Companies these days spend thousands of dollars on their computer security. They buy the best **firewalls** and computer programs. However, Kevin Mitnick thinks the biggest danger these days is not a weakness in **technology**.

In the 1990s, Kevin Mitnick was an infamous hacker. He **hacked into** government and **corporate** computer systems. After being sent to **prison**, Mitnick decided to use his skills in a different way. He started his own computer security **firm**. He now advises people on how to keep their computers safe.



According to Mitnick, the biggest danger to security is people. However, by this he doesn't mean hackers. In fact, he means the people using the programs. "If an attacker can get one trusting person to give his or her information, the attacker gets in. All that money spent is basically **wasted**." A hacker can get around everything with just one person within the company.

Unfortunately, people are still too trusting. In a recent test of the US **tax office** (the IRS), security experts called 100 **managers**. They posed as IRS computer **technicians**. The experts were able to **fool** 35 of the managers. They gave both their passwords and IDs. In the hands of real hackers, this would have been a disaster!

Choose the best answer.

1. What is the main idea of this reading?
   a. Managers need to be more careful about who they talk to.
   b. Hackers can help us make our computers safe.
   c. Technology is not helpful if people aren't careful.
   d. It's important to get the newest technology.

2. What is true about Kevin Mitnick?
   a. He now works for the US government.
   b. He thinks security technology is too expensive.
   c. He used to be a criminal.
   d. He teaches people how to hack computers.

3. What happened at the IRS?
   a. Hackers stole important information.
   b. Employees gave information to the wrong people.
   c. The security technology had a problem.
   d. Managers tested the computer system.

4. What is Kevin Mitnick's advice to us?
   a. Don't give information to strangers.
   b. Buy the newest firewalls.
   c. Test your computer systems often.
   d. Don't store important information on computers.

5. What does the word "they" refer to in line 22?
   a. Experts
   b. Technicians
   c. Managers
   d. Hackers

LIVEWORKSHEETS