KASPERSKY lab

KASPERSKY FRAUD PREVENTION FOR ENDPOINTS

www.kaspersky.com

KASPERSKY FRAUD PREVENTION

1. Ways of Attacking Online Banking

The prime motive behind cybercrime is making money, and today's sophisticated criminal gangs have a range of techniques to help them steal from online banks and financial services. Whether using malware to manipulate legitimate transactions and divert cash into their own accounts, or combining social engineering and phishing to gain access to accounts, cybercriminals have several ways of robbing users of online banking services.

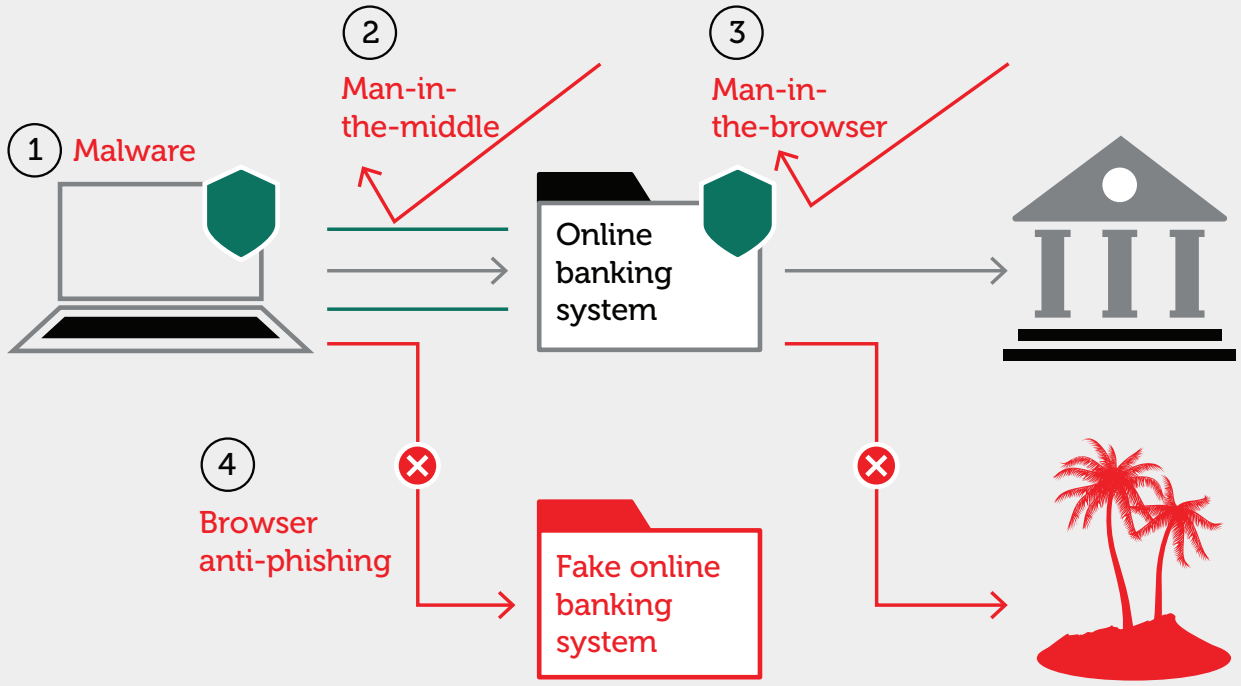
There are two main threats:

- **Account take over** – stealing a user's credentials and using them to take money from the account
- **Transaction tampering** – changing transaction details, or creating a new transaction on behalf of the customer

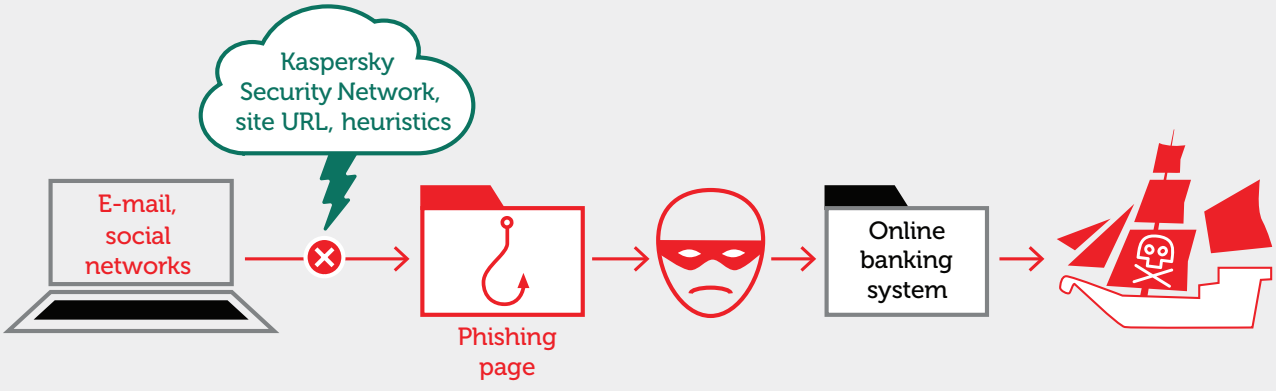
These cybercriminal objectives are generally achieved through a combination of techniques, including:

- Credentials theft
- Phishing
- Web page modification (web-injects)
- Form grabbing
- Keylogging
- Screenshotting
- Spoofing attacks
- Transaction tampering
- Man-in-the-middle (MITM) attacks
- Remote access
- Man-in-the-browser (MITB) attacks

2. Fraud Prevention in Action



2.1 Malware scan and removal



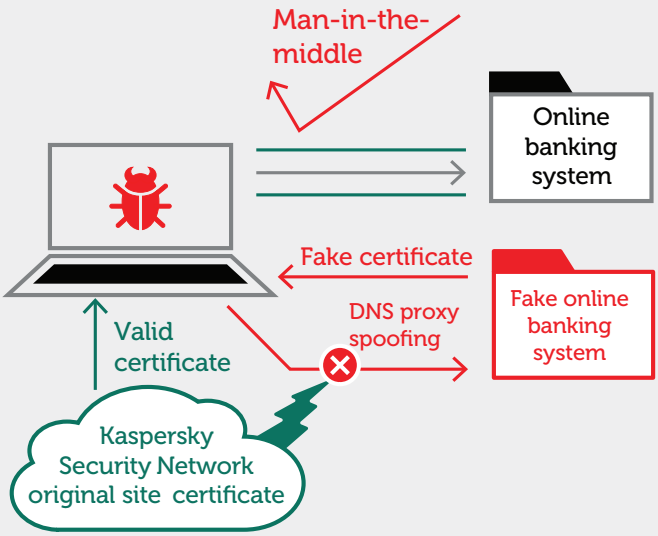
Even if there is already malware on a user's computer, Kaspersky Fraud Prevention can still protect online banking operations. As soon as it is installed, Kaspersky Fraud Prevention performs a system scan to find banking malware. Users are alerted to any problems and invited to delete the malicious file(s) and disinfect the machine. The solution runs an additional scan every time the protected banking browser starts up.

CASE STUDY

A large Russian bank was targeted by a piece of malware that automatically redirected its clients to a phishing page. Not only did this redirect trick users into handing their banking credentials over to cybercriminals, it also made it impossible for them to access the bank's real web site. Kaspersky Fraud Prevention successfully deleted the malware on clients' computers, ensuring they could bank online safely in future.

Kaspersky Fraud Prevention for Endpoints is compatible with all leading anti-malware software, and is designed purely to find banking malware. It should be used to complement, not replace, a traditional anti-malware solution.

2.2 Protecting Internet connections



Kaspersky Fraud Prevention doesn't just make sure that the computer is a safe environment for online banking, and that it is visiting a legitimate banking resource. It also ensures that no third party can interfere with the Internet channel between the bank and its clients.

Every time a user logs in to an online banking session, Kaspersky Fraud Prevention verifies the website's security certificate by comparing it with the reference certificate stored in the cloud-based Kaspersky Security Network. This check protects against man-in-the-middle attacks, and DNS and proxy spoofing.

If a suspicious certificate is detected, the system alerts the user.

2.3 Protection against browser threats

2.3.1 EXTERNAL BROWSER CONTROL ATTACKS

Kaspersky Fraud Prevention for Endpoints provides protection from browser control with messages to browser windows (so that third parties cannot gain remote access).

2.3.2 CODE INJECTION ATTACKS

Protection from the upload of untrusted modules into browser process, verifying DLL signature locally and in the cloud (KSN).

2.3.3 PROTECTION AGAINST SNAPSHOTS

Protection against snapshots includes:

- Protects against screenshotting techniques
- Protects the window currently opened in the protected browser

2.3.4 OS VULNERABILITIES SCAN

Dedicated updatable vulnerabilities database:

- Operating system only
- Kernel mode privileges escalation only

2.3.5 SECURE KEYBOARD

When using the protected browser, Kaspersky Fraud Prevention for Endpoints secures all entry fields. Kaspersky Fraud Prevention intercepts and processes all keystrokes through the KFP keyboard driver, thus preventing the interception of input data by malware. The Secure Keyboard can be used in Safe Browser and in regular browser windows.

2.3.6 CLIPBOARD PROTECTION

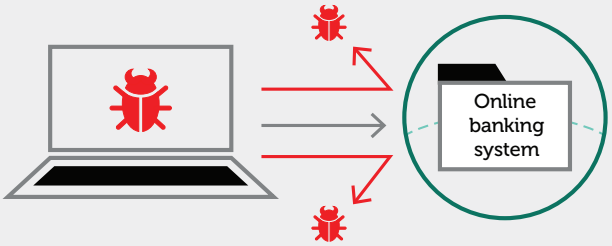
Restricts access to the clipboard for untrusted applications.

2.3.7 SELF-PROTECTION

Protects against modifications to Kaspersky Fraud Prevention for Endpoints:

- Windows registry keys
- Files
- Processes
- Threads

2.4 Browser anti-phishing



Kaspersky Lab's Anti-Phishing system combines heuristic and cloud-based technologies with traditional off-line databases to ensure that even emerging, previously unseen threats are blocked.

The rapidly-updated Cloud Anti-Phishing module contains masks of phishing URLs. New threats can be added within seconds of their detection, protecting your clients' computers against phishing sites that are not yet included in local databases. Whenever the user encounters a URL that is not in the local base, the system automatically checks it in the cloud.

The heuristic web component of the anti-phishing system is triggered when the user clicks a link to a phishing web page that is not yet included in Kaspersky Lab's databases.

In addition, a comprehensive off-line anti-phishing database, stored on users' devices, contains all the most widespread masks of phishing URLs.

3. Kaspersky Fraud Prevention Console

For easy management, the Kaspersky Fraud Prevention for Endpoints solution uses a single console that provides deeper and broader contextual and correlated information about the user, the user's device, and the session.

3.1 Reporting dashboard

The console collects information from Kaspersky Fraud Prevention for Endpoints about the user's device, sessions and environment, as well as any attacks launched on the user's machine (phishing, MITB or MITM attacks, malware attacks).

3.2 Remote configuration

The console provides management capabilities that can change Kaspersky Fraud Prevention for Endpoints settings remotely.

3.3 Statistical feed

The console has an integration point, which makes it possible to send statistics to internal transaction monitoring systems, increasing the detection rate and decreasing the number of false positives.

4. Implementation Details

Integration usually comprises three steps:

1. Customizing the solution in accordance with the bank's requirements to create a custom-built online banking service. Kaspersky Lab's white-labelling approach makes it possible for a bank to create its own bespoke online user experience using its own logos, color schemes, typefaces and preferred layouts on the page. Desktop and system tray icons can also be customized as required.

2. Configuring integration with the bank's internal systems. Kaspersky Fraud Prevention for Endpoints makes it possible to retrieve details of the product version and status when connecting to an online bank. This information is retrieved by a dedicated script, as described in the documentation. We recommend three main working scenarios, but every bank is free to choose how it uses the retrieved data.

3. The bank is then free to choose how to distribute the application among its clients, perhaps by checking whether Kaspersky Fraud Prevention is already running on users' machines and inviting them to download Kaspersky Fraud Prevention if necessary. Alternatively the bank can choose another way of distributing the application. To conserve the bank's computing resources, most of the application is stored on Kaspersky Lab's servers and is accessed using a 2MB downloader file handed to the bank during the implementation phase.

Typically, it takes about two weeks to complete the installation process. Kaspersky Lab's special implementation team is available throughout the installation process to help integrate the solution with the rest of the bank's network, and to resolve any problems that might emerge.

Contact us to find out more: KFP@kaspersky.com
http://www.kaspersky.com/business-security/fraud-prevention