



Online privacy

Speaking – Intermediate+



WARM-UP

Discuss:

- What is happening on the pictures?
- What does the term “online privacy” mean to you?
- Why is it important to maintain your online privacy?

READING

1. Who might watch and track you online? Make a list. Check your ideas on the next page:



Online privacy

Speaking – Intermediate+

2. look through the list of those who can track your online activities. Match the titles with the paragraphs:

ISP (INTERNET SERVICE PROVIDER)
GOVERNMENT
HACKERS AND CYBER CRIMINALS

YOUR EMPLOYER
ADVERTISERS AND CORPORATIONS

A. _____

Your personal information and online browsing behavior data are very valuable to them. These data help them determine which products or services to promote to you and which ads to show to you.

B. _____

They assign an IP address to your device each time you connect to the Internet. From your IP address, they know everything you do online, including the browser you use, the websites you visit, the emails you send and receive, the files you download, etc.

C. _____

They want you to be productive at work and can monitor your online activities to make sure you don't waste too much time on social media sites, dating sites, or doing other personal activities.

D. _____

They may be spying on you. They also can demand your private information from companies such as Google, Facebook, and your ISP.

E. _____

They make a living out of stealing people's private and financial information. They use a variety of tools and methods available to collect your private information little by little.



Online privacy

Speaking – Intermediate+

3. Discuss:

- Do they have the right to track you?
- For which purposes does each of them track you?
- What negative affect does it have on you?
- Which of them is your biggest privacy concern?

SPEAKING

1. What do you do to protect your online privacy?

2. Read the list of recommendations. Which of these rules do you follow? Why?/Why not? Why each of them might be useful?

1. DO AN ASSESSMENT OF YOUR ONLINE ACTIVITIES
2. INSTALL THE LATEST ANTIVIRUS SOFTWARE ON YOUR DEVICES
3. USE A PERSONAL VPN (VIRTUAL PRIVATE NETWORK)
4. BE CAREFUL WHAT YOU SHARE ON SOCIAL NETWORKING SITES
5. FOLLOW EMAIL SECURITY RULES
6. MAKE SURE SHOPPING SITES ARE SECURE
7. USE STRONG PASSWORDS
8. DELETE OR CLEAR THE TRACKING COOKIES
9. USE PUBLIC WI-FI WITH CAUTION
- 10.REMEMBER TO LOG OUT



Online privacy

Speaking – Intermediate+

3. In your opinion, which those things pose a threat to privacy? Explain your choice.

- CCTV in supermarkets
- Safety cameras in the street
- Hidden cameras in private homes (e.g. to check on babysitters)
- RFID "spy chips" (= radio frequency identification tags: minuscule microchips, which are used to identify things)
- Banks keeping tabs on your financial history
- Mobile phones with tracking systems (GPS)