Secure web surfing with Kaspersky Lab Advanced Anti-phishing technology

The Internet is already far more than just a computer network intended for data exchange. It has become part of life for many users worldwide. More and more people consider the Internet as a primary source of information and means of communication. They use it for work, entertainment, online shopping, managing their personal finances, etc. However, just as in real life, the virtual environment is a fertile ground for lots of scammers who seek to earn dishonest payments through various fraudulent schemes.

Phishing is a type of criminal activity which is especially popular with cyber fraudsters because it allows them to easily access users' valuable information. It helps them to steal social networking accounts and credentials for e-banking, e-stores, online gaming accounts and other sites which may contain the user's personal details.

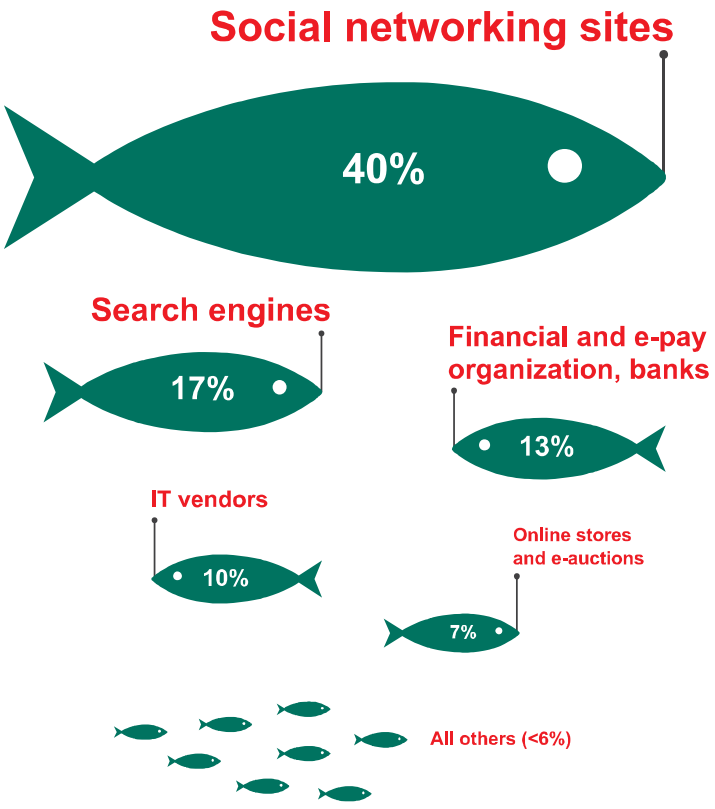

Figure 1. Targets of phishing attacks (source: Kaspersky Security Network, January 2013)

Technically, most phishing attacks are rather primitive: as a rule, the phishers create a copy of a web page which is often used by the victim, place it on a domain similar to the original and try different means (usually via messages in email, social networking sites or IM such as Skype) to lure the user to visit it.

Figure 2. A phishing site imitating the interface of a popular e-pay system

To lure users to the fake site, criminals actively deploy social engineering and psychological techniques. Usually, attackers try to generate interest by offering users pseudo-secret or sensational information, promising a large cash prize or even threatening imaginary fines or other sanctions from an official organization. The chosen scenario largely depends on the attackers' ultimate aim.

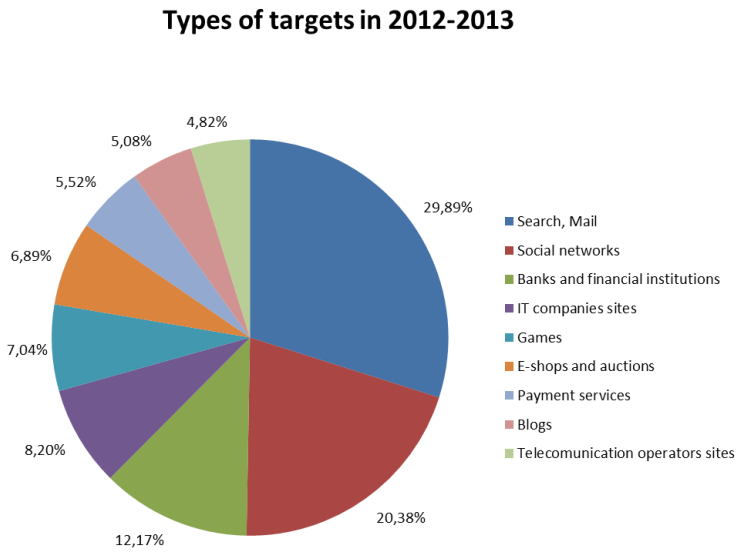

Figure 3. Types of site imitated most often by cybercriminals (source: Kaspersky Security Network, May 2012 – April 2013)

In other words, the success of a phishing attack often depends on the plausibility of the fraudster's scheme rather than on the sophistication of the malware used. This creates a situation in which phishing, unlike a conventional malicious attack, is very hard to detect with antivirus software.

At the same time the organization of a phishing attack often requires no special computing skills. This detail in particular attracts more and more criminals to this kind of illegal activity. As a result, phishing is no longer just one of many types of email spam – it has become a large-scale threat faced by users in email, text messages, IM and on social networking sites.

How the right anti-phishing technology should work

The Anti-phishing module implemented in Kaspersky Internet Security – a solution for home users – provides effective protection against phishing schemes using three basic protective components:

- Web antivirus
- Kaspersky Security Network;
- Heuristic analyzer

Depending on the nature of the link, any or all of these components may be involved in the analysis. For example, when users open a potentially dangerous link, web antivirus analyzes it for malicious activity. This may be accomplished by checking against a database of known phishing links, or with the help of Kaspersky Security Network or by scanning with heuristic module. If any of these three modules recognize it as a phishing link, it is blocked immediately.

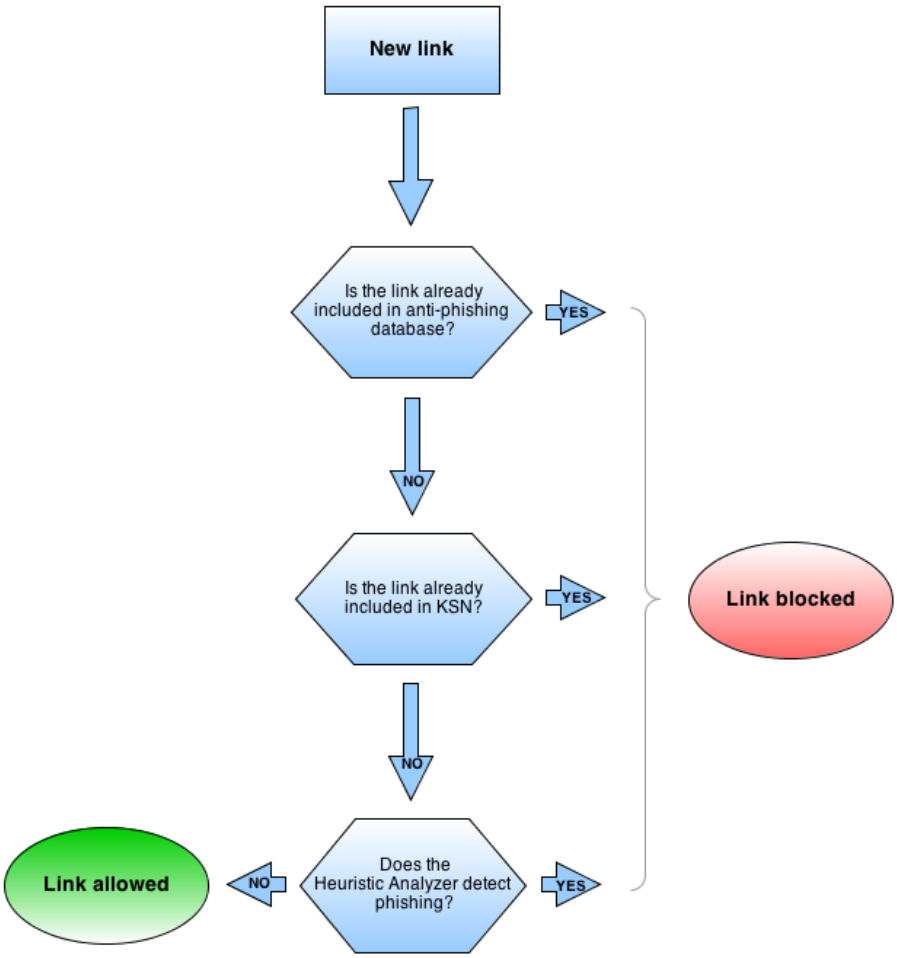

Figure 4. The process of detecting a phishing page using web antivirus

Kaspersky Lab's anti-phishing database is a constantly updated database accumulating information about all phishing pages which have been detected by the company's experts and its partners. This database is the first stage of verifying a link. If the anti-phishing database does not contain the link under review, the Kaspersky Lab product checks this link against the cloud-based Kaspersky Security Network.

Kaspersky Security Network is able to quickly warn users about an emerging phishing threat. When new malicious code is detected on the computer of any Kaspersky Security Network user, information about this threat is made available to all other users of the service within 15-30 seconds of the detection. In addition, Kaspersky Security Network has a unique base of SSL certificates corresponding to domain names, an extra criterion for determining the safety of a site.

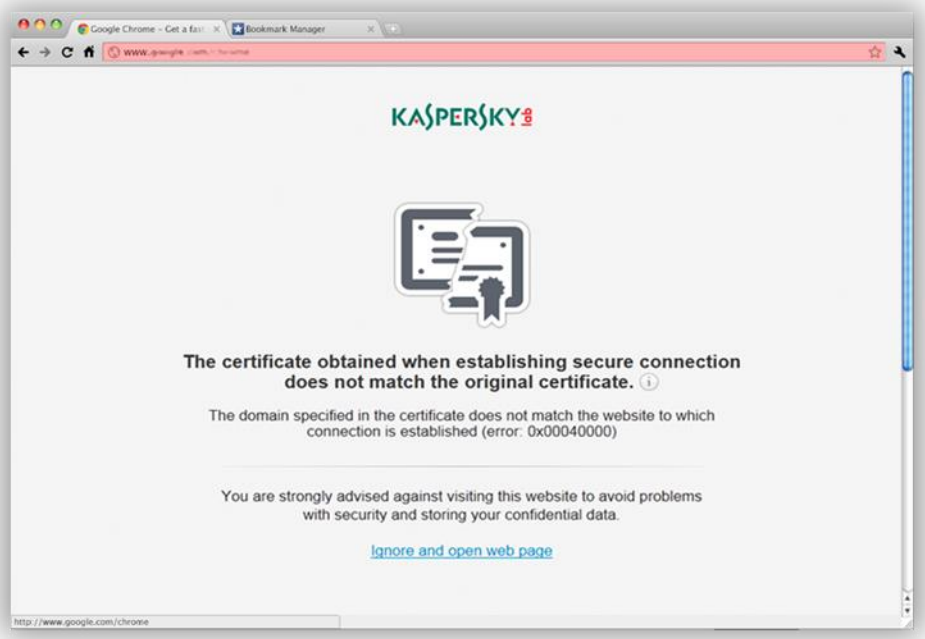

Figure 5. Warning page alerting the user to a potentially fake certificate provided by a website

However, Kaspersky Security Network databases may not contain the suspicious link. This can happen if the cybercriminals have just launched the campaign and to date only a small number of users have seen the new phishing page. In this case, the link and the page to which it leads are additionally checked against a regularly updated set of features by an integrated heuristic module. Elements of the HTML code of the page and its address are selected. The heuristic module looks for evidence of suspicious vocabulary, input forms and unreadable sequences of symbols. If the heuristic module identifies the analyzed page as a phishing site, it immediately blocks it and sends the information about it to Kaspersky Security Network. 69.41% of all links sent to Kaspersky Lab anti-phishing databases between May 2012 and the end of April 2013 were detected using heuristic methods.

The advantages of cloud reputation technologies

The best protection against phishing is to avoid following suspicious links. But how can we say which links are malicious and which are not? Kaspersky Security Network also includes Kaspersky Lab's extensive knowledge base about the reputation of files, Internet resources and software. It enables users to find out which links on any page lead to fake or malicious pages without actually clicking on these links.

This technology is indispensable for combating phishing, since attackers use all sorts of tricks to give credibility to their links: they publish them in the newsfeeds of compromised accounts on social networks, use various illegal SEO schemes to push fake pages to the top of search engine results for popular keywords, etc. The Kaspersky URL Advisor reputation service can alert users to the potential consequences of following these links: if there are phishing links among search results, Kaspersky Internet Security will mark them with a special icon right there on the search query results page.

The reputations on which these alerts are based are extremely accurate, because Kaspersky Lab uses several sources of data in its calculations:

1. product users who submit categorization requests for specific web resources;
2. information from domain registrars on domain names registered in all top-level domains, including "com", "net", "info" etc.;

3. search engine results for sets of popular keywords, which are analyzed in order to identify the phishing resources which come up in response to various search queries.

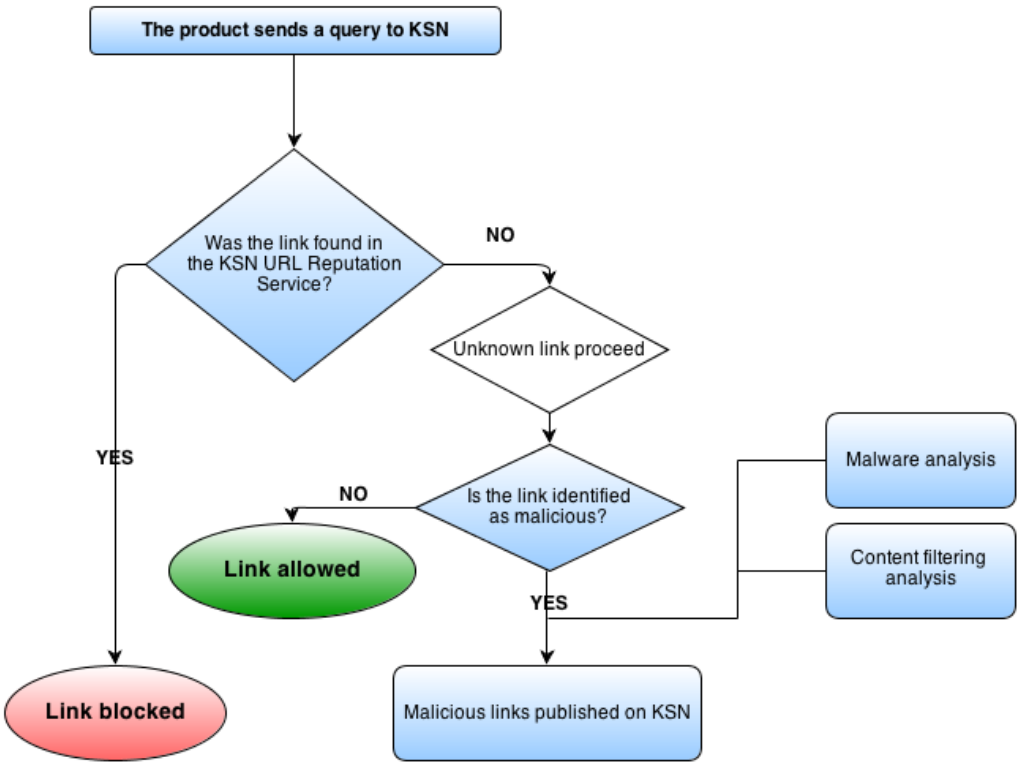

Figure 6. How Kaspersky Lab products recognize phishing links

A web experience protected by Kaspersky Lab Anti-phishing technologies

Kaspersky Internet Security combines advanced anti-malware technologies with a range of anti-phishing mechanisms, which offer the following advantages:

- **Comprehensive approach**: the same link undergoes up to three different checks before being classified as secure;
- **Minimal response time**: the Kaspersky Security Network cloud protects users against even the most recent phishing campaigns;
- **Proactive protection**: Kaspersky Lab's heuristic anti-phishing module can identify a phishing web page even if no other Kaspersky Security Network user has come across it before;
- **Early warning**: The Kaspersky URL Advisor reputation service identifies phishing links in the browser without having to follow any dubious links;
- **Few false positives**: a proven technology for checking the authenticity of links enables Kaspersky Internet Security to distinguish fake pages from real ones effectively;
- **Recognition by experts**: the effectiveness of the anti-phishing technologies in the Kaspersky Internet Security product family **has been confirmed** by independent experts.

The protection that Kaspersky Internet Security offers with its advanced anti-phishing technologies amounts to more than a mere set of mechanisms for handling specific threats. This is an integrated solution that makes the online experience of users secure, no matter how sophisticated the fraudulent schemes devised by cybercriminals might be.