Банк у телефона!

Банки слушают... Слышат ли пользователи?

Владимир Безмалый

Сегодня банки стараются сделать все, чтобы клиентам было удобно пользоваться их услугами. С развитием рынка мобильных устройств вырос и спрос на программы доступа с мобильного телефона к службам банка. Хотя все банки заявляют о своей готовности предложить такие услуги, меня все же посещают сомнения, а всегда ли представители банков понимают, что же они делают? И уж тем более, готовы ли клиенты к использованию такого программного обеспечения? В настоящей статье я попытаюсь ответить на эти вопросы. Но сначала давайте дадим определение понятию «мобильный банк», так как во многих банках под этим все еще понимают другую возможность — «SMS-банк».

Что такое мобильный банк?

По мере развития банковской системы и мобильной связи все чаще обсуждается вопрос о простоте и мобильности осуществления операций по банковским картам. С помощью мобильного телефона любой владелец пластиковой карты сегодня может делать следующее:

- получать информацию об изменениях счета;
- покупать или продавать валюту;
- осуществлять денежные переводы;
- пополнять счета на других картах;
- оплачивать коммунальные услуги, мобильную связь, Интернет и т. д.;
- заблокировать пластиковую карту в случае утери или хищения и многое другое.

Преимущества мобильного банка очевидны, для его использования не нужен ни компьютер, ни постоянный доступ в Интернет. Необходим только мобильный телефон стандарта GSM.

Функция «SMS-банк» предоставляет похожие возможности для операций с банковским счетом. Разница лишь в том, что для подключения данной услуги не требуется устанавливать на мобильный телефон специальное программное обеспечение. Фактически данная услуга предназначена для информирования пользователя о движении средств на его банковском счете.

Итак, вернемся к вопросу о том, готовы ли клиенты использовать предоставляемые возможности. На мой взгляд, нет, и поясню почему. Пользователи по-прежнему не заботятся о своей информационной безопасности. Уровень их знаний до сих пор значительно ниже уровня сложности устройств, которыми они пользуются, и установленных на них программ. И никто из производителей еще не решил

проблему обновлений. Об обновлении компьютеров написано множество статей, но компании часто забывают, что необходимо обновлять не только операционные системы, но и прикладные программы. Пора уже привыкнуть к тому, что программы пишут люди, а людям свойственно ошибаться.

Проблемы обновления

Чтобы не быть голословным, приведу несколько цифр. 27 января этого года компания Eset представила отчет об уязвимых местах программных продуктов Microsoft в 2015 году. Отмечен четырехкратный рост числа уязвимостей в различных компонентах пользовательского интерфейса Windows. Эти слабые места могут быть использованы для удаленного исполнения вредоносного кода или получения максимальных привилегий в системе.

Второй год подряд большинство уязвимостей программных продуктов Microsoft приходится на Internet Explorer — 231. Тем не менее их число незначительно снизилось по сравнению с 2014 годом (243). Закрытые уязвимости браузера могли использоваться для скрытой установки вредоносного программного обеспечения. В новом браузере Microsoft Edge, представленном в 2015 году, за отчетный период закрыто 27 пробелов. Продукт использует усиленные настройки безопасности, которые по умолчанию выключены в Internet Explorer 11.

Некоторые ошибки программных продуктов Microsoft использовались при атаках. В частности, уязвимость диспетчера монтирования дисков CVE-2015-1769 позволяла запускать произвольный код с USB-носителя с максимальными привилегиями. Она напоминает ошибку, которая ранее использовалась для распространения червя Stuxnet. Уязвимость системного драйвера http.sys CVE-2015-1635 позволяла удаленно исполнять код, предпринимать DDoS-атаки или вызывать критическую системную ошибку Windows (BSoD). В целом в 2015 году Microsoft исправила 571 ошибку в своих продуктах, что на треть больше, чем в 2014 году.

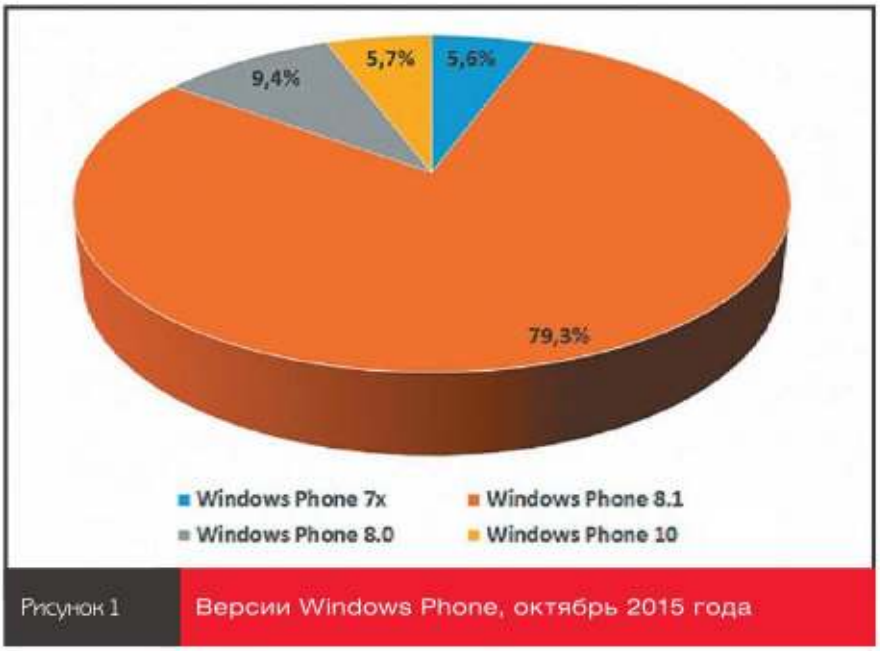


Рисунок 1 Версии Windows Phone, октябрь 2015 года

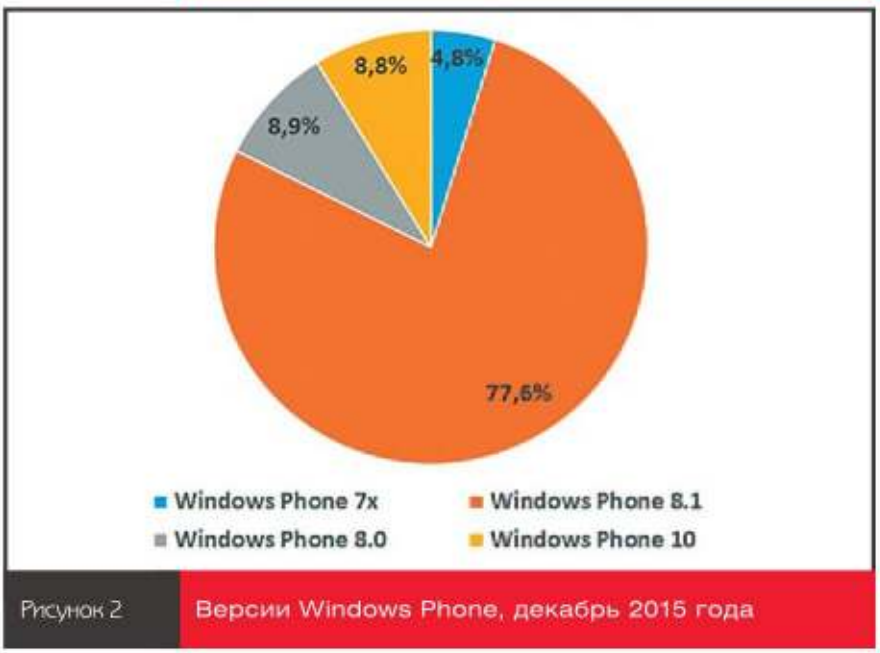


Рисунок 2 Версии Windows Phone, декабрь 2015 года

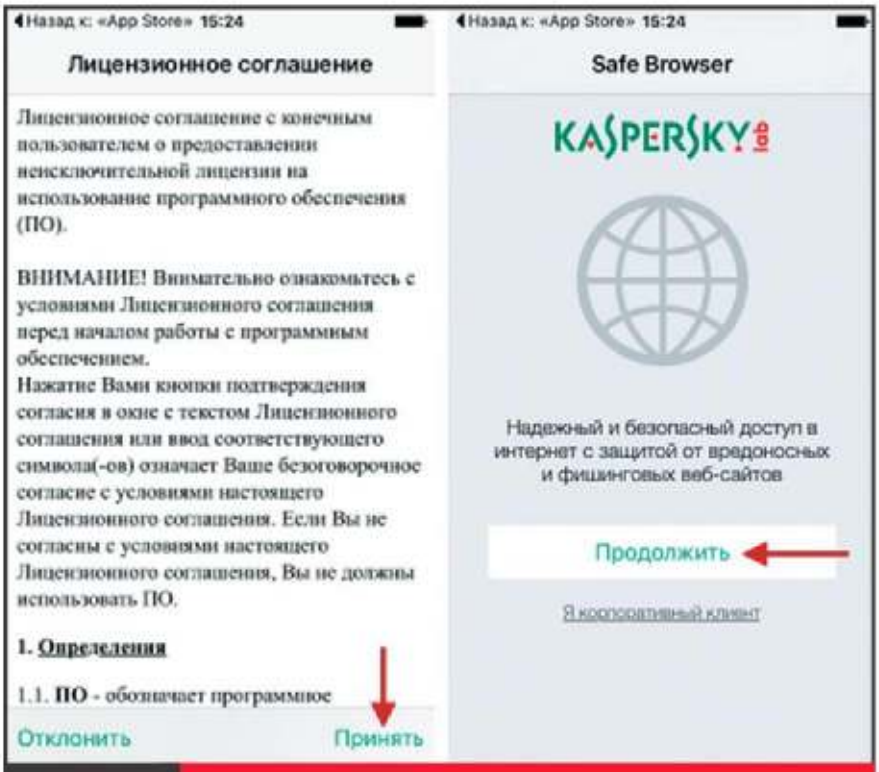
А как обстоит дело с обновлением Windows и приложений на компьютерах? Обратимся к статистике компании Secunia, основанной на сборе данных 20000 пользователей.

Общее число компьютеров, на которых установлена одна или несколько небезопасных программ составляет 98,09%, то есть 98 из 100 компьютеров, подключенных к Интернету, содержат небезопасное программное обеспечение. Исследователи получили следующее распределение компьютеров по числу небезопасных программ:

- 0 опасных программ — на 1,91% компьютеров;
- 1–5 опасных программ — на 30,27% компьютеров;
- 6–10 опасных программ — на 25,07% компьютеров;
- 11 и более небезопасных программ — на 45,76% компьютеров.

Небезопасной программой считается программа, имеющая новую версию, доступную у поставщика, в которой исправлены ошибки. При этом пользователь должен установить эту новую, более защищенную версию.

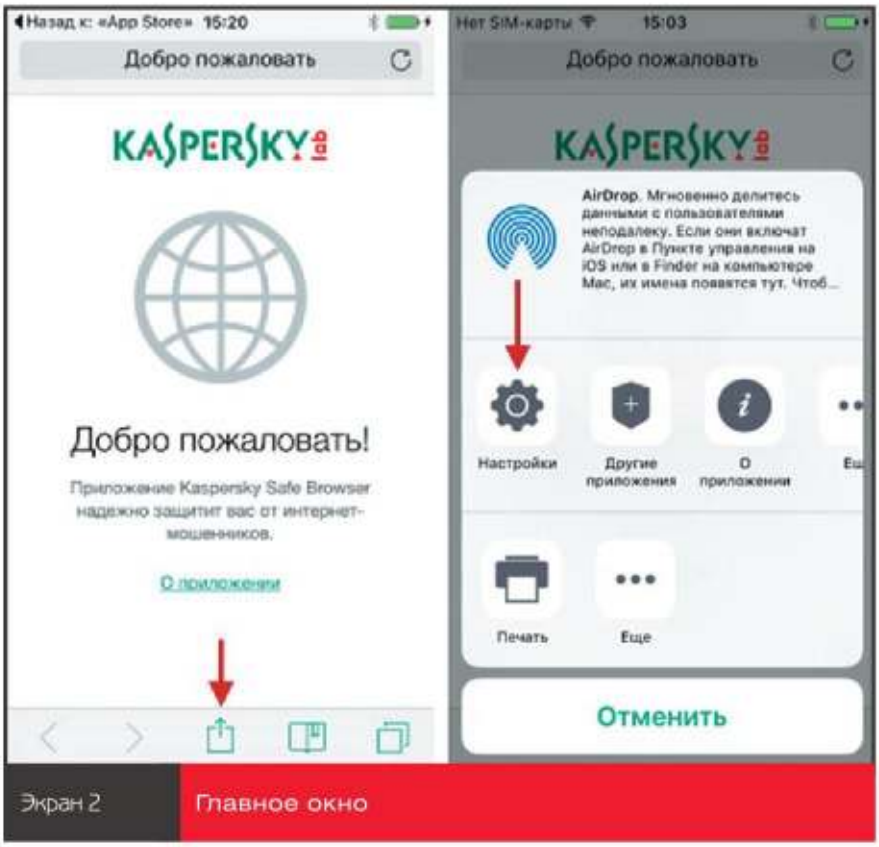
Уязвимость в программе может быть использована злоумышленниками для автоматической установки троянца (вредоносной программы), хищения конфиденци-



Экран 1 Лицензионное соглашение

альной информации и т.д. Следует помнить, что никакой антивирус не сможет защитить от угрозы наличия уязвимостей в программном обеспечении. Жизненно важно устанавливать исправления в программном обеспечении вовремя.

Вы спросите меня, а какое отношение все это имеет к мобильному банку? На самом деле все просто.



Экран 2 Главное окно

Сегодня мы используем планшеты под управлением Windows. Чем они отличаются от стационарных компьютеров? По большому счету — ничем. А как обстоят дела с обновлением смартфонов под управлением Windows Phone?

Обновление Windows Phone

Рассмотрим данные из отчета рекламной сети AdDuplex Windows Phone Statistics Report (за октябрь 2015). Отчет составлен на базе 5422 приложений Windows Phone, использующих AdDuplex SDK v2 и выше (см. рисунок 1).

В декабре 2015 картина изменилась (см. рисунок 2).

Безусловно, пользователи обновляют свои устройства, однако это очень медленный процесс. Вместе с тем стоит учесть, что переход с Windows Phone 8.0 на версию 8.1 осуществлялся уже давно и был бесплатным, более того, версия 8.0 уже не поддерживается. Что же мы наблюдаем? Почти 10% пользователей так и не обновили свою операционную систему.

Обновление iPhone

Устойчивый миф о продуктах Apple гласит, что они более безопасны, чем все остальные. Однако стоит подчеркнуть, что в этой системе, увы, как обычно, самое слабое звено — человек, который использует продукты Apple. Для того чтобы смартфоны и планшеты были защищены от последних образцов вредоносного программного обеспечения, пользователи должны их регулярно и своевременно обновлять.

Как показало новое исследование Duo, пользователи iPhone так же безответственно относятся к обновлению iOS, как и владельцы устройств с Android. И если для последних зачастую просто нет обновлений, то для iOS они есть, но пользователи этого просто не замечают. Например, спустя пять дней после появления iOS 8.4.1 только 9% пользователей iPhone установили последнюю версию операционной системы.

Приблизительно половина iPhone работает под управлением устаревших версий iOS. Поэтому

сотни дыр в системе безопасности до сих пор не заделаны, включая дефект ins0 mnia, обнаруженный исследователями компании FireEye.

На 31% iPhone все еще установлена iOS 8.2. А ведь на этих устройствах должно быть исправлено более 160 уязвимостей.

Проблемы фишинга

Для мобильных устройств отдельно стоит упомянуть проблему фишинга. На сегодня порядка 98% атак на мобильные устройства нельзя осуществить, не используя приемы социальной инженерии. Что можно этому противопоставить, например, на iPhone? Только установку защищенного браузера, ссылки в адресной строке которого можно проверять в «облаке». В качестве примера такого браузера можно рассмотреть установку Kaspersky Safe Browser. Сама установка Kaspersky Safe Browser (iOS) проста:

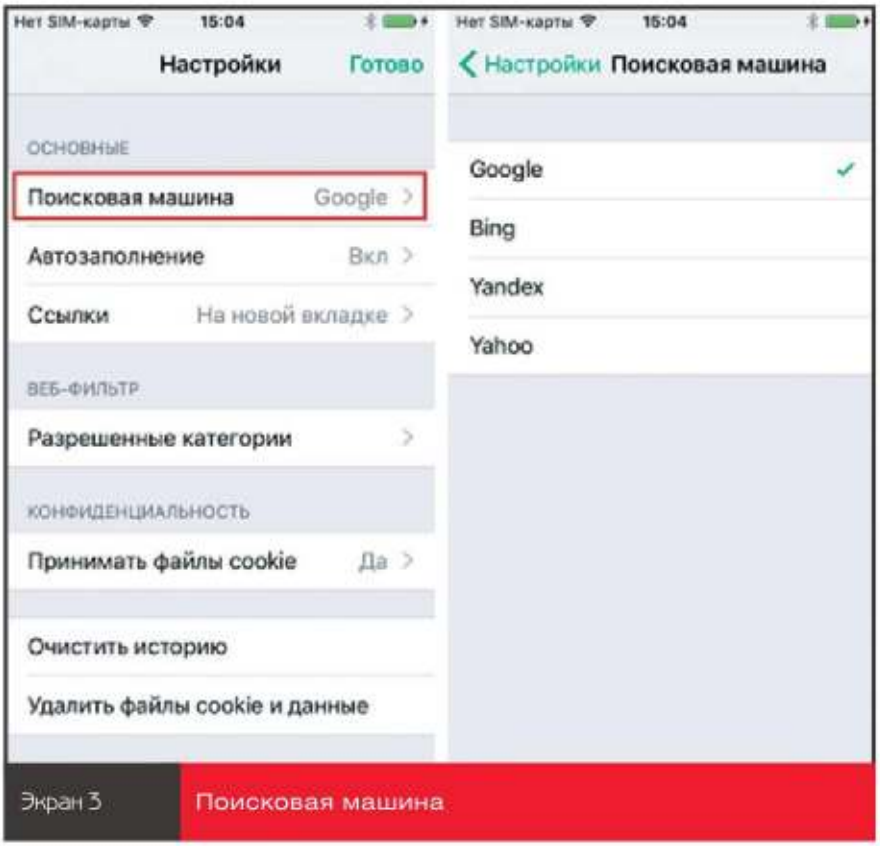
1. Откройте App Store.
2. Введите в строке поиска Kaspersky Safe Browser.
3. Нажмите «Загрузить», «Установить».
4. Введите пароль для Apple ID и щелкните OK.
5. Откройте Kaspersky Safe Browser.
6. Ознакомьтесь с «Лицензионным соглашением» и нажмите «Принять» (см. экран 1).
7. Нажмите «Продолжить».

Настройка параметров Kaspersky Safe Browser (iOS) также проста:

1. Откройте Safe Browser.
2. Выберите «Настройки» (см. экран 2).
3. Нажмите «Поисковая машина» (см. экран 3).
4. Выберите одну из поисковых машин.
5. Нажмите «Автозаполнение».
6. Установите переключатель «Имя, пароль» в нужное положение (см. экран 4).

Автозаполнение

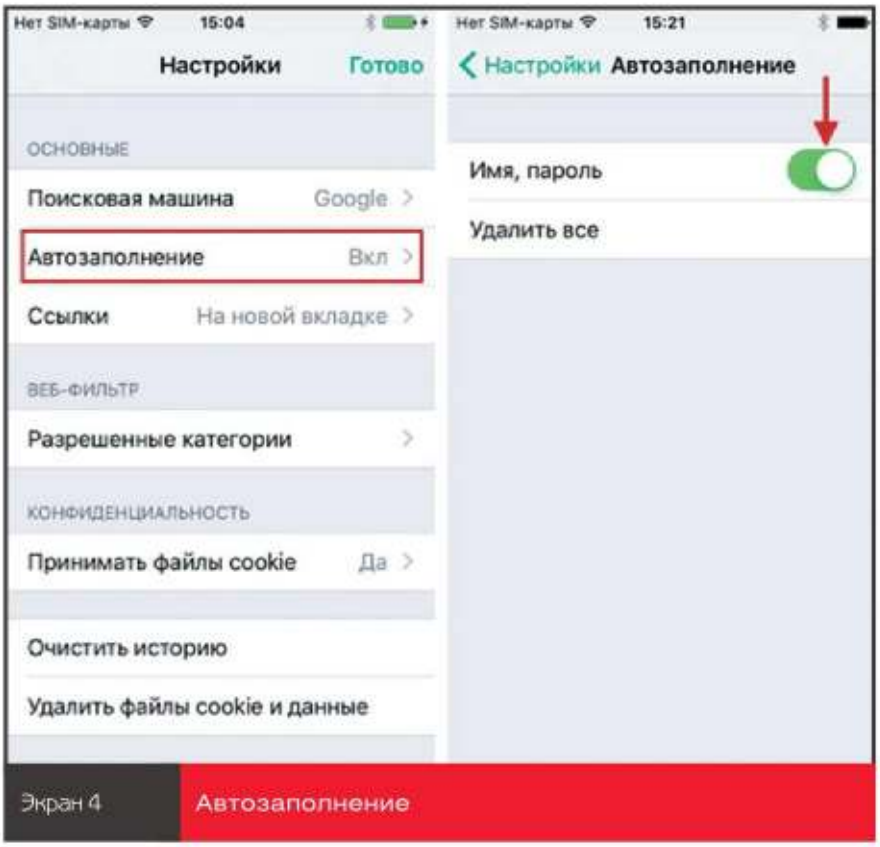
Чтобы удалить сохраненные в памяти значения автозаполнения, нажмите «Удалить все». Затем нажмите «Ссылки» и выберите режим открытия ссылок (см. экран 5).



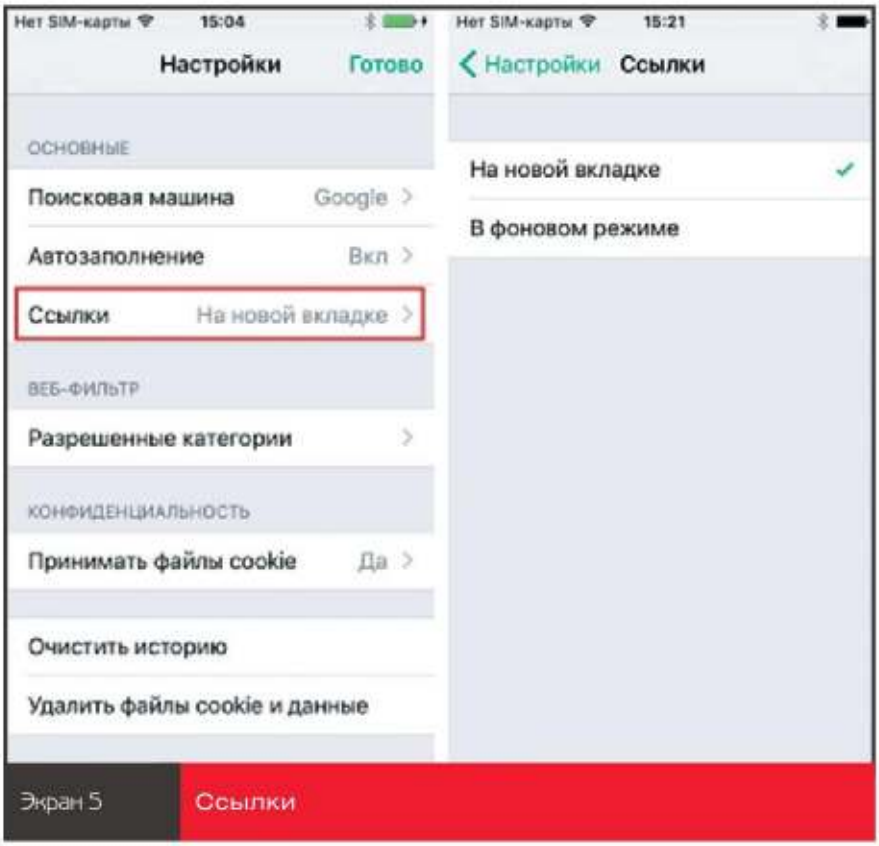
Экран 3 Поисковая машина

Для настройки веб-фильтра нажмите «Разрешенные категории» и выберите категории сайтов, посещение которых будет разрешено. Переключатель для этих категорий должен быть зеленого цвета (см. экран 6).

Категории «Фишинг» и «Вредоносные ссылки» запрещены по умолчанию.



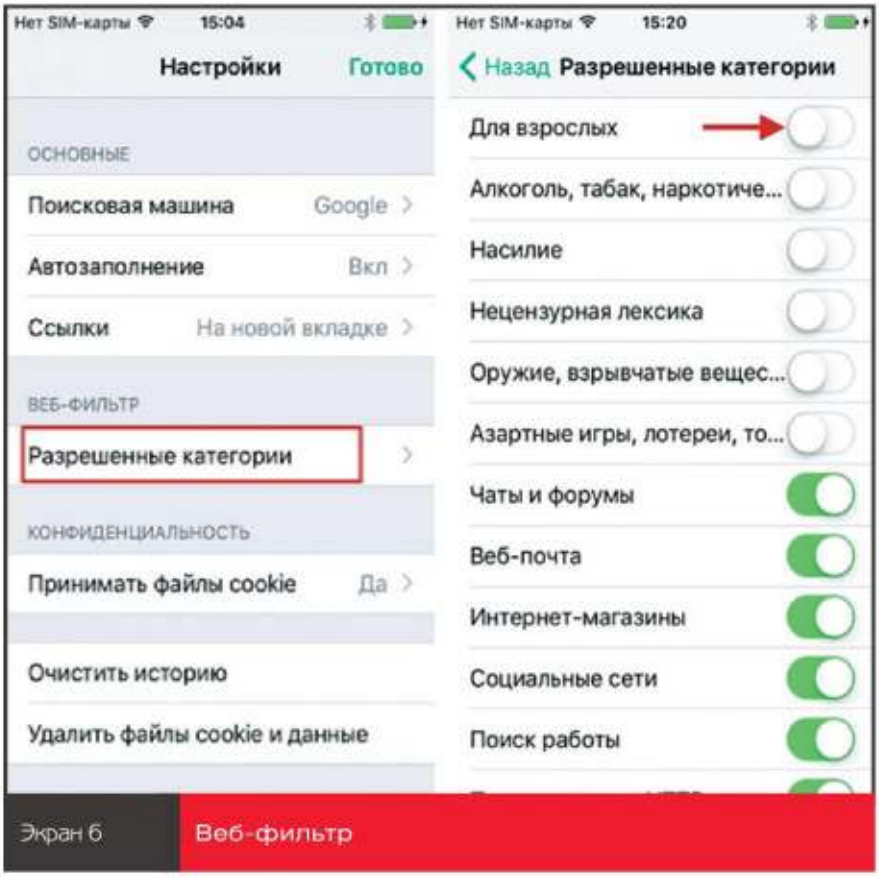
Экран 4 Автозаполнение



Экран 5 Ссылки

Файлы cookie требуют особого внимания, для их настройки нажмите «Принимать файлы cookie» и выберите «Да» или «Нет» (см. экран 7).

Очистка истории запускается нажатием на ссылку «Очистить историю». Затем подтвердите удаление истории (см. экран 8).



Экран 6 Веб-фильтр

Удаление файлов cookie и данных позволяет устранить сбои в работе некоторых программ, для этого нажмите «Удалить файлы cookie и данные» и подтвердите удаление (см. экран 9).

Фишинг и QR-коды

Код QR (Quick Response — «быстрый отклик») может содержать любую текстовую информацию, в том числе ссылки на интернет-источники. QR-код можно встретить повсюду — на рекламных щитах и листовках, в магазинах, на веб-сайтах, билетах и т.д. Пользователь смартфона, фотографируя QR-код, должен понимать, что ссылка может привести его на страницу вредоносного приложения. Сегодня популярны мошеннические схемы, связанные с QR-кодами. Например, не редки случаи, когда злоумышленники аккуратно наклеивают свой вредоносный QR-код поверх оригинального. Это явление получило название QRishing по аналогии с фишингом.

Фишинг (phishing) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей: именам учетных записей и паролям. Это достигается с помощью массовых рассылок электронных писем от имени популярных торговых марок, а также отправки личных сообщений внутри различных сетей, например от имени банков или в социальных сетях. В таком письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с перенаправлением. После того как пользователь попадает на поддельную страницу, мошенники пытаются разными способами побудить его ввести на поддельной странице имя и пароль, которые он использует для доступа к определенному сайту.

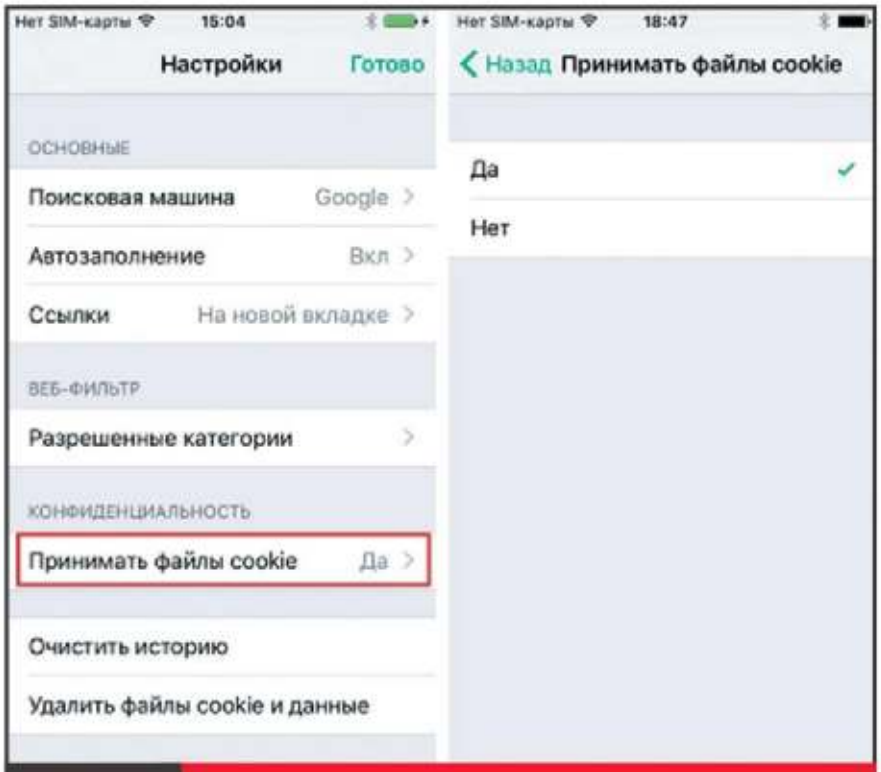
Фишинг — одна из разновидностей социальной инженерии, основанная на незнании пользователями правил сетевой безопасности: в частности, многие просто не знают о том, что компании и банки никогда не рассылают писем с просьбами сообщить свои учетные данные, пароль и пр.

Тип сведений, интересующих киберпреступников, в конечном счете определяет тип фишинговой атаки. Например, если целью фишинга является получение доступа к учетной записи в социальной сети, то злоумышленник попытается, используя поддельный веб-сайт, похожий на социальную сеть, принудить жертву оставить адрес своей электронной почты и пароль к сети. Если цель киберпреступника — завладеть деньгами жертвы, то поддельный веб-сайт может содержать поля для ввода учетных данных, связанные с финансами и информацией о кредитной карте.

Статистика показывает, что 75% всех известных мобильных фишинговых сайтов были мошенническими версиями известных банковских или финансовых сайтов. Часть фишинговых сайтов разработана для имитации сайтов социальных сетей (2%) и сайтов магазинов (4%). Небольшое число фишинговых сайтов для социальных сетей может объясняться тем, что пользователи предпочитают специальные приложения для общения в социальных сетях.

Легко представить, насколько опасен QR-код, наклеенный в общественном месте и содержащий вредоносную ссылку. Проблема усугубляется тем, что, когда вы используете смартфон или даже планшет, вы далеко не всегда можете увидеть полную адресную строку, а это не позволяет определить, правильная страница перед вами или фишинговый сайт.

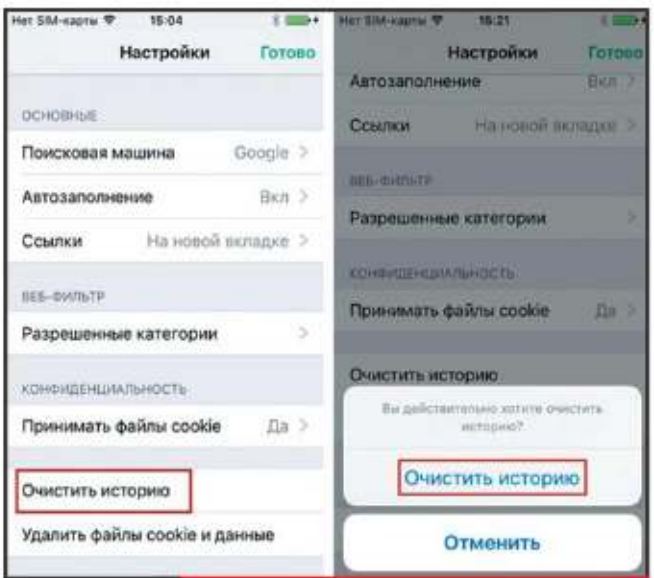
Специфика смартфонов в том, что мобильные браузеры выводят на экран только одно окно браузера за раз. Браузеры Android и iOS выводят на экран URL текущего окна в верхней строке экрана. Однако веб-сайты могут скрыть панель URL, как только страница загрузилась. Если целевой сайт скрывает свою панель URL, то мобильное приложение может загрузить фишинговый веб-сайт в браузере. На сегодня многие защищенные паролем веб-сайты, например Amazon и Facebook, скрывают свои URL.



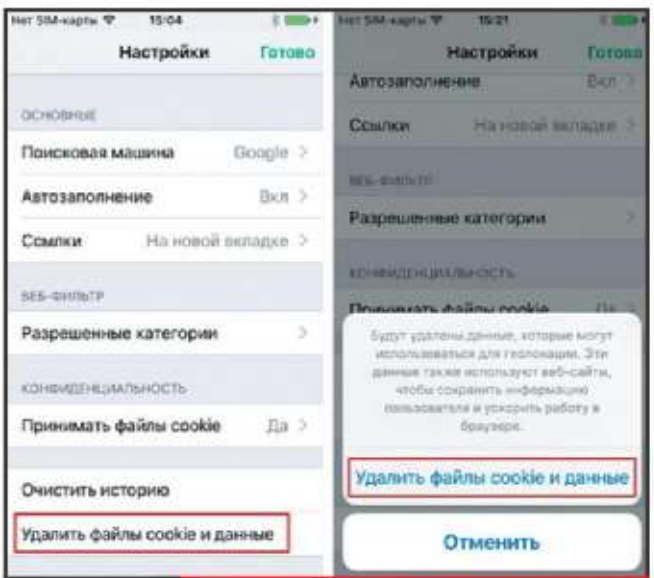
Экран 7 Cookie

Как избежать проблем

Чтобы не попасть в ловушку, можно принять следующие меры.



Экран 8 Очистка истории



Экран 9 Удаление файлов cookie и данных

Экран 10 QR-сканер

Экран 11 Опасная ссылка

Пользователям

- Перед сканированием убедитесь, что QR-код не изменен, например не наклеен поверх другого.
- После того как в браузере вы откроете страницу по QR-коду, убедитесь, что это действительно тот сайт и та страница, куда вы хотели попасть.
- Установите на смартфон приложения, которые могут проверять сайты на вредоносное содержимое. Особенно это важно для смартфонов на базе Android, ведь для них существуют десятки тысяч вредоносных приложений.
- Пользователям iOS и Windows Phone 8.1 не стоит обольщаться. Проблема фишинга актуальна для пользователей любых мобильных операционных систем.

Предприятиям

- Сотрудник, который знает, что такое фишинг, вряд ли пропустит атаку, подвергнув опасности данные компании.
- Фишинг может использоваться как один из этапов в атаке, направленной на вашу компанию. Нередко цели такой атаки — завладеть деньгами компании, осуществить корпоративный шпионаж или похитить персональные данные сотрудников. Именно поэтому крайне важно использовать комплексные решения по обеспечению безопасности. Лучшим вариантом решения будет антивирусный продукт, в котором реализованы репутационные технологии проверки веб-страниц.

Защищенный сканер QR-кодов

QR-коды позволяют быстро открыть веб-сайт или изображение, загрузить контактную информацию или подключиться к Wi-Fi, и все это одним касанием экрана! Удобно, не правда ли? К сожалению, как я объяснил выше, это еще и небезопасно: подменить код на рекламном постере в банке, в аэропорту или общественном транспорте может кто угодно. С этим видом мошенничества можно и нужно бороться: внимательно осматривать рекламный плакат (не наклеили ли поверх

одного кода другой) и, прежде чем вводить свои данные, проверять, точно ли вы попали на нужный сайт. Впрочем, этот подход сводит на нет основную идею использования QR-кодов — быстроту и удобство. Конечно же, в век цифровых технологий есть и более подходящие средства защиты, например бесплатное мобильное приложение Kaspersky QR Scanner.

Данное приложение работает как обычный сканер QR-кодов, но у него есть еще одна важная функция: оно проверяет каждый отсканированный код. Используя Kaspersky QR Scanner, можно быстро и, главное, безопасно получить любую интересующую вас информацию. Вам больше не придется вводить данные вручную, чтобы перейти на веб-сайт, открыть картинку или текст, автоматически подключиться к Wi-Fi или же буквально за секунду сохранить контактные данные с визитки (см. экран 10). Приложение доступно для пользователей смартфонов под управлением Apple iOS и Google Android. В его интерфейсе нет ничего лишнего; если со ссылкой, которая содержится в QR-коде, все нормально, то она сразу откроется. Если же в ней содержится что-то подозрительное, то вы увидите предупреждение (см. экран 11).

Обновление Android

Проблемы обновления мобильных устройств обсуждаются давно. Но, увы, смартфоны, особенно под управлением Android, обновляются производителями весьма неохотно. Или не обновляются вовсе. Обратимся к статистике. Опубликованные в январе результаты анализа Security Duo показывают, что не менее 90% устройств на базе Android сегодня работают под управлением устаревших версий операционной системы, что влечет за собой значительные риски для корпоративных и частных пользователей. Приблизительно 70% устройств работают под управлением Android 4.4 и более старых версий. Получается, что они восприимчивы к таким уязвимостям, как Stagefright. Данная уязвимость открывает злоумышленнику доступ к устройству и далее к корпоративной сети через сообщение MMS, например фото или видео.

По оценке Duo, более 20 млн устройств Android более не поддерживаются производителями и потому не могут быть обновлены до последних версий программного обеспечения, что позволило бы устранять их слабые места.

Позиция производителей известна. Так, Google официально заявила, что не будет выпускать обновления для устройств старше двух лет. Однако такая позиция не защищает производителя. Так, иск за отсутствие своевременных обновлений программного обеспечения смартфонов на базе Android компании Samsung предъявляет ассоциация Dutch Consumers' Association (DCA). Согласно исследованию DCA, по крайней мере 82% смартфонов Samsung, доступных на голландском рынке, не получили обновлений до последней версии Android за два года. Это привело к тому, что большинство из них содержит уязвимости. Сотрудники DCA сообщили, что агентство связывалось с Samsung, но достичь соглашения не удалось и поэтому было решено обратиться в суд.

Однако не стоит думать, что, даже если суд обяжет Samsung принять необходимые меры, ситуация с безопасностью на рынке смартфонов на Android заметно улучшится. На сегодня не существует стандарта этой операционной системы, и каждый производитель смартфонов выпускает свою версию прошивки для своего смартфона, поэтому обновление требует значительных усилий. А ведь таких уникальных устройств на базе Android, по результатам исследований, выпущено более 10000. Таким образом, проблема обновлений на сегодня практически не имеет решения.

Что делать? Duo рекомендует принимать следующие меры для снижения рисков.

- Все владельцы устройств должны использовать PIN-коды для их блокировки.
- Запретить использовать смартфоны с правами администратора, или root.
- Обязательно обновлять мобильные устройства.
- Обновить или заменить устаревшие смартфоны, которые более не обновляются производителем.
- Рекомендовать пользователям приобретать смартфоны с более частыми обновлениями от производителя.

Что должны делать банки

Банкам можно рекомендовать в их версиях мобильного банка сделать следующее:

1. Проверять версию операционной системы и, если она отличается от текущей, рекомендовать обновить операционную систему (для iPhone и WP). Для пользователей Android, если версия операционной системы старше текущей на две и более, рекомендовать сменить смартфон.
2. Если на смартфоне осуществлялся взлом установленного производителем встроенного программного обеспечения или применяются права учетной записи root, рекомендовать не использовать услуги мобильного банка.
3. Если на смартфоне под управлением Android отсутствует антивирус, рекомендовать установить его.
4. Если разрешена установка программ из сторонних хранилищ, посоветовать запретить это делать.

Или можно просто вывести на экран список параметров, которые, по мнению банка, снижают безопасность мобильного устройства. Естественно, банк может лишь рекомендовать пользователю усилить меры безопасности, а делать это или нет, решает владелец устройства. И в случае проблем с безопасностью он отвечает за свои действия сам. Задача банка — его предупредить.

Владимир Безмалый (vladb@windowslive.com) — специалист по обеспечению безопасности, имеет звания MVP Consumer Security, Microsoft Security Trusted Advisor