# Protect yourself online

There are five simple things we can all do to protect ourselves online.

1. Use a strong password to protect your laptop, computer and mobile devices. To choose a good password, follow [NCSC guidance](https://www.cyberaware.gov.uk/passwords).
2. Think before clicking on links or attachments within emails. By hovering your cursor over the link you can see the actual URL. If you are unsure if an email is genuine, [contact your IT or security team](/guidance/security/report-a-security-incident/).
3. Do not use your work email address to register for accounts on websites for personal use. For example, a shopping website does not need your work email address. Using the wrong address could open up your work email account to spam and fraudulent emails. This in turn could harm your department’s IT system.
4. Protect your online identity. Do not share sensitive information about your work on social media or online professional networks.
5. Do not disclose your level of vetting. If you share this information, you advertise what resources you have access to. This could make you a target for malicious individuals.

For more information, see the [user access page](/guidance/security/it-computer-security/user-access/).

## Contacts

For any further questions relating to security, contact: [security@justice.gov.uk](mailto:security@justice.gov.uk), or for security advice, contact the [Cyber Assistance Team](mailto:CyberConsultancy@digital.justice.gov.uk).

## Feedback

If you have any questions or comments about this guidance, such as suggestions for improvements, please contact: [IT policy content](mailto:itpolicycontent@digital.justice.gov.uk).