



## Protecting your bank account using Safe Money technology

It's all about money. The modern Internet environment is unimaginable without online payments. According to IDC, 2012 will see over a billion online purchases worth a total of more than \$1.2 trillion. Today, 60% of users regularly use the Internet for banking and buying online.

Unfortunately, the explosion in online payments has been accompanied by an equally rapid surge in Internet fraud. There exist 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 owner. Once that is accomplished, the imposters can perform any transactions they please with the 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 the user is genuine.

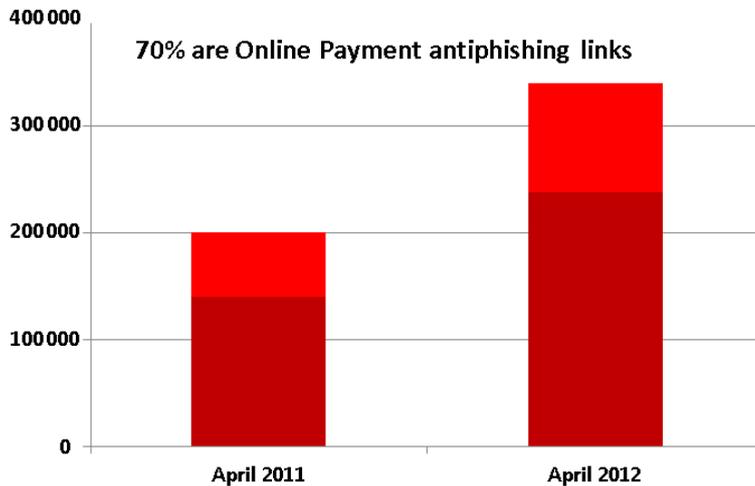
But how do cyber-criminals get this data in the first place? Various tools and techniques are used for this purpose, but the most common method is by means of a Trojan. Once a computer is infected with a Trojan, the fraudsters are free to steal almost any information they please. Computers can become infected in one of the following ways:

- Through the introduction of malicious code, reading the memory or other unsanctioned operations in the browser in order to collect login and password details, or substitute the content (amount, bank account, etc.) of banking transactions
- By displaying fake windows on the user's screen that imitate the real website to intercept private data
- By taking screenshots
- By logging keyboard and mouse strokes
- By intercepting online traffic through a variety of techniques all with the aim of gathering input user data

---

In the majority of cases, the user is unaware that their personal data has been compromised until they check their bank statement.

Nevertheless, online payments are a fact of modern life. According to eBay, online commerce accounts for 15% of global CAGR (compound annual growth rate). And recent data from Harris Interactive indicates that more than 60% of all Internet users consider theft of bank details to be the most serious online threat. Where can users find reliable protection?



The figure shows the growth in the number of anti-phishing links added to Kaspersky Lab's database. 70% of them are links to phishing payment systems. It is indicative that the number of phishing links detected by Kaspersky Internet Security increased by 100% in Q1 2012 against the previous quarter.

## Traditional anti-virus

Traditional anti-virus programs offer a suite of tools that significantly lower the risk of infection by a Trojan. Technologies such as anti-phishing, web anti-virus and file anti-virus 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 means of protection.

It is crucial that users have comprehensive and multi-level security. Every stage at which malware could penetrate the user's computer or attempt to perform any action on it must be tightly controlled. On top of that, all the security levels need to be closely integrated with each other.

For that very reason, the new Kaspersky Internet Security with integrated Safe Money technology not only combines all the best traditional anti-virus tools, but offers 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:

### 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 Internet Security 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, which provides special protection and extra security for all online operations. 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 Internet Security blocks access to the online payment site.

### Trusted environment

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 must ensure that all personal data is protected against theft or modification by fraudsters. Safe Money and Kaspersky Internet Security achieve this by blocking any attempts to introduce malicious code via the browser, read the memory, display fake windows, or take screenshots.

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

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

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.

## 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 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 Banking 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. This creates an accessible and secure point of entry to these sites.

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, which provide deep-level control at all stages of the online payment process. These innovative technologies, newly integrated in Kaspersky Internet Security 2013, guarantee maximum security and protection not only for online banking transactions, but for all other Internet activities, too.

---