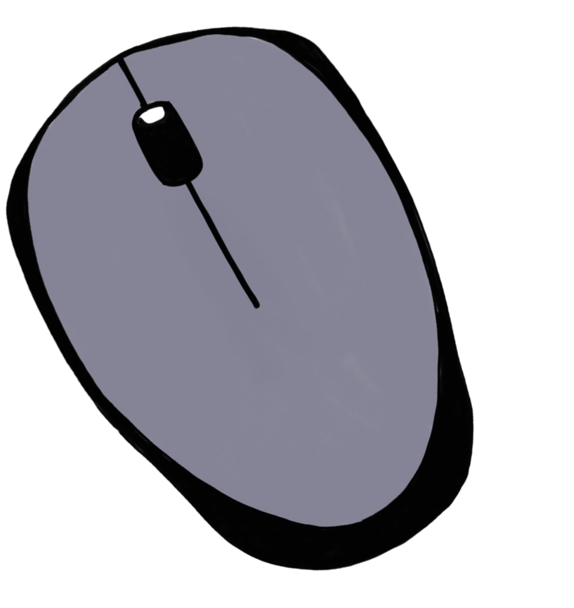
SciencesPo

INTERNET SECURITY BEST PRACTICES

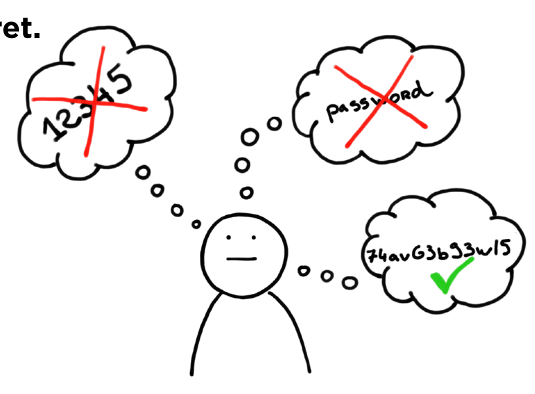


Key Pointers

1 Getting your passwords right

A SECURE PASSWORD IS:

- **Complex** and includes upper and lower case letters, numbers, etc.
- **Unique** to each website.
- **Changed regularly.**
- **Secret.**



IT IS NOT PERMISSIBLE TO:

- ✗ Use the same password for multiple websites.
- ✗ Write a password down on paper or in non-encrypted notes.
- ✗ Share it with others.
- ✗ Save it in one's browser memory.

IF NECESSARY
Use the "forgotten password" function

2 Your Sciences Po password

- Must contain **12 characters minimum.**
- Must include at least **one upper case letter, one lower case and two numbers.**
- To manage your password, visit **https://scpoaccount.sciences-po.fr/**

IF IN DOUBT
Contact the helpdesk:
01 45 49 77 99
sos@sciences-po.fr

3 Updating your devices

- Your devices (computer, telephone, tablet etc.) must be updated regularly.
- All Sciences Po equipment will update automatically, please allow it to do so.
- Please apply security updates on your personal devices too.

4 Protect your devices from unauthorised access

- When in the office, your **laptop must be secured** with a security cable. If you do not have one, **lock your door** when you leave.
- Do not risk allowing someone to use your workstation without your knowledge, always **lock your workstation** when you are not using it.
- Always **log out** of all applications, particularly sharing tools and social networks.

- Your devices must be encrypted. **Keep a close eye on your devices** when using public transport.

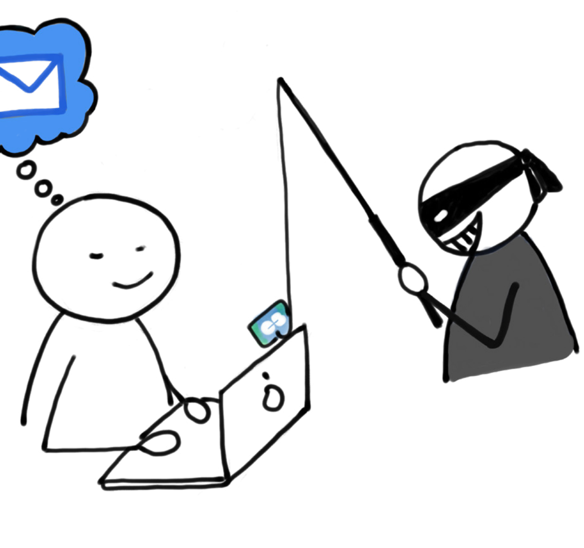
5 Protect confidential data

- ! **Avoid using unsecured wifi networks** when viewing or sharing data.
- Ensure that your phones and devices **require a passcode to unlock.** This will protect your personal data.
- It is imperative that you **encrypt any confidential or sensitive data** before sharing it.
- **Clean out** any unnecessary data on a regular basis.
- ! **Do not trust USB sticks,** particularly if they do not belong to you.

6 Watch out for scams

BE ALERT:

- ✗ **Never share personal information** by phone or email (login details, passwords, bank account numbers etc).
- ✗ Do not reply to **bank transfer** requests.
- ✗ **Do not open links or attachments** without taking certain precautions. Follow best practices.



GENERAL RULES TO FOLLOW:

- ✗ **Never open attachments from unknown senders**
- **Check the sender address** by clicking "Reply" (without sending). If the address seems strange to you, go no further!
- **Check where a hyperlink will take you** by hovering your cursor over it. Only click it if you recognise the address!

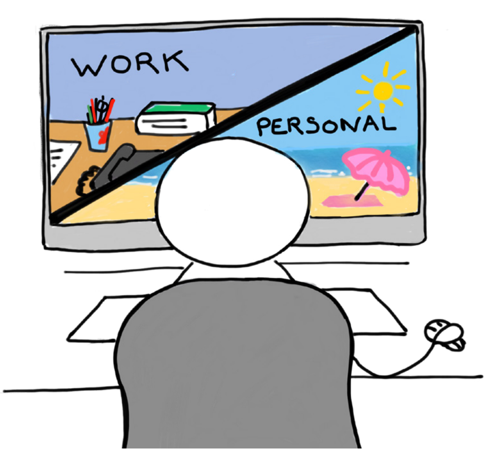
IF IN DOUBT:
Contact the helpdesk:
01 45 49 77 99
sos@sciences-po.fr

7 Protect Sciences Po's legal obligations

- **Secure any contractual documents:** any contract with a third-party company that engages the responsibility of Sciences Po on data must be reviewed by the Legal Department and appraised by the IT department (DSI) and the Data Protection Officer (DPO).
- **Declare any processing of personal data** in the institutional register. Contact the DPO: dpo@sciencespo.fr
- ✗ Data has value. Do not use your Sciences Po account to sign up for any free online software or subscription.

8 Keep your work and your personal life separate

- Organise your private documents and emails into a **folder marked "Private" or "Personal"**
- ✗ **Do not store professional data in your personal online storage tools.**
- ✗ **Do not use your Sciences Po password for personal accounts.**



Browse our Digital Uses site

For any question, please contact the SOS - IT Help Desk

sos@sciencespo.fr

Tel. +33 1 45 49 77 99