Top Scams on the Web

645 Administrator Thu, Sep 2, 2010 Internet Based Business 0 3137

PandaLabs has drawn up a ranking of the most widely used internet scams over the last few years. These confidence tricks, which are still in wide circulation, all have the same objective: to defraud users of amounts ranging from $500 to thousands of dollars.

Typically, these scams follow a similar pattern. Initial contact is made via email or through social networks. The intended victim is then asked to respond, either by email, telephone, fax, etc. Once this initial bait has been taken, criminals will try to gain the trust of the victim, finally asking for a sum of money under one pretext or another.

Below are the most frequent scams of the last 10 years, based on their distribution and the frequency with which they are received.

Nigerian scam: This was the first type of scam to appear on the Internet, and continues to be widely used by cyber-criminals today. This typically arrives in the form of an email, claiming to be from someone who needs to get a very large sum of money out of a country (normally Nigeria, hence the name). You are promised a substantial reward if you help to do this. However, those that take the bait will be asked to forward an initial sum to help pay bank fees (often around $1,000). Once you have paid, the contact disappears and your money is lost.

Lotteries: In essence, this is similar to the Nigerian scam. An email arrives claiming that you are the winner of a lottery, and asking for your details in order to transfer the substantial winnings. As with the previous scam, victims are asked to front up around $1,000 to cover bank fees, etc.

Girlfriends: A beautiful girl, normally from Russia, finds your email address and wants to get to know you. She will always be young and desperate to visit your country and meet you, as she has fallen head-over-heels in love with you. She wants to come immediately, but at the last moment there is a problem and she needs some money (once again, around $1000 should cover it) to sort out flight tickets, visas, etc. Unsurprisingly, not only does your money disappear, but so does the girl.

Job offers: This time you receive a message from a foreign company looking for financial agents in your country. The work is easy -you can do it from home- and you can earn up to $3,000 working just three or four hours a day. If you accept, you'll be asked for your bank details. In this case you will be used to help steal money from people whose

bank account details have been stolen by the cyber criminals. The money will be transferred directly to your account, and you will then be asked to forward the money via Western Union. You will become a 'money mule', and when the police investigate the theft, you will be seen as an accomplice. Although this is often referred to as a scam, it is different from the others in that the 'money mule' also stands to gain, albeit by unwittingly committing a crime.

Facebook / Hotmail: Criminals obtain the details to access an account on Facebook, Hotmail, or similar. They then change the login credentials so that the real user can no longer access the account, and send a message to all contacts saying that the account holder is on holiday (London seems to be a popular choice) and has been robbed just before coming home. They still have flight tickets but need between $500 and $1,000 for the hotel.

Compensation: This is quite a recent ruse, and originates from the Nigerian scam. The email claims that a fund has been set up to compensate victims of the Nigerian scam, and that your address is listed as among those possibly affected. You are offered compensation (often around $1 million) but naturally, as in the original scam, you will need to pay an advance sum of around $1,000.

The mistake: This has become very popular in recent months, perhaps fueled by the financial crisis and the difficulty people are having in selling goods or houses. Contact is made with someone who has published a classified ad selling a house, car, etc. With great enthusiasm, the scammers agree to buy whatever it is and quickly send a check, but for the wrong amount (always more than the agreed sum). The seller will be asked to return the difference. The check will bounce, the house remains unsold and the victim will lose any money transferred.

What should I do if I'm targeted by one of these scams?

- It's normal that if you're not aware of these types of criminal ploys, you might think that you have won a lottery or found true love on the Internet. So here are some practical tips that will help keep you out of harm's way:
- Have a good antivirus installed that can detect spam. Many of these messages will be detected and classified as junk mail by most security solutions. This will help you be wary of the content of any such messages.
- Use your common sense. This is always your best ally against this kind of fraud. Nobody gives away something for nothing, and love at first sight on the Internet is

a very remote possibility. As a general rule, you should be highly suspicious of these kinds of contacts from the outset.

- The Internet is a fantastic tool for a great many things, but if you really want to sell something, it's better to have the buyer standing right in front of you. So even if you make contact across the Web, it's better to make the transaction in the 'real world', to verify the genuine intentions of potential buyers.