The ex-hacker

STARTER 1 Find the answers to these questions as quickly as you can.

1 Which group hacked into Hotmail?
2 Who was 'The Analyser' and what did he do?
3 Which hacker was sent to jail for fraud?
4 What was the effect of the 1996 raid on Scotland Yard?
5 Which of the cases reported here involved teenagers?
6 What did hackers do to the Yahoo! website?
7 What crime was Raphael Gray accused of?

Kevin Mitnick is the hackers' hero. His latest spell in jail was a 46-month sentence for fraud relating to breaking into the systems of several multinational corporations. He was released on condition that he did not have any contact with a computer.

Hotmail, Microsoft's free email service, was hacked into last September, exposing the correspondence of more than 40m users. A group calling itself Hackers Unite posted a Web address with details of how to access any Hotmail account. The service was shut down for five hours.

In March 2000, a Welsh teenager allegedly stole information from more than 26,000 credit card accounts across Britain, the US, Japan, Canada and Thailand, and published the details on the Internet. FBI agents and British police raided the home of Raphael Gray,18, and arrested him and his friend. He has been charged with 10 counts of downloading unauthorised information.

The UK Department of Trade and Industry has twice been prey to hackers, once in 1996 and again in 2000 when a DTI computer was programmed to reroute email. The Home Office investigated nine cases of hacking last year, one of which was the leaking of a report on a murder. In August 1996 hackers ran up a £1m phone bill for Scotland Yard but did not access flies.

In 1998 Washington revealed that an Israeli hacker called 'The Analyser' was responsible for 'the most organised attempt to penetrate the Pentagon's computer systems'. He turned out to be Ehud Tenenbaum, 18, who had planted a list of his own passwords in the Pentagon system and passed them to other hackers.

In 1997 hackers got into the Yahoo! website, replacing the homepage with a ransom note demanding the release of their hero, Kevin Mitnick. Unless the demand was met, the note said, a virus would be released in all Yahoo!'s computers. The company dismissed the threat as a hoax, but the 'Free Kevin' slogan continued to appear on other hijacked sites.

In 1997 the son of a fraud squad detective walked free from a court in London after charges of breaching the security of the US air force were dropped. Three years earlier Mathew Bevan, then 19, and a friend, Richard Pryce, 16, used the Internet to gain access to several US military bases. Pryce was fined £1,200 after admitting several other offences.

LISTENING **2** Think about these questions before you listen.

1 How could you hack into a system?
2 How could you stop people hacking into a system?

3 Now listen to Part 1 of the recording to check your answers to Task 2 and to find the answers to these questions:

1 What was Ralph arrested for?
2 What does he do now?
3 Why does he say people are too trusting?
4 What passwords does he suggest for trying to get into a system?
5 What does a firewall do?
6 What is the advantage of a callback system?
7 To prevent hacking, what sort of passwords should you avoid?
8 What do event logs show?

4 Now listen to Part 2 of the recording and find the answers to these questions:

1 How did Ralph start thinking about computer security?
2 How did he find the most senior ID in the American company's system?
3 According to Ralph, why do people hack?
4 Why did he and his friend hack?
5 How did the police find him?
6 Why does he say companies should use his services?
7 Do hackers know each other?
8 What's the difference between Hollywood hackers and the real world?
9 How risky is credit card use on the Internet?
10 What advice does he give for people intending to use credit cards over the Internet?

5 Now listen to both parts again to find the answers to these questions:

1 What evidence did Ralph and his friend leave to show that they had hacked into the American company's system?
2 What is a 'white hat' hacker?
3 What two ways does Ralph give for hacking into a system?
4 What terms does Ralph use to describe someone obsessed by computers?
5 How does he maintain contact with the policeman who arrested him?
6 How does he describe his lack of enthusiasm for the Hollywood hacker?
7 What does he mean by 'It's the retailers who get done'?
8 What's the problem with using smart cards for Internet purchases?

LANGUAGE WORK Phrasal verbs

A phrasal verb is a verb + preposition combination. For example, *look up, take down, turn over.* Phrasal verbs are common in informal, spoken English. Sometimes they have a more formal one word equivalent, for example, *work out* = determine.

Often phrasal verbs have two meanings.

One we can work out from the meaning of the two words separately:

She *looked up* at the roof.

A special meaning which does not easily relate to the separate meanings of the words:

She *looked up* a word in the dictionary.

6 Study these phrasal verbs from the Task 1 texts and the recording:

break into	grow up	throw away
get into	phone up	log on
hack into	run up	find out
go about	keep at	track down
set about	shut down	hand over
keep ahead		

Now complete each blank with the appropriate phrasal verb in the correct form. In some cases, more than one answer is possible.

WORD STUDY **8** **Semantic groups** Group these terms into the five headings, A to E, below.

A	B	C	D	E
Viruses and other destructive programs	Data protection	Communication systems	Internet	World Wide Web

anti-virus software
backups
bandwidth
browser
domain name
encryption
firewalls
FTP
GPS
IRC
ISP
hyperlink
logic bomb
pagers
passwords
router
trigger routine
Trojan
URL
Usenet
XML

SPEAKING **9** **Role play** Work in pairs. Together make up your own questions on these prompts. Then play the parts of the interviewer and Ralph.

1 first interested in hacking
2 reason for being arrested
3 present job
4 ways to avoid hackers
5 views on Hollywood hackers
6 safe ways of paying for Internet shopping

WRITING **10** Write a news item like the short newspaper texts given in Task 1 about Ralph or about any other hacking case known to you.

11 Study this extract from a virus information database. Then make a flowchart to show each step in the method of infection for this virus. Steps 1 and 2 are done for you.

Step 1 An infected .EXE file arrives as an email attachment.
Step 2 The infected .EXE file is opened.

Virus name W32/Magistr.@MM
Risk assessment Medium
Date discovered 12/3/01
Origin Sweden
Length Varies, adds at least 24KB
Type virus Sub-type worm

Method of infection

This is a combination of a files infector virus and an email worm.

The virus arrives as an .EXE file with varying filenames. When you execute the attachment, your machine is infected and in turn is used to spread the virus.

When first run, the virus may copy one .EXE file in the Windows or Windows System directory using the same name but with the final character of the filename decreased by a factor of 1. For example, EHGEDI57.EXE will become EHGEDI56.EXE, TCONTRACT.EXE will become TCONTRACS.EXE.

This copy is then infected and a WIN.INI entry, or registry run key value may be created, to execute the infected file when the system starts up.

This copied executable infects other 32 bit .EXE files in the Windows directory and subdirectories, when run.

Five minutes after the file is opened, the email worm attempts a mailing routine. It creates a .DAT file hidden somewhere on the hard disk. This contains strings of the files used to grab email addresses from address books and mailboxes. The .DAT file name will be named after the machine name in a coded fashion. For example, y becomes a, x becomes b. Numbers are not changed. The worm uses mass mailing techniques to send itself to these addresses. The subject headings, text and attachments will vary. The text is taken from other files on the victim's computer.

This worm may also alter the REPLY-TO email address when mailing itself to others. One letter of the address will be changed. This makes it difficult to warn the victim that their machine is infecting others as the message will be returned to sender.

1 Hackers try to ..... passwords so they can penetrate a system.
2 Don't ..... your password to anyone who asks for it.
3 The police ..... Ralph ..... by talking to his friends and acquaintances.
4 Some hackers ..... systems to get commercially valuable information.
5 When you ..... to a network, you have to provide an ID.
6 How do you ..... hacking into a system?
7 Hackers may ..... , pretending to be from your company, and ask for your password.
8 Never ..... your credit card receipts where someone can find them.
9 Ralph was a hacker as a teenager but he's ..... now and become more responsible.
10 ..... a system is strictly illegal nowadays.
11 It's a constant race to ..... of the hackers.

7 Replace the verb in italics with a phrasal verb of similar meaning. All the phrasal verbs required have been used in this book.

1 Don't *discard* your credit card receipts; they could help fraudsters.
2 Trying to *penetrate* computer systems is against the law.
3 The typical hacker is a young person who has not *matured* yet.
4 The best way to *begin* hacking into a system is to try to get hold of a password.
5 If someone *telephones* you and asks for your password, don't *provide* it.
6 Hackers *closed* Hotmail for five hours.
7 Hackers *accumulated* a telephone bill of £lm for Scotland Yard.
8 The difficult thing was to *determine* how the website would look.
9 So you won't forget, *record* the ID number the support technician gives you.
10 *Examine* the manufacturers' websites before you phone for help.

WORD STUDY **8** **Semantic groups** Group these terms into the five headings, A to E, below.

A	B	C	D	E
Viruses and other destructive programs	Data protection	Communication systems	Internet	World Wide Web

anti-virus software
backups
bandwidth
browser
domain name
encryption
firewalls
FTP
GPS
IRC
ISP
hyperlink
logic bomb
pagers
passwords
router
trigger routine
Trojan
URL
Usenet
XML

SPEAKING **9** **Role play** Work in pairs. Together make up your own questions on these prompts. Then play the parts of the interviewer and Ralph.

1 first interested in hacking
2 reason for being arrested
3 present job
4 ways to avoid hackers
5 views on Hollywood hackers
6 safe ways of paying for Internet shopping

WRITING **10** Write a news item like the short newspaper texts given in Task 1 about Ralph or about any other hacking case known to you.

11 **Study this extract from a virus information database. Then make a flowchart to show each step in the method of infection for this virus. Steps 1 and 2 are done for you.**

Step 1 **An infected .EXE file arrives as an email attachment.**
Step 2 **The infected .EXE file is opened.**

Virus name W32/Magistr.@MM
Risk assessment Medium
Date discovered 12/3/01
Origin Sweden
Length Varies, adds at least 24KB
Type virus Sub-type worm

Method of infection

This is a combination of a files infector virus and an email worm.

The virus arrives as an .EXE file with varying filenames. When you execute the attachment, your machine is infected and in turn is used to spread the virus.

When first run, the virus may copy one .EXE file in the Windows or Windows System directory using the same name but with the final character of the filename decreased by a factor of 1. For example, EHGEDI57.EXE will become EHGEDI56.EXE, TCONTRACT.EXE will become TCONTRACS.EXE.

This copy is then infected and a WIN.INI entry, or registry run key value may be created, to execute the infected file when the system starts up.

This copied executable infects other 32 bit .EXE files in the Windows directory and subdirectories, when run.

Five minutes after the file is opened, the email worm attempts a mailing routine. It creates a .DAT file hidden somewhere on the hard disk. This contains strings of the files used to grab email addresses from address books and mailboxes. The .DAT file name will be named after the machine name in a coded fashion. For example, y becomes a, x becomes b. Numbers are not changed. The worm uses mass mailing techniques to send itself to these addresses. The subject headings, text and attachments will vary. The text is taken from other files on the victim's computer.

This worm may also alter the REPLY-TO email address when mailing itself to others. One letter of the address will be changed. This makes it difficult to warn the victim that their machine is infecting others as the message will be returned to sender.