KASPERSKY lab

Secure Web Surfing With Kaspersky Lab Advanced Anti-Phishing Technology

Identity, or the digital representation of a person, holds value to others, as well as its owner. Certain cybercriminals hunt for user credentials that confirm a person's authenticity, in order to resell them to other fraudsters, or use the credentials themselves. Some of the common uses for identity data include stealing money from a user's bank accounts or sending malware to friends from a user's contact list on a social network. One of the most widespread methods for stealing credentials is phishing.

Most phishing attacks involve creating a copy of a web page, which is often used by the victim. The copy can be placed on a domain similar to the original and various means can be used to lure the user to visit it and enter their credentials.

To lure users to the fake site, criminals actively deploy social engineering and psychological techniques. Usually, attackers try to generate interest by offering users (usually via messages in email, social networking sites or IM such as Skype) pseudo-secret or sensational information, promising a large cash prize or even threatening imaginary fines or other sanctions from an official organization.

Fraudsters employ hundreds of tricks to conceal their efforts to steal credentials. Some of them make it almost impossible to tell a fake site from the original. Apart from the common means of URL concealment (replacing unreserved characters with percent-coded values, URL-forwarding, or using short aliasing services or IP-addresses instead of the normal names), they use browser specific visual decoys — graphics, depicting the legitimate web address, placed over the address bar with the fake one, or using browser scripting languages. They also can imitate SSL padlock or HTTPS encrypted connection signs this way.

According to statistic from the Kaspersky Security Network, in the first half of 2015 alone, the Kaspersky Lab anti-phishing system was triggered 80 million times on the computers of Kaspersky Lab users.

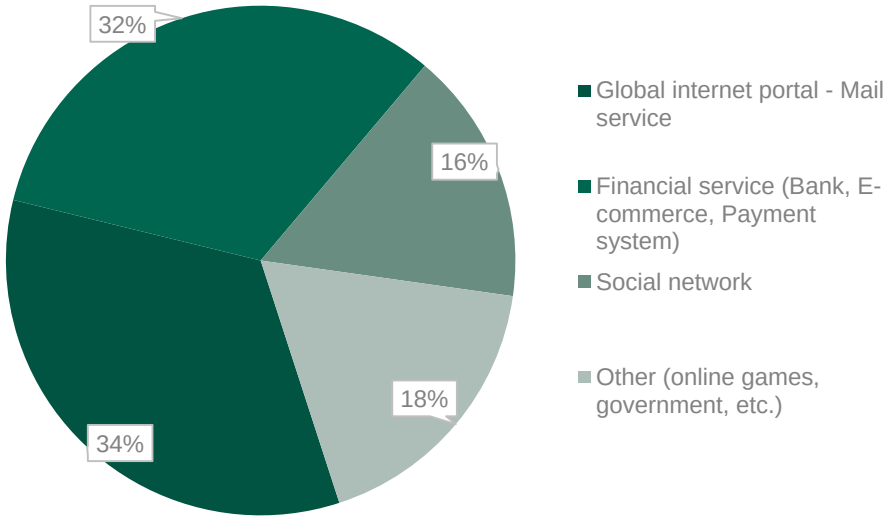

Figure 1. Targets of phishing attacks in the first half of 2015

How Kaspersky Lab's anti-phishing technology works

The anti-phishing module implemented in Kaspersky Lab's solutions provides effective protection against phishing schemes combining three methods of detection:

- Sites are checked by the product's local anti-phishing databases on the user's device;
- Sites are checked by cloud databases located on the Kaspersky Security Network;
- Heuristic analysis (helps to recognize a phishing webpage even if it's not yet featured in these databases).

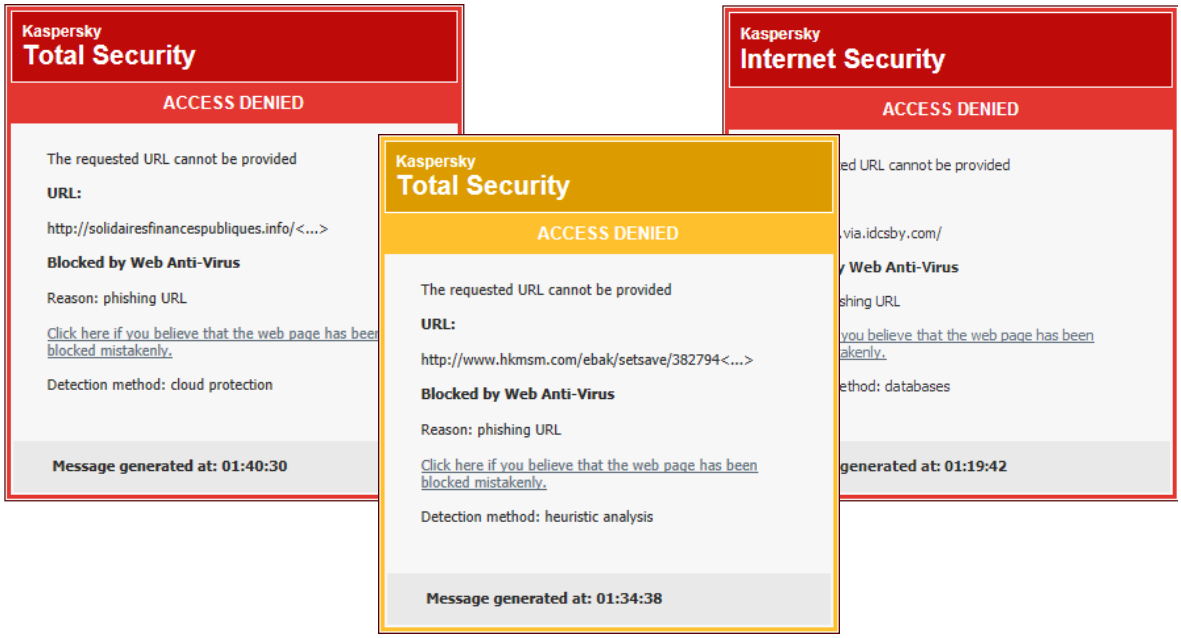

Figure 2. Phishing sites are blocked by Kaspersky Lab products using different methods

Databases check

Kaspersky Lab maintains a vast, constantly updated, database of phishing sites. It accumulates information about all phishing pages received from a number of partners as well as those detected by Kaspersky Lab's technologies. Bases that contain harmful URLs are regularly sent to Kaspersky Lab's solutions, as well as the cloud database (Kaspersky Security Network), which holds the most full and accurate collection of these. When a new malicious URL is detected on the computer, information about this threat is made available from the cloud database within 15-30 seconds of detection. In addition, the Kaspersky Security Network has a unique base of SSL certificates corresponding to domain names, an extra criterion for determining the safety of a site.

However, if the cybercriminals have just launched their latest campaign and only a small number of users have seen the new phishing page to date, the link may not yet be in the databases. In this case, the heuristic module comes into use.

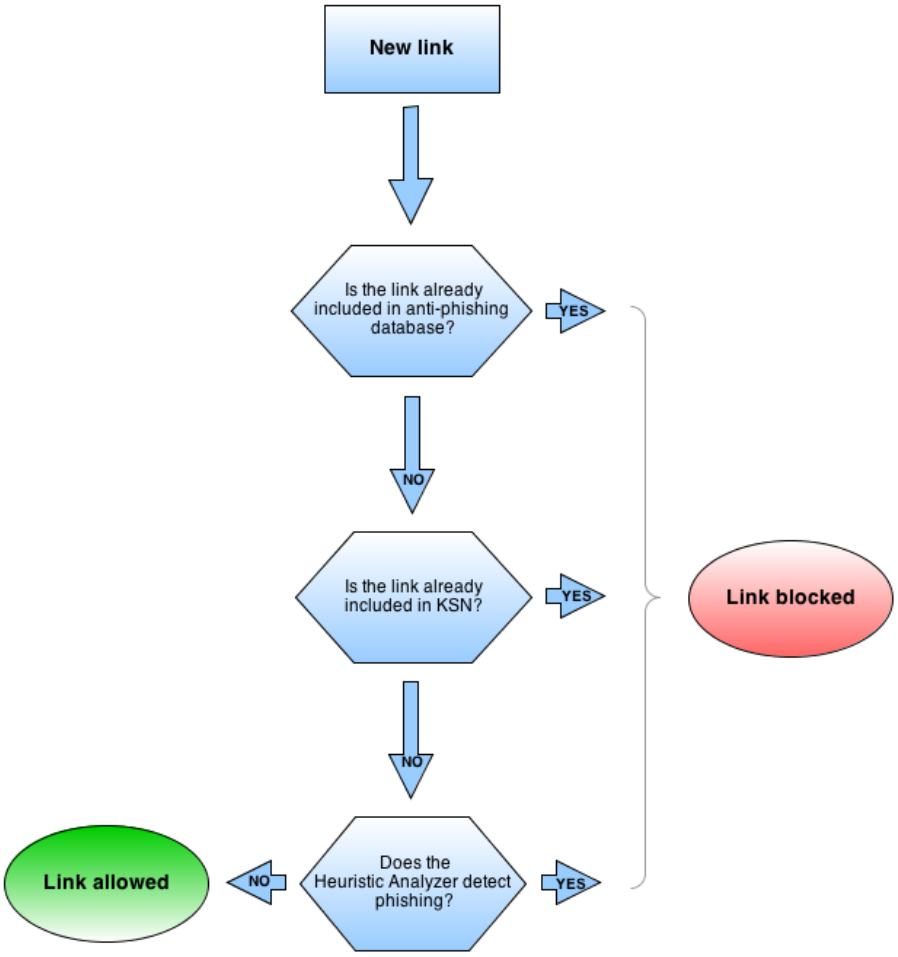

Figure 3. The process of detecting a phishing page using web antivirus

Heuristic detection

The heuristics module is a user's last line of defense against a phishing attempt. It is a highly effective system that allows Kaspersky Lab to give a reliable verdict about whether a site encountered by the user is a phishing one or not, even if it is not listed in the local or cloud databases. According to Kaspersky Lab's statistics, almost 50% of phishing detections are made by this system.

First of all, this is not just a checking machine that looks for the predetermined attributes that can evidence a fake site (although, if it finds one of those attributes, it definitely will alert the user). Modern sophisticated phishing technologies allow cybercriminals to conceal their handiwork, leaving no "definite evidence". However, some indirect indicators still can be found.

Take, for example, the use of a data Uniform Resource Identifier (URI) scheme. This is a legal way to include data in-line in web pages. However, this method can be used to add phishing content to a legal page. Another example is cross site scripting, or attempting to use external scripting code: this can be an indication of fraudulent intent or just the consequences of the programmer's laziness (and this is not rare even in banks and other serious organizations). Anti-phishing modules look at dozens of phishing symptoms, compare them with other indications (domain names, frame usage, input encryption usage, and hundreds more), and bases its verdict on this indirect evidence. It can even "look into" a picture and analyze what is written on it. In isolation each of these attributes is not necessarily evidence of a malicious site, but their combination may be. The effectiveness of the heuristics system hinges on those indications and their combinations.

The heuristics module is an intelligence system that analyses and classifies those indications, based on the knowledge of known modern phishers' methods and the vast Kaspersky Lab database of already detected phishing sites.

If the heuristics engine shows that a site may be a phishing one, but cannot guarantee it, it may send data to Kaspersky Lab's cloud infrastructure, which has much more resources to complete an analysis with its own, more powerful, heuristics engine. This helps to save the resources of the user's computer and brings a precise verdict in a matter of seconds. If the heuristic module identifies the analyzed page as a phishing site, it immediately blocks it and sends the information about it to the Kaspersky Security Network to prevent other users from visiting it.

URL Advisor reputation service

The same database of anti-phishing sites also strengthen the functionality of yet another technology – information from this database, supplemented with data about other malicious sites, is being used by the Kaspersky URL Advisor reputation service. When someone uses one of the popular search engines, the URL Advisor checks the links that were found and marks them with green (if they can be trusted) or red (if they lead to a phishing or malicious site).

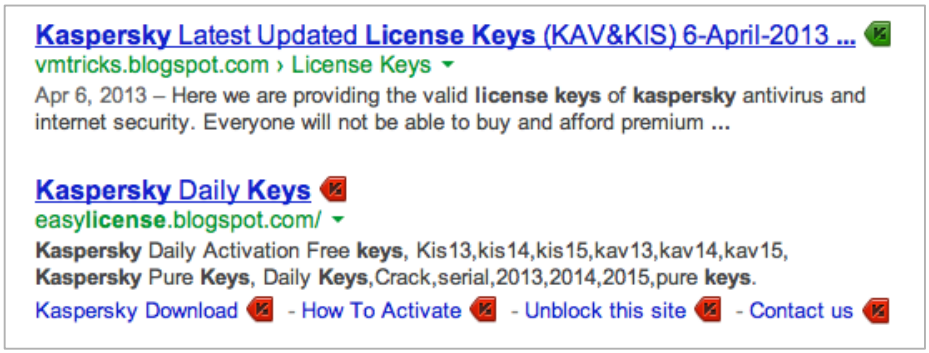

Figure 4. Malicious links, marked with the red icon by Kaspersky Lab's product

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.

This feature works for Windows and Mac OS X only.

Benefits of Kaspersky Lab Anti-phishing Technologies

- Comprehensive approach: the same link undergoes up to three different checks before being classified as secure;
- Minimal response time: Kaspersky Lab's anti-phishing technologies protect 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 it is not yet added to the database;
- Early warning: The Kaspersky URL Advisor reputation service identifies phishing links in the browser without having to follow any dubious links.

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.

Availability

The above-described anti-phishing technology is integrated into the following products:

For home users

- Kaspersky Anti-Virus
- Kaspersky Internet Security
- Kaspersky Internet Security – Multi-Device
- Kaspersky Internet Security for Mac
- Kaspersky Internet Security for Android
- Kaspersky Total Security – Multi-Device
- Kaspersky Safe Browser for iOS
- Kaspersky Safe Browser for Windows Phone

For business

- Kaspersky Endpoint Security for Business
- Kaspersky Security for Linux Mail Server
- Kaspersky Small Office Security