Anti-phishing technology

The number of Internet users is constantly increasing, and new online services and e-shops are appearing every day, which means that more and more information, including private data, is being transferred via the web. As a result, there are more and more people trying to steal this sensitive data. One popular technique used by the criminals is phishing – a combination of social engineering and traditional digital data theft.

How does data theft happen?

The cybercriminals are primarily after bank card details and authorization data for financial service websites. These include e-banking services, payment systems and other resources where access to a victim's data makes it easy to earn money. Often the intruders try to steal logins and passwords to social networks and similar services. This information does not directly profit the thieves, but makes it possible to send malicious messages from the victim's accounts.

Recently this mass distribution of phishing messages via email and social networks has become increasingly commonplace, making it one of the preferred tools for stealing users' personal data. In these messages the intruder impersonates a representative of a bank or payment system asking the victim to send personal data, or visit an "official" website. However, it's not that easy to spot a fake message: the intruders copy the format and style of official letters and use perfectly plausible excuses, such as an update being made to a site's authorization system.

If a user clicks the malicious link, things can unfold in one of several ways. Sometimes the perpetrators create an exact copy of the resource that allegedly sent the letter, and host the page on a domain with an almost identical name. The user is invited to go through an authorization process on the forged website and data is stolen as soon as it is entered. The procedure takes a couple of seconds. After that the victim is redirected to the legitimate website that was mimicked by the phishers. As a result, the victim may not know he has been on a malicious site and that his computer is now infected with a Trojan. In future, the malicious program could alter the bank's original page to intercept any information entered by the victim – including credit card numbers or passwords.

Staying out of the phishing net

More than 50% of users are not confident they could recognize a phishing letter or web page by themselves, according to a survey conducted by O+K Research in May 2012. Statistics about the number of thefts and infections suggest that for the vast majority it is almost impossible to distinguish between real and fake web pages. The knack of recognizing a phishing message is definitely useful, but if you need real protection from the perpetrators, it is better to make use of dedicated anti-phishing technologies.

Kaspersky Lab products for home users, such as Kaspersky Anti-Virus, Kaspersky Internet Security and Kaspersky PURE, include a special module which checks links and flags up phishing sites. It detects malicious websites and any links to them in real time, regardless of the source – the module analyses emails and messages shared on social networks as well as web pages. To check those sites, the products use heuristic analysis as well as up-to-the-minute data from the cloud security system Kaspersky Security Network. This interaction with a cloud-based service ensures that the anti-phishing modules always receive the latest updates and information about infected sites.

Mobile phishing

Mobile phishing, which is increasingly popular, also deserves a mention. According to research by Harris Interactive, 23% of tablet users and 19% of smartphone owners access online banking services from their devices. Moreover, many banks implement double authentication and send SMS messages to their customers in order to verify any financial operation. All this data is of great interest to criminals.

Therefore, Kaspersky Lab mobile solutions (Kaspersky Mobile Security and Kaspersky Tablet Security) for Android-based devices offer protection against malicious and phishing websites, just as users would expect from desktop products.

Conclusions

To steal data, including financial data, from users, the perpetrators make active use of fake letters from banks and payment systems, infected web pages and standard malware. Kaspersky Lab products for home users check all potentially dangerous links and web pages with the help of heuristic analysis and the Kaspersky Security Network database. Anti-phishing technologies provide efficient security, but the best results require a combination of other protection methods, including antivirus security, an anti-spam module, anti-exploit technology etc.