

Five Point Cyber Security Checklist for Employees

The 8x8 Business Owners' Toolkit: a series of handy tips for busy people.

Five Point Cyber Security Checklist for Employees

You've heard about cyber security and threats from hackers and probably invested in anti-virus software, firewalls, and data encryption. But did you know that the biggest security risk to your businesses comes from your employees? According to [Kaspersky](#), 52% of businesses believe they are at risk from within – that staff, whether intentionally or lack of knowledge, are putting their employer at risk.

We appreciate staff training, and even keeping up with best practice yourself, can be time consuming – so we've created an 'Employee Cyber Security Checklist,' based on advice from the [National Cyber Security Centre](#). Share it with your team to help them minimise business security risks.

Keep your users safe from cyber threats with our handy checklist.

1

Back up your data in the cloud

- This will prevent the company from being blackmailed through ransomware attacks.
- It will also ensure you can continue to work if there is physical damage or theft to your device.

2

Avoid malware

- Accept and install all updates and security patches for your operating system.
- Only download apps from approved stores, such as Google Play and Apple Store.
- Avoid using third party memory sticks where possible or check with your IT Team before you plug into your device.

3

Protect your devices

- Keep all devices used for work password or PIN protected.
 - Use software (such as Google's '[Find my device](#)' to track your device and, if necessary, wipe the data from it.
 - Where possible, avoid public Wi-Fi – such as in hotels and cafés.
-

4

Use strong passwords

- Never use common or predictable **passwords**.
- Use a password manager such as **Keeper** to create and store passwords – so you only need to remember one.
- **Two factor log-in** allows you to increase security by requesting an extra action, such as verifying your ID by text. Use it for important accounts.

5

Watch out for signs of phishing attacks

- Does the message address you by name? Is the sender's address legitimate?
- Does the artwork look high quality? Are there spelling or grammar errors?
- Watch out for veiled threats and requests for action like 'update payment details.'

What next?

Security is just one of the many things business owners need to tightly manage to mitigate business risk.

If you'd like to get more bite-sized knowledge for your toolkit.

- Like and follow our 8x8 social media pages so you don't miss out on the next handy instalment of advice and tips.
- Follow us on **Facebook** and **LinkedIn**.



If you're interested in helping your workforce work from anywhere, **Speak to an 8x8 expert.**

8x8

8x8, Inc. (NYSE: EGHT) is transforming the future of business communications as a leading Software-as-a-Service provider of voice, video, chat, contact center and enterprise-class API solutions powered by one global cloud communications platform. 8x8 empowers workforces worldwide to connect individuals and teams so they can collaborate faster and work smarter. Real-time analytics and intelligence provide businesses unique insights across all interactions and channels so they can delight end-customers and accelerate their business. For additional information, visit www.8x8.com, or follow 8x8 on LinkedIn, Twitter and Facebook.

© 8x8, Inc. All Rights Reserved. Unless otherwise specified, all trademarks identified by the ®, TM, or SM are registered trademarks, trademarks, or services marks respectively of 8x8, Inc.

