STAY COOL THIS SUMMER

11 tips to be secure online on holiday

Summer holidays are a chance to relax, but they can be a source of high stress themselves if you aren't safe online. To help with this, the European Data Protection Supervisor has created a simple guide to help you stay secure – and in a sunny mood!

1. Think twice on social media

Social networks are great for staying connected with the people we love. However, you should always think about what you publish online. Respect the privacy of other people, and take control of the accessible information you provide.

2. Watch out for online games

Free online games often hide malware. Often your personal data is the "fee" you pay to play, so don't hand out your personal information for a few minutes of fun.

3. Avoid open WiFi

Open WiFi networks might be traps used by hackers to steal your data, avoid them when possible!

4. Be smart about passwords

Passwords are your accounts' main defence. You should use different passwords for each account and change them often; you can make use of a trustworthy password manager to make this easier. Whenever possible, make use of two-step authentication.

5. Check your privacy settings

Always check the privacy settings on your apps: if you are asked for unnecessary permissions (for example a weather forecast app asking to read your contacts or access your camera), just say no!

6. Know your spam & phishing emails

Carefully check all the email you receive: You might be the target of spam or phishing emails. Pay attention to the sender's email, and never open attachments if you are not 100% sure it is safe.

7. Use antivirus & firewalls

Antivirus software and firewalls can prevent your devices from being infected by malware or attacked by hackers, so keep them up-to-date! But remember as well that antivirus software is not perfect – always think before clicking!

8. Back up your data

How important is your data? Imagine that your computer were stolen or your smartphone were lost; would you regret not having a backup copy?

9. Be ready for hacking

Is your account compromised? Don't wait, take action now! Change your passwords as soon as possible, and alert your bank if there is payment information involved.

10. Log off

Always be sure to log off from your accounts after you use a public device.

11. http or https?

Ever wondered what the difference is between http and https in website addresses? The 's' stands for secure, which means it's encrypted. If you don't see the 's', don't give out any personal information – especially for payments.