teams can continue to collaborate.

For example, you may want to consider services that provide chat rooms, video teleconferencing (VTC) and document sharing.

This NCSC guidance has been created to help you make sure you're organisation is prepared now we're all back to home working in this third lockdown period.

This NCSC guidance also helps you;

- To spot the increased numbers of coronavirus (COVID-19) scam emails
- Setting up new accounts and accesses
- Preparing your staff for home working
- Controlling access to corporate systems
- Helping staff to look after devices
- Removable media
- Using personal rather than work devices