# Personal data security: how to prevent some common personal data breaches

1. Take care when printing and photocopying

If you’re printing or photocopying on a shared printer, check you’ve left nothing behind before returning to your desk. Put a sign at the printer to remind staff to collect all of their paperwork, including original copies.

2. Double-check letters before posting them

Picking up two letters instead of one is an easy mistake to make if you’re working your way through a stack of them. Ask a colleague to double-check that the right letter is in the right envelope before you post them. Or you could use place-markers to help you spot where one letter ends and the next one starts.

3. Include a return address on your envelopes

If you send a letter and it ends up at the wrong address, the person who receives it by mistake can return it without opening it if you put a return address on the back.

4. Disable autofill in your email settings

If people’s email addresses come up automatically when starting a new email message then you have autofill enabled in your settings. While this tool might save time, it could cost you if you send an email to the wrong person by mistake, so it’s a good idea to disable it.

5. Close your messages when screensharing or presenting online

If you’re doing an online presentation to a group of people, the last thing you want is for a personal message or email to pop up. Close your emails and messaging services before sharing your screen with others.

6. Lock your screen when you’re away from your desk

Encourage everyone to lock their screens when they’re away from their desks. This helps prevent others from seeing information they’re not authorised to see.

7. Don’t share passwords

Staff should all have their own separate log-ins and passwords. They shouldn’t share their passwords with each other. This increases the risk of an unauthorised person seeing or reading personal data.

8. Send electronic documents securely

If you need to send electronic documents, consider encrypting or password-protecting them. This reduces the risk of the wrong person being able to access the documents.

9. Send passwords to protected documents in separate emails

If you’re sending password-protected electronic documents, make sure you send the password separately.

10. Keep your IT systems up-to-date

You can reduce your risk of cyber threats, such as attacks on computer systems, by making sure you regularly install security updates.