

Account Security Checklist

Purpose: A one-page checklist to lock down the email and login accounts your business relies on, so no single lost password or departed colleague can cost you your accounts.

Part 1: For every email account

- ☐ I created this account myself (it was not bought or handed down from an unknown source).
- ☐ The password is unique and made of three or more random words, or generated by a password manager.
- ☐ The password is not based on a pet, family name, sports team, significant date or anything on my social media.
- ☐ 2-step verification is switched on (authenticator app or security key preferred over text message where offered).
- ☐ Backup codes are saved somewhere safe, offline or in the password manager.
- ☐ The recovery phone number is one I control.
- ☐ The recovery email address is one I control.
- ☐ I have checked the list of signed-in devices and removed any I do not recognise.
- ☐ I have checked connected apps and removed any I no longer use.
- ☐ Automatic forwarding rules are checked (attackers sometimes add one to copy your mail).

Part 2: For the business as a whole

- ☐ We keep an account register: which email belongs to which tool, who owns it, who has backup access.
- ☐ Business tools use a business email (ideally on our own domain), not a personal address.
- ☐ Staff get access through each platform's own roles or delegation, not by sharing a password.
- ☐ Shared passwords are kept in a business password manager with named users.
- ☐ A leaver checklist exists: remove access, change shared passwords, transfer ownership, check forwarding.
- ☐ At least two trusted people can recover each key account (owner plus a backup).
- ☐ We review this register every 3 months. Next review date: _____

Part 3: Account register (copy into a spreadsheet)

Columns: Tool or account | Login email | Owner (name) | Backup person | 2-step verification on? (Y/N) | Recovery phone/email checked (date) | Last password change | Notes

Part 4: If you think an account has been compromised

1. Sign in from a trusted device and change the password straight away.
2. Turn on 2-step verification if it is not already on.
3. Sign out of all other devices.
4. Check recovery details and forwarding rules have not been changed.
5. Change the password on any other account that used the same or a similar password.
6. Check sent mail and security alerts for activity you did not do.
7. Warn contacts if the account sent anything suspicious.
8. If money or personal data may be involved, report it: in the UK, Action Fraud (fraud) and, for personal data, the ICO.

Part 5: Bought or inherited accounts

- ☐ I have stopped using any bought account for anything important.
- ☐ Every service linked to one now uses an email address I created.
- ☐ Passwords on everything connected have been changed.
- ☐ I am watching for password-reset emails I did not request.

Quick rules to remember

- Email is the key to everything else. Protect it first.
- One account per genuine purpose, created by you.
- Never share a password in chat, email or a spreadsheet.
- If a deal on accounts sounds too cheap, it is.

Want a hand putting this into practice?

Delivered Social is a social media, SEO and web agency based in Guildford and Portsmouth. Say hello at deliveredsocial.com/contact/ and we will point you in the right direction.