8c A hacker's life

Reading

1 Work in pairs. How do you (or could you) keep your internet use private and your personal details secure? Think of four ways, using the words to help you. Compare your ideas with another pair and discuss which are most useful.

back up	download	identity	password
theft	transaction	wi-fi	

2 Look at the two definitions for a 'hacker'. Which definition fits your idea of a hacker? Then read the article about a hacker's conference on page 27. What is the author's view?

---

hacker (n) /ˈhækə/

1 an enthusiastic and skilful computer programmer or user

2 a person who uses computers to gain unauthorised access to data

---

3 Read the article again and answer the questions. Compare your answers with your partner.

1 What do DefCon hackers do to help improve internet security?
2 What are most hackers not?
3 What do hackers look at apart from online security?
4 What do they do with the information they find?
5 What does the writer like about the people at DefCon?
6 What two words sum up what *Capture the Flag* is?
7 What does the writer say about the majority of people who use the Internet?
8 What really motivates the hackers at DefCon?

4 Has your opinion of hackers changed after reading this article? How? Discuss with your partner.

Critical thinking identifying personal opinions

5 Work in pairs. Underline the adjectives and adverbs in the article that the writer uses to express his personal opinion.

Example:
But then comes the worrying realisation that …

6 What would you say, in summary, were the writer's personal opinions about the following?

1 the mixture of people he met at the DefCon conference
2 the security of personal data on the Internet
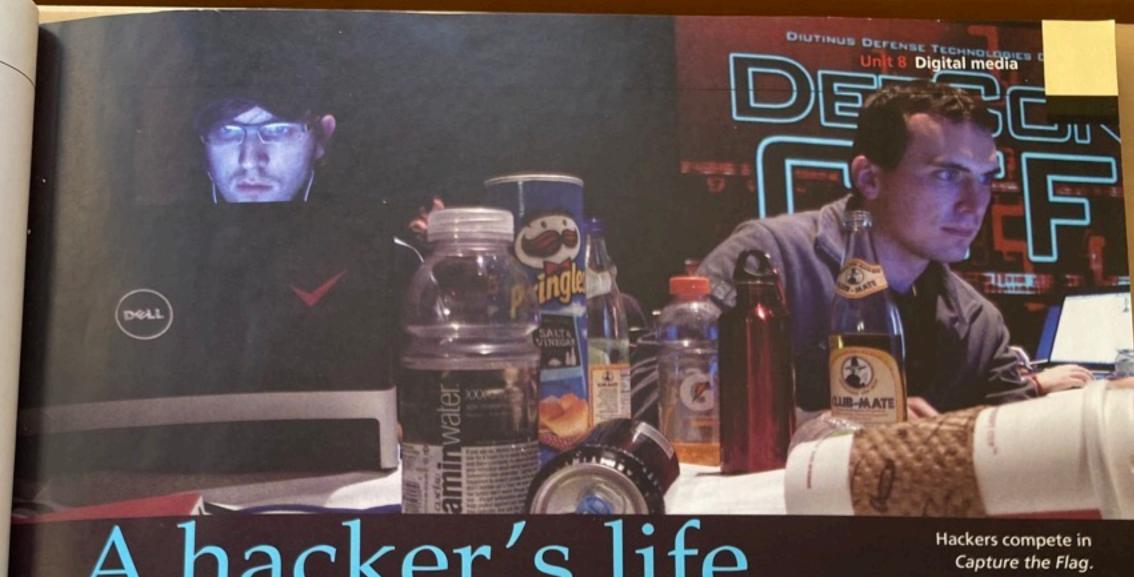3 how we should feel about hackers

Word focus *break*

7 Work in pairs. Find three expressions with *break* (in paragraphs 1, 3 and 5) and discuss with your partner what each expression means.

8 Look at the sentences using expressions with *break* (1–6) and match the expressions with the correct definitions (a–f).

1 The manager called everyone together to **break the news** about the company closing.
2 During the first lesson, the teacher got us to play a couple of games to **break the ice**.
3 They are hoping that their new social networking site will really **break the mould**.
4 You really should buy a new pair of shoes. It won't **break the bank**.
5 It's a very big job but I think we've **broken the back of** it now.
6 We didn't make a profit but I think at least we **broke even**.

a do something very different
b do most of the (hard) work
c help people relax
d make neither a profit nor a loss
e tell (someone) something important
f use up all one's money

9 Write a sentence using one of the expressions with *break*. Read it to your partner, omitting the phrase, and ask them to guess what the missing phrase is.

Speaking

10 Work in pairs. Some important data has gone missing from an office computer. You are going to act out a meeting between a small business owner and an internet security consultant.

Student A: Turn to page 81. Look at the notes and prepare your answers.

Student B: turn to page 82. Look at the notes. Then prepare to ask questions and give advice.

A hacker's life

Hackers compete in
Capture the Flag.

Have you ever locked yourself out of your home and had to try to break in? First, you get a sense of accomplishment in succeeding. But then comes the worrying realisation that if *you* can break into your own place as an amateur, a professional could do so five times faster. So you look at the weak point in your security and fix it. Well, that's more or less how the DefCon hackers conference works.

Every year passionate hackers meet at DefCon in Las Vegas to present their knowledge and capabilities. Mention the word 'hacker' and many of us picture a seventeen-year-old geek sitting in their bedroom, illegally hacking into the US's defence secrets in the Pentagon. Or we just think 'criminals'. But that is actually a gross misrepresentation of what most hackers do.

The activities and experiments that take place at DefCon have an enormous impact on our daily lives. These are people who love the challenge of finding security gaps: computer addicts who can't break the habit. They look with great scrutiny at all kinds of systems, from the Internet to mobile communications to household door locks. And then they try to hack them. In doing so, they are doing all of us a great service, because they pass on their findings to the industries that design these systems, which are then able to plug the security holes.

A graphic example of this is when I attended a presentation on electronic door locks. Ironically, one of the most secure locks they demonstrated was a 4,000-year-old Egyptian tumbler lock. But when it came to more modern devices, the presenters revealed significant weaknesses in several brands of electro-mechanical locks. A bio-lock that uses a fingerprint scan for entry was defeated, easily, by a paper clip. (Unfortunately, although all the manufacturers of the insecure locks were alerted, not all of them responded.)

DefCon is a vast mix of cultures as well as a culture in itself. People in dark clothes and ripped jeans talk to people in golf shirts and khakis. Social status here is based on knowledge and accomplishment, not on clothing labels or car marques. It's kind of refreshing. There are government agents here, as well as video game enthusiasts. Not that people ask each other where they work – that would break the hackers' etiquette.

In an attempt to attract the brightest hackers, DefCon runs a competition called *Capture the Flag. Capture the Flag* pits elite hackers against each other in a cyber game of network attack and defence, that goes on 24 hours a day. In a large, dimly lit conference hall, small groups of hackers sit five metres from each other, intensely trying either to protect or to break into the system. There are huge video projections on the walls, pizza boxes and coffee cups are strewn everywhere. The room is mesmerising.

In another room, another contest is taking place. Here participants have five minutes to free themselves from handcuffs, escape from their 'cell', get past a guard, retrieve their passport from a locked filing cabinet, leave through another locked door, and make their escape to freedom.

If you're someone who dismisses the DefCon attendees as a group of geeks and social misfits, then you probably have the same password for 90 per cent of your online existence. Which means you are doomed. Because even if you think you're being clever by using your grandmother's birth date backwards as a secure key, you're no match for the people that I've met. There is no greater ignorance to be found online than that of an average internet user. I'm happy to admit that I'm one of them. I'm also aware that there are other people out there – big business among them – who are trying to get more and more access to the data of our personal online habits. Sadly, we have few tools to protect ourselves. But there is a group of people who are passionate about online freedom and have the means to help us protect our privacy. Many of them can be found at DefCon.

---

do someone a service (v) /duː ˈsʌmwʌn eɪ ˈsɜːvɪs/ help someone
etiquette (n) /ˈetɪket/ code of polite behaviour
handcuffs (n) /ˈhæn(d)kʌfs/ a pair of metal rings placed on the wrists to restrain someone
khakis (n) /ˈkɑːkis/ light-coloured smart casual trousers

5B Student A

a Read the text and prepare to tell your partner about the main points in each section.

ESS VERIFIED

'A passion for technology and a keen eye for detail is required.'

Ethical hacker

Typical salary: $60,000 to $90,000 at the team leader level, while a newly-qualified hacker can expect a minimum salary of $35,000 to $50,000.

The job: A company will pay an ethical hacker to hack into its computer system to see how well it might stand up to a real attack.

Qualifications: For government work, ethical hackers must hold a relevant qualification. In the financial services sector, these qualifications are a mandatory requirement for some types of specialist work. However, you don't necessarily need a degree in computer science, says Ian Glover, president of Crest. 'The industry accepts individuals with a very wide range of academic backgrounds and skills. Often, people have not come the traditional route through education because the "system" did not necessarily match their way of working and learning.'

To succeed as an ethical hacker, you need ... a passion for technology and detail. You should also have a very good analytical mind, enjoy solving difficult problems and be able to articulate your observations to senior management.

Worst thing about the job: 'When we're called in to test the security of a new customer's network, only to discover that they have already been the victim of a data breach,' says Matthew Gough from cyber security consultancy Nettitude, 'we have to explain that sensitive data belonging to the company's customers has been compromised by hackers. It's not pleasant.' To stay on top of the latest threats, you have to constantly update your knowledge in your spare time. Specialist consultancies will also expect you to be flexible and willing to travel.

b ▶ Now go back to p.61

3C

a Read conversations 1–4. Complete the sentences with your own ideas. Think about how you will describe your experiences.

① I wouldn't travel by _____ to _____ if I were you.
Why not?
In a nutshell ... (summarise what's wrong with it)

② I had a terrible time when I went to _____.
What happened?
Well, to cut a long story short ... (summarise what happened)

③ I shouldn't have said _____ about _____.
Why not?
Well, what I meant by that was ... (paraphrase what you intended to say)

④ I think that _____ is absolutely perfect!
Really?
That is to say ... (rephrase your opinion, giving your evidence)

b Student A use the pink speech bubbles. Start conversation 1 with Student B. Student B use the green bubbles. Have conversations 1 to 4. Then swap roles.