

Online fraudster

Level 3 • Advanced

1 Key words

Match these key words from the text with the definitions below.

1. a fraudster
2. a piece of kit
3. a spree
4. chip and pin
5. a party piece
6. a scam

- a. A dishonest plan for getting money.
- b. A kind of criminal who gets money from people by tricking them.
- c. A short period of time in which you do something a lot, such as spending money or drinking.
- d. A system for paying for something using a credit/debit card that has information stored on it using a microchip.
- e. A tool used for a particular purpose.
- f. A trick, song, or dance that you can perform at a party to entertain people.

2 What do you think?

Read the headline of the article. What do you think the article is about?

1. Online shopping sites are creating a new generation of criminals.
2. Despite tougher security, identity and credit card theft are at an all-time high.
3. Comic criminal describes ways to get rich quick.
4. Giving personal details over the phone causes great risk to consumers, says report.

Online fraudster

Level 3 • Advanced

It's easy money, says online fraudster who stole £250,000

Bobbie Johnson, technology correspondent
May 3, 2007

- 1 On the outside, Tee was a typical student. Living away from home was proving expensive, and he had racked up a sizable debt in a short time. Like most of his peers, he had a computer and a phone in his room - but instead of using them to study, he turned them into the tools of a 21st century criminal.
- 2 In his short career as a fraudster, Tee - who is trying to rebuild his life after serving a long prison sentence, and agreed to speak anonymously - estimates that he stole as much as £250,000 through a mixture of harvested credit card details, identity theft and bank account takeover. Police officials last week said the volume of online crime was so high that they could not investigate every case, and that big criminals were moving into the fast-growing field.
- 3 Bill Hughes, director general of the Serious and Organized Crime Agency, told a House of Lords investigation into Internet security: "Everybody has a laptop now, and it's seen as just another piece of kit, almost like a toaster or kettle. But it's not, and it can be used in another way."
- 4 For Tee, who served almost four years for conspiracy to defraud, the chance to use people's ignorance against them was just too easy. "Although it sounds really flippant, it wasn't even like a part-time job - because at least in a job you have to work a few hours," he said. "Maybe it took an hour a night if I really felt like it. But to me it felt like a bit of fun and a pastime which developed into an easy way of making money."
- 5 In spare moments around his university schedule - he was studying law - the young Yorkshireman would take card details lifted from insecure websites or passed on from other criminals, and embark on spending sprees that netted him cars, clothes and cash. Sometimes scant details such as a name and phone number could open the door.
- 6 "I used to go through different methods depending on how confident I felt," he said. "I used to call people up and pretend to be from a fraud department and just ask them for their details. But sometimes it's as easy as getting information from a local video shop."
- 7 Now, 26, Tee admits that by the time he was caught he was looking into the possibility of getting bank loans and even mortgages using stolen identities.
- 8 "It was just a game to see how far you could go," he said. "My little party piece was that you get a card in someone's name and use it. Then, within 24 hours, you call the bank up and convince them that you're the genuine person and that you haven't made those transactions - and they refund it. Then you just go to the cash machine and take it all out again." He even sent flowers to one victim, using their stolen bank details to pay for the bouquet as a callous gesture of thanks.
- 9 People like Tee represent the smallest end of what is now a multibillion pound criminal industry. Statistics from Cifas, the UK's fraud prevention service, show that identity theft was up almost 20% last year, while Internet and card fraud rose to an all-time high of £414m in 2006.
- 10 Martin Gill, a criminologist at the University of Leicester, who has studied the actions and motivations of fraudsters - Tee was one of his interviewees - said the perceived ease of fraud, particularly when using the Internet, was encouraging to those who commit crime. "One of the things that comes through is the belief that they're not going to get caught," he said.
- 11 Industry insiders say a large number of cases still go unreported because conviction has proved so difficult.
- 12 "The common reaction among companies selling goods is a real frustration at how hard it is to prosecute and get convictions for people who commit fraud," said Keith Marsden, managing

Online fraudster

Level 3 • Advanced

director of 192.com, which sponsors Prove-ID, a private industrial forum on dealing with fraud. "It's a hard process to go through."

13 Instead, companies are opting for tougher security procedures and programmes to educate the public about safe Internet use.

14 But experienced fraudsters like Tee say that it is still too easy. Even chip and pin, which has drastically cut physical fraud levels, can prove beneficial to the seasoned criminal. "I thought chip and pin was brilliant - now cashiers think they've got no right to look at your card. If I wanted to, I could pretend to be anyone, because nobody will ever check. It's a new opportunity for them."

15 How to avoid scams

- Never give personal details over the phone. Banks should never ask for pin numbers or codes.
- Only shop on secure websites that display a padlock or key symbol in your browser. The address should start https instead of http.
- Only open email attachments if you are entirely sure it is necessary.
- Be wary of suspicious-looking email. Some viruses use the name of somebody you trust as a disguise.

© Guardian News & Media 2007

First published in *The Guardian*, 3/5/07

Online fraudster

Level 3 • Advanced

3 Comprehension check

Choose the best answer according to the text.

1. Why did Tee become a criminal?
2. Was Tee ever caught?
3. What three methods did Tee use to get people's personal information, according to the article?
4. According to criminologists, why do people commit online crime?
5. How are companies fighting online fraud?
6. Why does Tee think chip and pin is good for criminals?

4 Vocabulary 1: Words in context

Read the article again and choose the best definition for each of these words.

1. (para 4) If someone is **flippant** they are being a) serious. b) not serious.
2. (para 5) If you **net** something you a) catch it. b) lose it.
3. (para 5) **Scant details** means a) many details. b) few details.
4. (para 8) **Callous** means a) kind. b) cruel
5. (para 13) To **opt** for something means to a) choose it. b) reject it
6. (para 15) If you are **wary** of something you a) trust it. b) don't trust it

Online fraudster

Level 3 • Advanced

5 Vocabulary 2: Word formation

Complete the sentences with the correct form of the word in CAPITALS.

1. SIZE Tee built up a _____ debt while at University.
2. CONSPIRE Tee went to prison for _____ to defraud.
3. SECURITY Tee could find people's details on _____ websites.
4. INTERVIEW Martin Gill studied online crime and Tee was one of his _____ .
5. BELIEVE Criminals hold the _____ that they will not be caught.
6. BENEFIT Tee says that chip and pin methods are _____ to criminals.

6 Vocabulary 3: Collocations

Make collocations with the words from A and the words from B.

A

to rack up
a fast-growing
a spending
to commit
seasoned
to serve a
security
bank

B

crimes
criminals
debts
details
field
prison sentence
procedures
spree

7 Discussion

Do you feel secure when shopping or giving out your personal details online? What security precautions do you take when using the Internet?