# Cyber Aware

Whether you work for yourself or you run a small business with fewer than 10 employees, the following advice will help keep you secure online.

National Cyber Security Centre
a part of GCHQ

Cyber Aware

# Six Actions to Help Keep Your Business Secure Online

**We're all doing more online than ever. But we're not the only ones. So are cyber criminals. If you work for yourself or run a small business with fewer than 10 employees, follow these six practical steps to better protect your business online.**

## Improve your password security

Passwords are the gateway to your accounts. Here are three actions to make your passwords work harder to protect your business.

### 1 Create a separate password for your business email account

Your inbox contains lots of sensitive information about your customers, your business and your finances. So, if a hacker gets into your inbox, not only will they have access to this information, they could get access to every account linked to your email. Create a strong email password and make sure it's different to your others.

### 2 Create strong passwords using three random words

Hackers can easily guess weak, short passwords. Use three random words that are memorable to you, but are difficult to guess e.g. RedLeopardOcean, to make a strong password.
Hackers will try many different versions of words (Liverpool, L1verpool1, liverp00l!), so use three random words even when you need to add numbers or special characters e.g. RedLeop@rd0cean1.

### 3 Save passwords in your browser

Remembering passwords can be challenging because different websites and apps have different rules. And it's important to have separate passwords for business critical accounts like email.
Your internet browser will often give you the option to remember your passwords for you. It's safe and it will free you up to create strong, unique passwords without having to remember them all.

## Add extra protection

Now you've got your passwords sorted,
you're ready to take your cyber security to the next level.

### 4 Turn on two-factor authentication (2FA)

2FA is free. And it will stop hackers getting into your account even if they have your password. 2FA (also known as 2-step verification, or multi-factor authentication) simply means you'll be prompted for a second piece of information when signing into your accounts – usually a code which will be sent via text or email.

### 5 Update your devices

Tech companies are continually working to fix vulnerabilities in their software. So, when you receive prompts to update your devices don't ignore them. They contain important fixes which will help keep hackers out. You can make things even simpler by turning on automatic updates.

# Make sure you can recover quickly

Congratulations! If you've followed the actions above, you've protected your business from the vast majority of cyber attacks. But, if something does go wrong, backing up means you will always have access to your most recently saved data, enabling you to get your business up and running with the least amount of disruption.

## 6 Back up

Backing up regularly means you always have a copy of your important business data in the event it's lost or stolen (e.g. contract information, customers personal details, key contacts). Make sure that these backups are recent and can be restored. You can either back up to an external drive or to the cloud. If backing up online, you can turn on automatic backups and your devices will do the hard work for you.

For more information on how to keep you and your business secure online visit **cyberaware.gov.uk**

National Cyber Security Centre
a part of GCHQ

Cyber Aware