Защита личных данных от киберкриминала с помощью технологии «Безопасные платежи»

Финансовые операции в Интернете стали неотъемлемой частью современной цифровой среды наряду с загрузкой медиафайлов и общением в социальных сетях. По всему миру 47% пользователей совершают покупки через Интернет, а 44% регулярно работают с системами онлайн-банкинга – такие данные были получены компанией Harris Interactive в рамках исследования, проведенного специально для «Лаборатории Касперского». Согласно прогнозам IDC в 2012 году будет совершено более 1 миллиарда онлайн-покупок на общую сумму более 1,2 триллиона долларов. В сложившихся условиях рост онлайн-платежей сопровождается ростом активности мошенников, а пользователи все чаще переживают за сохранность своих данных. Кража финансовой информации всерьез беспокоит 40% опрошенных, а 21% считают ее хищение наиболее серьезной угрозой.

Основная цель злоумышленника – данные, благодаря которым он сможет выдать себя за настоящего владельца электронного счета. В этом случае он получает практически неограниченный доступ и может совершать любые финансовые операции с деньгами жертвы. Большой интерес представляют данные кредитных карт, в первую очередь номера. Их можно похитить, например, заманив пользователя на подложный сайт, где он сам введет свои данные в форму. Для доступа к счету в платежной системе, как правило, нужны имя пользователя и пароль, плюс платежный пароль для денежных операций. Их злоумышленники могу получить путем перехвата трафика, если он передается по незащищенному протоколу или по открытой сети Wi-Fi.

Снизить риск утечки данных до минимума поможет специализированное ПО. Базовую защиту обеспечивают традиционные антивирусные технологии, но следует помнить, что злоумышленники работают на опережение, и в Сети регулярно появляются новые модификации вредоносного ПО, справиться с которыми достаточно сложно. Потому защита компьютера должна быть комплексной, способной обеспечить безопасность финансовых данных на всех этапах хранения и передачи. Помимо антивируса нужны средства поиска уязвимостей, проверки подлинности ссылок, блокировки зловредных веб-скриптов и всплывающих окон, защиты данных от перехвата, а также виртуальная клавиатура для борьбы с кейлоггерами. «Лаборатория Касперского» воплотила эти пожелания в технологии «Безопасные платежи», входящей в состав нового продукта Kaspersky Internet Security.

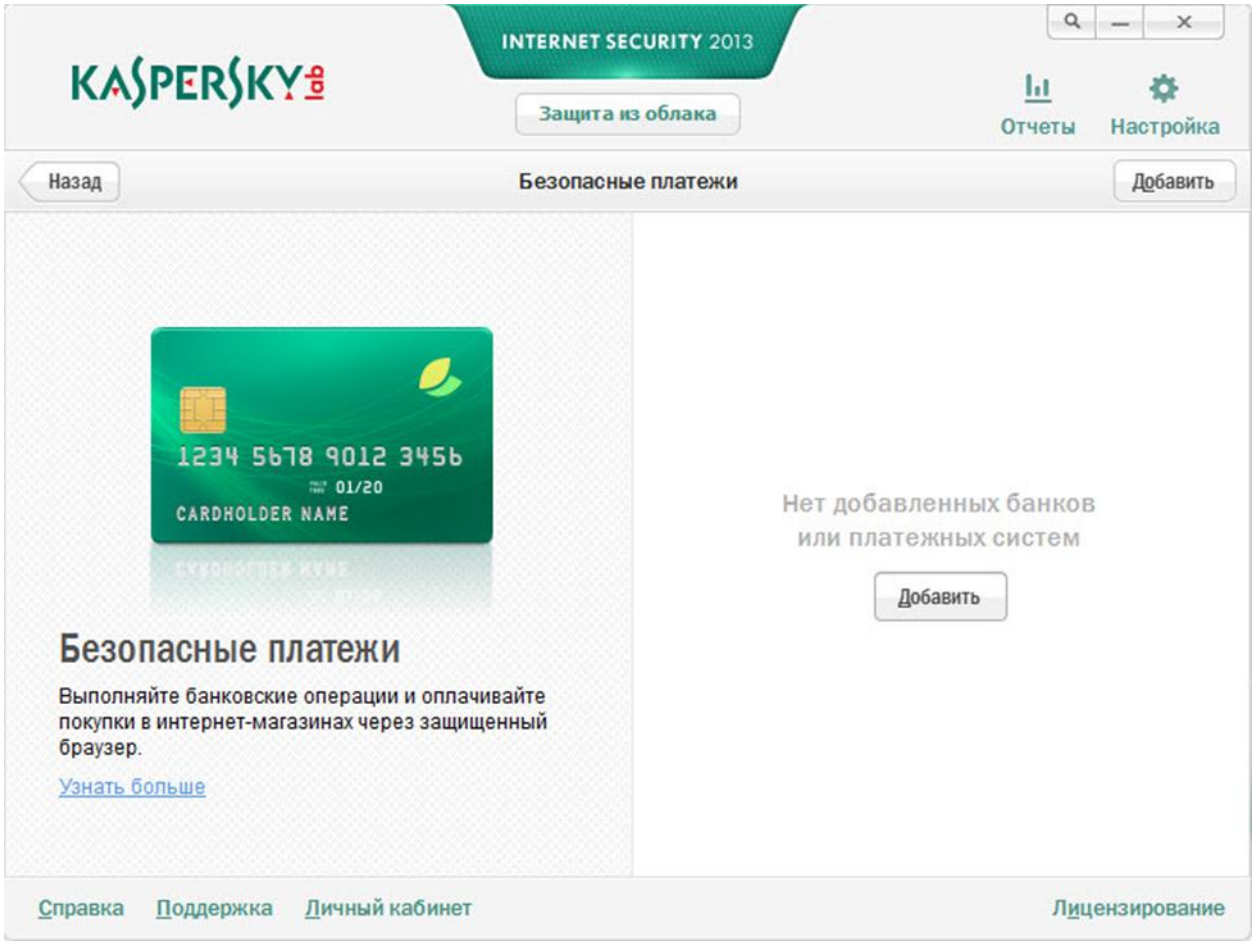
О технологии «Безопасные платежи»

Новая технология «Лаборатории Касперского» предназначена для защиты финансовой и другой важной информации во время совершения платежных операций. Она включает в себя три ключевых компонента защиты. Во-первых, это база доверенных адресов платежных и банковских систем. Как только пользователь заходит на сайт одной из таких систем, Kaspersky Internet Security проверяет адрес и предлагает перевести браузер в защищенный режим. Так технология «Безопасные платежи» гарантирует, что открываемый веб-ресурс является именно сайтом банка или платежной системы, а не подделкой злоумышленников.

Но не менее важно выполнять проверку подлинности сервера, с которым устанавливается соединение. Часто злоумышленники создают фальшивые онлайн-магазины с целью сбора пользовательской информации, поэтому сайт должен иметь сертификат подлинности. Этот электронный документ гарантирует, что данные онлайн-магазина проверены, владеющая им компания действительно существует, а соединение с сервером защищено от перехвата. Сервис проверки сертификатов, второй ключевой компонент «Безопасные платежи», поможет точно определить подлинность веб-сайта.

Одновременно с запуском защищенного режима браузера происходит проверка компьютера пользователя на наличие уязвимостей – это третий ключевой компонент

модуля «Безопасные платежи». Процесс проходит быстро, так как проверяются лишь уязвимости опредленного типа, влияющие на безопасность онлайн-банкинга (к примеру уязвимости класса повышения привелегий). В случае обнаружения «дыр» пользователю будет предложено устранить их в автоматическом режиме. При желании отложить обновление и продолжить операцию, однако это негативно скажется на безопасности системы. Также стоит отметить новую функцию «Защита ввода данных с аппаратной клавиатуры», позволяющую защитить ввод данных с аппаратной клавиатуры посредством специализированного драйвера, и управляемую при помощи мыши виртуальную клавиатуру, которые исключают перехват логинов и паролей в те моменты, когда пользователь вводит их в браузере или другой программе.



Технология «Безопасные платежи» работает для любых сайтов, требующих идентификации и работающих с различными платежными системами через протокол HTTPS. Кроме того пользователь самостоятельно может добавить в список доверенных ресурсов любой банк, платежную систему или интернет-магазин. Активации защитных механизмов не требует предварительной настройки модуля, за исключением подтверждения использования технологии для конкретного сайта. В дальнейшем активация будет происходить автоматически, но при этом пользователь всегда сможет отменить запуск «Безопасных платежей» и продолжить работать в обычном браузере. Также возможен простой запуск режима модуля для выбранного заранее сайта с помощью специального ярлыка на рабочем столе. Это дает возможность создать легкодоступную и безопасную точку входа на нужный сайт.

В итоге, используя новую технологию «Безопасные платежи» и другие методы защиты, продукт Kaspersky Internet Security позволяет создать безопасную среду, в которой пользователь может уверенно осуществлять банковские операции или делать покупки в Интернете.