INTERNET SECURITY
BEST PRACTICES

Key Pointers

1. Getting your passwords right

- It is not permissible to:
  - Reuse the same password across multiple websites.
  - Share your password with others.
  - Write down your password in a notebook.
  - Save your password in your browser's password manager.

- It is permissible to:
  - Change your password regularly.
  - Use a unique password for each website.
  - Keep your password in a secure location.

2. Your Sciences Po password

- Your Sciences Po password must:
  - Be complex (include upper and lowercase letters, numbers, etc.).
  - Be unique to each website.
  - Be changed regularly.
  - Be kept secret.

- If necessary, use the "forgotten password" function.

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

- Protect your devices in the office 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.

7. Protect Sciences Po’s legal obligations

- Secure any contractual documents:
  - All contracts with third party companies must be checked by Sciences Po's Legal Affairs, Purchasing and Contracts Department (DAJAM) and/or the Data Protection Officer (DPO) if they involve personal data.
  - Declare any processing of personal data in the institutional register.
  - Contact the DPO: marion.lehmans@sciences-po.fr

- Sciences Po’s data is precious. Do not share it via any free websites or software without first checking the potential risks with the DPO and Sciences Po’s Information Systems Security Officers (RSSI):
  - Laurence Gagelin: laurence.gagelin@sciences-po.fr
  - Grégory Quistrebert: gregory.quistrebert@sciences-po.fr

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.

For more information, please contact:
Laurence Gagelin
laurence.gagelin@sciences-po.fr
Grégory Quistrebert
gregory.quistrebert@sciences-po.fr

September 2020 - Drawings: © Sandrine Gaudin / Sciences Po

Browse our Online Tools site for more information.

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