

**ŽUPANIJSKO NATJECANJE IZ ENGLESKOGA JEZIKA**  
**za 2. razred srednjih škola**

<b>SLUŠANJE S RAZUMIJEVANJEM</b>
----------------------------------

---

**Good morning. May I have your attention, please? The listening part of the test will start now.**

[Note for the teacher: DO NOT stop or pause the recording until you hear the sentence: *This is the end of the listening task. You may now go on to do the other parts of the test.*]

**Open your tests to page 2. As you can see, the listening task and questions are on this page.**

**You will hear a news report on phishing, which is a type of computer fraud.**

**You will hear the report twice, and there will be a short pause between the two readings.**

**You can write your answers during both the first and second readings.**

**For questions 1- 10, complete the sentences using no more than one word or a number for each gap. You will hear the exact words that you need to use. You do not need to change them. The answers will occur in the same order as the questions.**

**While you are listening, write your answers on the task itself. You may cross out your answers, change them, make notes or underline words if you wish.**

**After the second reading, you will have 2 minutes to check your answers and transfer your final answers to the separate Answer Sheet.**

**Now, let's begin. You have 30 seconds to read through the questions.**

**Now you will hear the report.**

[Read the report at natural speed.]

[A pause of 10 seconds between the two recordings/readings ]

**Now you will hear the report for the second time.**

[Read the report at natural speed.]

[Count silently to 120 – and then say the following:]

**This is the end of the listening task. You may now go on to do the other parts of the test.**

## Phishing

One of the country's leading experts on computer crime has warned the nation's internet users of the dangers of phishing. Phishing, which is spelt p-h-i-s-h-i-n-g, is a particular type of online fraud in which criminals try to obtain details from computer users in order to access and empty their bank accounts. The word is based on the word fishing, spelt with an 'f', as the person committing the fraud hopes to catch their victim in the same way that an angler catches a fish. The phenomenon has been called social engineering, as it involves manipulating people to voluntarily provide confidential information via e-mail or even social network sites.

A typical phishing scam might involve sending an e-mail that appears as if it has been sent by the recipient's bank and which asks the recipient to confirm the number of their account and online banking password. If the person falls for the trick, the phisher then uses the information to gain access to the account and take money from it. These e-mails might also contain links to false websites.

Although the number of such phishing mails has risen lately, the number of people being tricked has gone down slightly. Last year, for example, the number of people not replying to phishing scams rose to 80 per cent compared to 70 per cent the previous year. There has been a similar decline in the amount of money lost in online scams. The figure for the twelve months that have just passed was about 30 million euros, which was some 10 million euros down on the year before. However, when it comes to falling victim to online crime, it's not just individuals who are at risk but businesses too. In particular, smaller companies are vulnerable because they do not have the resources that are available to large firms.

Victims are not only targeted for their bank details. Credit card owners can be fooled into paying for all sorts of things. A recent confidence trick involved PC owners receiving notification that their PC had been infected by a particularly harmful virus which could be removed by buying anti-virus software. Although such a message was an obvious attempt at fraud, it is estimated that three per cent of recipients were persuaded to enter their credit card details to buy it.

It would seem that the problem is not as new as some people think. The technique was first recorded in the United States some twenty-five years ago back in 1987, although the first actual appearance of the term dates to 1996 in the same country. By 2004, it was officially considered to be an economic crime in most states.

Nevertheless, the authorities have started to fight back against this menace. Six people were recently found guilty of committing online fraud in the state of California. They are currently awaiting sentencing and could face up to twenty-five years in prison. A year ago, across the border in Canada, a fraudster received 60 months in jail for phishing. There are also a number of similar cases waiting to come to trial in Europe.

Besides legal measures, there are also other responses available. For instance, you can always purchase anti-phishing software to protect your PC, although the most effective step is education on the risks involved. People receiving e-mails asking for confidential information should always check with the relevant firm or institution to see if the request is an authentic one.

One would imagine that phishing will become more common in the years to come. In fact, it would appear that it is likely to become a rarer occurrence as fraudsters turn to increasingly sophisticated online methods to gain access to information.