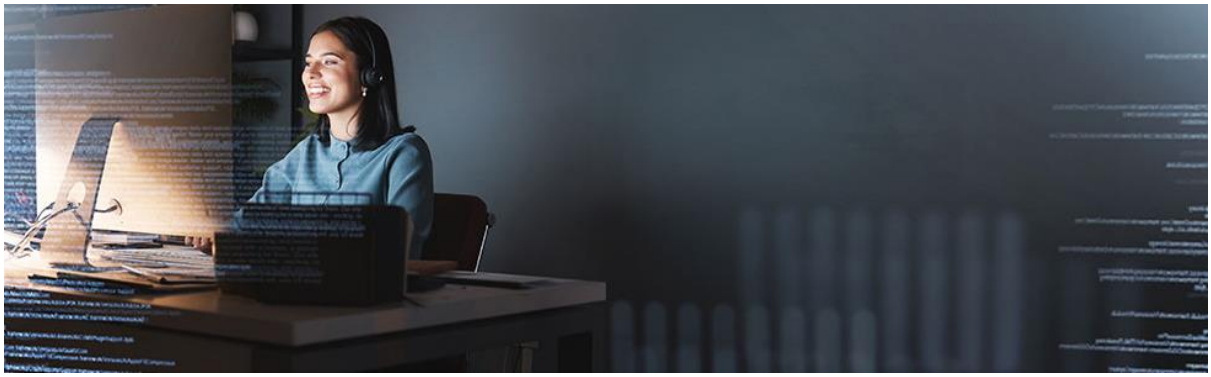
Cyber Security Checklist



With the risk of cybercrime rising, prevention is the most effective way to protect your business and your clients.

While every business's needs are different, there are some simple measures you can take to help keep you and your business safe.

1. Set secure passphrases
Passphrases are much harder to crack but easier to remember. Don't use the same passphrase more than once because if that passphrase is compromised, cyber criminals could gain access to your other accounts with the same passphrase.

2. Back up your files regularly
This means you can restore your files if they are stolen, or something goes wrong. It's important to do this regularly to ensure you have your most up-to-date files, photos, documents, or videos backed up. You can set up automatic backups, so this won't have to take up too much of your time.

3. Train your team on the common scams
By understanding what to look for, you know what to avoid. Familiarise yourself with common scams, such as dating scams or phishing emails and emails with messages and report it to ReportCyber before the damage is done.

4. Think before you click
Take a moment to think before opening any attachments or links in an email – especially one you weren't expecting. If you're still unsure, reach out to the person or company who sent it to check whether it's legitimate. Once you've recognised something as a scam, don't reply, click on any links, or open any attachments. Report the scam to ReportCyber and follow the advice.

5. Update your devices

These are one of the simplest yet strongest defences. Newer versions of the software are less vulnerable to attacks as they address security concerns or gaps. It's a good idea to turn on automatic updates, so you don't need to worry about remembering when a new update is released.

6. Turn on multi-factor authentication (MFA)

These extra checks prove your identity when you sign in or use an account. It could be a text, email, fingerprint or a series of questions. To learn more about MFA and how to turn it on for different accounts, visit here.

7. Develop a Cyber Incident Response plan for your business

Businesses often think about it too late, but a documented plan can help ensure an effective response and recovery. This plan should align with your organisation's emergency, crisis, and business continuity plans. Developing the plan is also a chance to assess the security of your business and fill gaps. To learn how to create yours, visit here.

8. Assess the security of your website

The majority of small businesses have a website nowadays, and these are becoming a target for cyber criminals. Making sure to use HTTPS and secure your e-commerce sites are just some examples.

9. Consider a password manager

Remembering passwords for every account can be difficult for most of us, which is why password managers have become popular. These help manage passwords for all of your accounts, and you'll only need to remember one master password. Learn more about this technology here.