

# Rat in your cellphone



I've just walked into a windowless room on an industrial estate where three cellphone analysts in blue shirts sit at their terminals, scrutinising some embarrassing romantic text messages on my SIM card that are invisible on my current handset and thus forgotten. 'If it's any consolation, we would have found them even if you had deleted them,' says one of the blue shirts.

Worse, it seems text messages aren't the only thing I have to worry about: 'Is this the address of your office?' another asks (the answer is yes). 'And did you enjoy your pizza on Monday night? And why did you divert from your normal route to work to visit this address in Camberwell, London, on Saturday?'

I'm at DiskLabs, a company that handles cellphone forensic analysis for UK police forces and for private investigations. I'm curious to know just how much personal information can be gleaned from our used handsets and SIM cards.

So just how secure is the data we store on our phones? If we are starting to use them as combined diaries and wallets, what happens if we lose them or if they are stolen?

According to the UK government's Design and Technology Alliance Against Crime (DTAAC), 80 per cent of us carry information on our handsets that could be used to commit fraud—and about 16 per cent of us keep our bank details on our phones. I thought my phone would hold few surprises, though, since I had only been using it for a few weeks before I submitted it to DiskLabs. Yet, their analysts proved me wrong.

Aside from the text messages stored on my SIM card, the most detailed personal information that could be gleaned from my handset came from an application called Sports Tracker. It allows users to measure their athletic performance over time and I had been using it to measure how fast I could cycle to work across London. It records distance travelled, fastest speed at different points along the route and roughly how many calories I burn off. Sports Tracker also recorded what time I normally leave the house in the morning and when I return from work. I had deliberately chosen to turn Sports Tracker on, and many people might not stop to consider how such programs could be used against them.

A phone-based calendar could also leave you vulnerable. Police in the UK have already identified burglaries that were committed after the thief stole a phone and then targeted the individual's home because their calendar said they were away on holiday.

A growing awareness of identity theft means that many people now destroy or wipe computer hard drives before throwing them away, but the same thing isn't yet happening with cellphones. So how can people go about making their phones more secure?

Turning on the security settings is an important first step, as this may dissuade potential thieves from going to the effort of trying to crack the codes. Then you make sure you delete anything you want to keep secret, while bearing in mind that it is often possible to recover it.

40. The 'Rat' in the title of the text refers to
- (A) an unwanted cellphone application.
  - (B) criminals who hack into people's cellphones.
  - (C) the forensic expert examining the writer's cellphone.
  - (D) the information in a cellphone that can be used against the owner.
41. The writer allowed her own SIM card to be analysed. During the process she is embarrassed about
- (A) her technological ineptitude.
  - (B) her lack of journalistic preparation.
  - (C) the disclosure of her personal information.
  - (D) the reaction of the analysts to her personal information.
42. Which word is closest in meaning to 'gleaned'?
- (A) stolen      (B) assumed      (C) interpreted      (D) extracted
43. Which of the following is **NOT** a purpose for using statistics in the text?
- (A) to quantify the magnitude of the problem
  - (B) to provide validity to the writer's statements
  - (C) to inform the public of the work that DTAAC does
  - (D) to raise awareness of an issue affecting cellphone users
44. Which word is closest in meaning to 'vulnerable' as it is used in the text?
- (A) weak
  - (B) fearful
  - (C) exposed
  - (D) dependent
45. 'many people now destroy or wipe computer hard drives before throwing them away, but the same thing isn't yet happening with cellphones.'
- Based on the information in the text, why is this the case?
- (A) People are not as aware of the potential for identity theft with cellphones.
  - (B) There are no hard drives in cellphones that users can remove information from.
  - (C) Cellphones are a more recent invention and do not have the same security settings.
  - (D) Data on cellphones is often protected by codes, making people complacent about their security.
46. Which option could replace the last sentence in the text and retain the same meaning?
- (A) After bearing in mind that information is easily recovered, try deleting anything you wish to keep confidential.
  - (B) Next, ensure anything that is to remain confidential is deleted, knowing that the information may be recoverable.
  - (C) Next, privately delete information, at the same time understanding that it is potentially recoverable.
  - (D) Keep in mind that data is frequently recoverable, then consider deleting sensitive information.