

Identity Theft Offline -- So Many Possibilities

Article by: Alexandra Gamanenko

Chris Simpson, head of Scotland Yard's computer crime unit was unpleasantly surprised to learn how easy it is to cheat anybody out of his or her personal info -- by means of a fake survey.

This survey wasn't a scam; in fact, it was an experiment. It was carried out in March for the Information Security show (April 26-28). The results showed that most people casually give out their personal info.

Market researchers questioned 200 people on London streets in a bogus survey on theater-going habits. 92% of those who took part disproved the common stereotype of British as reserved people. They readily gave out personal data, including first school and birth dates, mothers' maiden names, names of pets -- valuable info for, say, cracking passwords. During the survey many people volunteered such key details as name, address and postcode.

The chance to win free tickets was enough for these people to reveal almost everything one might need to impersonate them. By the end of the survey, the fake researchers had everything they needed to take out credit cards in their name and even open bank accounts. These 200 people were lucky -- the survey was just a trick. But what if it hadn't been?

Instead of laughing at naive and unwary Londoners, let's think whether we all are careful enough with such personal data. Aren't we sometimes give away information without a clear idea how it will be used -- and by whom?

Much cautioned about identity theft and phishing in the Internet, we tend to relax when speaking in person. Most of us will never click links in spam or open attachments if we don't know who sent the email. We don't trust letters asking us for sensitive information. We are getting wiser.

We have heard about identity theft plenty of times. We know that good deal of identity theft occurs offline. But all the same, some of us are still far from having good habits such as shredding personal correspondence before throwing it into the trash, or not having the same easy-to-guess password just for everything.

The odds of identity theft online partly depend on such factors as what anti-virus and anti-spy software is installed on a PC and how often it is updated. Software vendors try to develop and provide effective means of defense against information-stealing malware. Of course, much depends on whether the user is careful enough to avoid a phishing scam, and even on what sites he visits -- one can easily pick malware while visiting certain websites.

As for plain looking over your shoulder when you are writing something down, digging out papers from your trash or picking some valuable info from a casual talk -- nothing will help you if you carelessly scatter information about yourself.

Alexandra Gamanenko currently works at Raytown Corporation, LLC -- an independent software developing company that provides solutions for preventing identity theft.

The company's R&D department created an innovative technology, which capable of blocking information-stealing malware. The company's anti-keylogging software disables the very processes of information capturing -- keylogging, screenshots, etc.

Learn more -- visit the company's website <http://www.anti-keyloggers.com>