Protecting your money online with Safe Money technology

It’s all about money

The modern Internet environment is unimaginable without online payments. According to the findings of a survey conducted by B2B International in 2013, 98% of Internet users regularly bank or shop online.

Unfortunately, the explosion in online payments has been accompanied by an equally rapid surge in Internet fraud. There are various methods of swindling people out of their cash, but perhaps the most common technique employed by fraudsters is to trick the online payment system into believing that they are the real account owners. Once that is accomplished, the imposters can perform any transactions they please with victim's funds.

How fraudsters get hold of personal data

The fraudster enters the owner's name (or credit card number, registered alias, etc.) and the correct password (pin code, code word, etc.). That is enough to convince the payment system that this user is genuine.

But how do cybercriminals get this data in the first place? Various tools and techniques can be used, but the most common method is by means of a Trojan. Once a computer is infected with a Trojan, the fraudsters are free to steal almost any information they please. Cybercriminals can obtain confidential data using one of these methods:

- By introducing malicious code which reads the memory performs or other unsanctioned operations in the browser to collect login and password details, or substitute the content (amount, bank account, etc.) of banking transactions
- By using phishing webpages that imitate the real website to intercept private data
- By taking screenshots
- By logging keyboard and mouse inputs
- By intercepting online traffic through a variety of techniques aimed at gathering input user data

In the majority of cases, users are unaware that their personal data has been compromised until they check their bank account.

The B2B International study indicates that 59% of Internet users are worried about online banking fraud. Where can users find reliable protection?

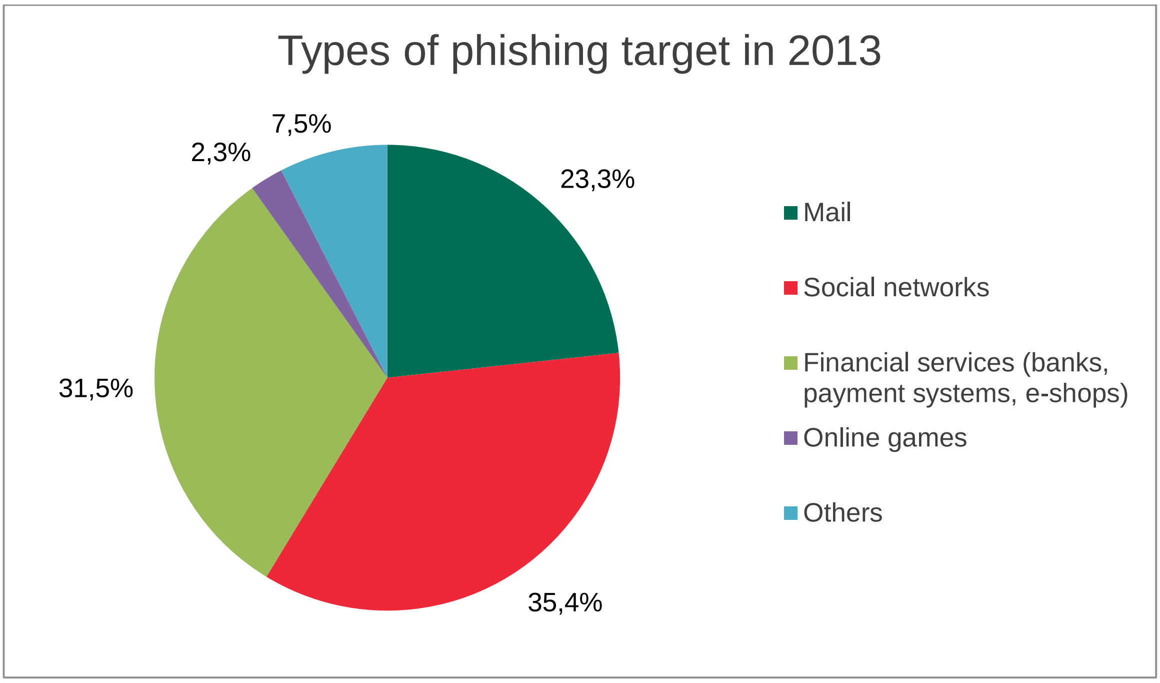

Figure 1. The distribution of the main phishing targets detected by Kaspersky Lab's anti-phishing component, which is activated every time a user attempts to click on a phishing link, regardless of whether the link is in a spam email or on a web page. The diagram shows that about one third of all phishing attacks are against financial and e-pay organizations, banks, online stores and e-auctions. Overall in 2013 the number of Internet users who faced phishing attacks around the world exceeds 396 million. Source: Kaspersky Security Network.

Traditional antimalware tools

Traditional antimalware programs offer a suite of tools that significantly lower the risk of being infected by a Trojan. Technologies such as anti-phishing, web antivirus and file antivirus prevent the introduction of malicious code at various stages. However, fraudsters are becoming increasingly inventive and have released many modifications of malware able to bypass traditional protection methods.

It is crucial for users to have a comprehensive multi-level security solution. There must be tight controls at every stage at which malware could penetrate the computer or attempt to perform any action on it. On top of that, all the security levels need to be closely integrated.

That is exactly why Kaspersky Lab's products with integrated Safe Money technology not only combine all the best traditional antimalware tools but also offer a new range of technologies specially developed to protect your computer during online payments and transactions.

Safe Money technology

Kaspersky Lab's Safe Money online protection technology consists of three key components:

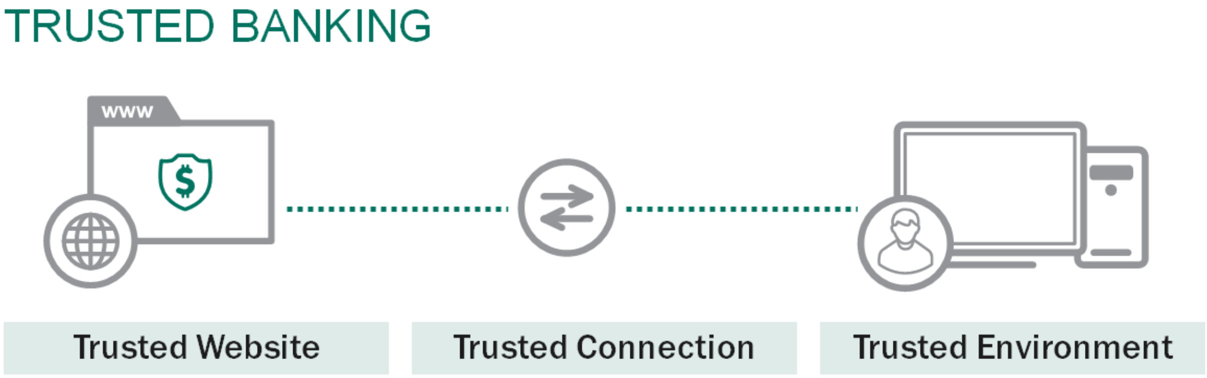

Figure 2. How Kaspersky Lab's Safe Money technology works

Trusted sites

The user goes to the website of their bank or online payment system however they choose – via an email or browser link, by typing the address in the URL, or from the list of sites in the Kaspersky product window compiled by the user in advance.

Before the site loads, its URL is automatically checked against the database of trusted addresses maintained by Kaspersky Lab or specified by the user. If a match is found, the browser switches to Safe Money mode, protecting itself from injections of suspicious code and providing special additional security for all online operations. If there is no match in the database, the website will be inspected by a heuristic analyzer designed to spot phishing scams. If the heuristic engine delivers a verdict that website's content is unsafe, the attempted transaction will be blocked. This guarantees that the user opens the genuine site of the bank or payment system, and not a fake site hosted by fraudsters.

Trusted connection

It is also important to check the authenticity of the server that the user connects to when banking or paying online. Kaspersky Lab's digital certificate verification service can be used to establish beyond doubt that the site is authentic. If the certificate cannot be verified Kaspersky Lab's product uses Safe Money technology to block access to the online payment site. To accelerate this working process, every time a certificate is verified, Safe Money stores the verdict locally for some time. So when the browser switches to Safe Money mode while connecting to a site the first thing it does is check whether there is a verdict in the local cache. It only queries Kaspersky Security Network if no such verdict is found.

Trusted environment[i]

Before every online purchase or payment, Safe Money checks the security of the computer on which the transaction is to be made. This includes a scan for OS vulnerabilities. The high speed of the operation is the result of scanning for vulnerabilities of a certain type known to compromise the security of online banking (for example, vulnerabilities that can be exploited to gain increased privileges). The presence of vulnerabilities renders banking transactions unsafe, and the user is prompted to remove them in automatic mode using Windows Update.

Having launched the browser in Safe Money mode, the user is sure that all personal data is protected against theft or modification by fraudsters. Safe Money achieves this by blocking any attempts to introduce malicious code via the browser, read the memory, display fake windows, and protects plugins and profiles from illegal deactivation or change. It also blocks any attempt to take screenshots, including full desktop area screen capture made with the use of application programming interfaces such as GDI, DirectX or OpenGL.

In addition, when the web browser is working in Safe Money mode, untrusted applications have no access to the clipboard, where sensitive data could be stored briefly during copy/paste operations. Therefore, no third-party software will get access to the temporary data buffer in attempt to steal passwords or logins.

At the same time, two options are available to prevent confidential data input from a hardware keyboard from being intercepted:

- *Virtual Keyboard*[ii], which is displayed on the user's screen and controlled via the mouse.
- *Secure Keyboard*, a feature that uses a special driver to protect data input from a hardware keyboard.

Another important feature of Safe Money is its extra protection of the browser in Safe Money mode. It constantly scans the protected browser’s address space in search of any unexpected, untrusted modules that potentially could be loaded by some rootkits. If this kind of module is found the user is alerted by a warning that opens on a new webpage.

When the payment transaction via Safe Money is complete, the user is automatically redirected to a normal browser window to finish the process or continue shopping in the online store. Safe Money is fully compatible with all recent versions of the most popular web browsers: Internet Explorer, Apple Safari, Google Chrome and Mozilla Firefox.

Availability

Safe Money technology for secure online transactions is integrated into the following products:

- Kaspersky Internet Security
- Kaspersky Internet Security for Mac
- Kaspersky Internet Security – Multi-Device

- Kaspersky Total Security – Multi-Device
- Kaspersky Small Office Security

Benefits

Safe Money works for any site that requires identification and interfaces with payment systems via the HTTPS protocol. What's more, the user can independently add any bank, payment system or online store to the list of trusted sites.

The main advantages of Safe Money are:

- The protective mechanisms operate automatically – at the right time and in the right place.
- The modified browser window lets the user see that the protective mechanism is active and working.
- Safe Money does not require any pre-configuration to activate the protective mechanism (or only minimal configuration and a one-time confirmation to use Safe Money for a particular website). The flexible settings always allow Safe Money mode to be enabled or disabled for various sites, depending on the content.
- Quick launch of Safe Money mode is also available for sites selected in advance by the user via the special shortcut on the desktop (for Windows OS). This creates an accessible and secure point of entry to these sites.
- Native integration with advanced anti-malware solution provides multi-layered protection against most fraud techniques.

Safe Money technology developed by Kaspersky Lab ensures maximum protection for online banking and payment transactions. This is achieved through Trusted Sites, Trusted Connection and Trusted Environment[i], which provide deep-level control at all stages of the online payment process. These innovative technologies guarantee maximum security and protection not only for online banking transactions but for all other Internet activities, too.

Quality proven by industry experts

Safe Money technology has taken leading positions in independent tests:

- Matousec Online Payments Threats, 1 part
- Matousec Online Payments Threats, 2 part
- AV-TEST Innovation Award 2013
- MRG Effitas Online Banking/Browser Security 2013
- MRG Effitas Online Banking/Browser Security 2014

[i] Trusted environment is currently only available for Windows OS. It will be available in the next version of Kaspersky Internet Security for Mac

[ii] Virtual Keyboard is also available for Mac OS X