УДК 004

ОПАСНОСТИ МОБИЛЬНОГО ИНТЕРНЕТА

Ширякова В.О., студентка 3 курса 5 группы экономического факультета
Научный руководитель – Голубев С. В., к.э.н., доцент
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *мобильный интернет, угрозы, гаджеты, интернет - ресурсы, пользователь, мошенничество, банкинг.*

В статье рассмотрены угрозы и опасности, с которыми может встретиться пользователь мобильного интернета и то, каким образом осуществляются мошенничества в сфере мобильного интернета.

В настоящее время мобильный интернет завоевывает все большую популярность и по своей распространенности скоро догонит традиционный проводной аналог. Увеличиваются скорости передачи данных, развиваются связные технологии и каждый современный смартфон использует возможности мобильного соединения в полном объеме. Гаджет всегда находится вместе со своим владельцем и оперативное решение таких задач, как работа с электронной почтой, создание и редактирование документов, а также веб-серфинг с помощью мобильного устройства, уже давно являются частью обыденности. Основные виды опасностей мобильного интернета указаны в схеме.

Доступность беспроводного интернета практически в любой точке земного шара таит в себе ряд специфичных опасностей. Вредоносные программы, которые эффективно фильтруются антивирусами на компьютерах, на просторах мобильного интернета в полной мере проявляют себя, угрожая безопасности вашего устройства. Не стоит забывать и про то, что баланс лицевого счета абонента представляет большой интерес для недобросовестных контент-провайдеров и различного рода мошенников.

Одной из опасностей мобильного интернета является угроза, которая возникает при пользовании мобильным банкингом. В текущем году «Лабораторией Касперского» вместе с компанией B2B International было проведено исследование, которое показало, что 79% отечественных клиентов оперируют с онлайн-сервисами финансовой направленности. А для онлайн-банкинга свои мобильные гаджеты применяют около 21% клиентов банковских учреждений. Но финансовые операции в Ин-

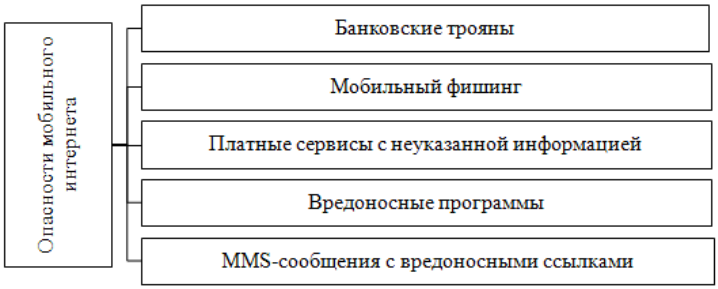

Рисунок 1 - Опасности мобильного интернета

тернете пока не могут похвастать безопасностью. [6] Главной опасностью для владельцев гаджетов на данный момент являются банковские трояны. Они представляют собой специализированные программы, цель которых – хищение данных пользователя финансового характера. Армия таких вирусов растет постоянно. Для своей защиты они применяют все более эффективные методы. То же касается и собственно похищения средств и заражения новых устройств. Однако, необходимо помнить, что уже есть троянцы не только под Android, но и под Blackberry, либо Symbian. Создатели вирусов внимательно изучают новинки сервисов мобильного банкинга. После инфицирования вирусом смартфон в первую очередь проверяется на предмет привязки к пластиковой карте.

Мобильный фишинг – это еще одна угроза для гаджетов. То же можно сказать и о краже данных о пластиковых картах, перечислении средств со счета клиента на счета преступников. [1] Определить же наличие троянца на смартфоне самому клиенту довольно сложно. Чаще всего люди узнают о присутствии «гостя» только после попасться на удочку мошенников можно при посещении определенных ресурсов. Так, во время веб-серфинга часто можно встретить предложения «обновления» программного обеспечения. Такие оповещения можно получить, например, при переадресации с других, безопасных сайтов. После взаимодействия с таким информационным баннером происходит загрузка вредоносной программы, которая автоматически рассылает СМС-сообщения на платные короткие номера. С проблемой автоматической рассылки СМС-сообщений также сталкиваются пользователи, которые устанавливают программное обеспечение с многочисленных

сайтов, предлагающих взломанные версии платных программ.

Существует и такая схема: на устройство приходит извещение о том, что для данного номера пришло MMS-сообщение. При переходе по ссылке, указанной в информационном письме, происходит загрузка вредоносной программы с последующей рассылкой СМС-сообщений на платные номера. В последнее время для автоматической загрузки вредоносного ПО достаточно просто открыть такое сообщение, особенно если у вас подключена опция автоматического перехода по полученным ссылкам.

Особую бдительность следует проявлять, пользуясь платными сервисами, которые предоставляют различные интернет-ресурсы. Порой на них бывает указана неверная информация, занижена стоимость предлагаемого контента. Рассчитывая скачать содержимое за написанную крупным шрифтом сумму, можно не обратить внимание на едва различимое примечание внизу, что цена указана на одни сутки. При этом вы оплачиваете подписку сразу на несколько месяцев. Также на сайте может быть не обозначено количество СМС-сообщений, которое необходимо отправить для совершения покупки.

Из сказанного выше можно сделать вывод о том, что мобильный интернет стал частью повседневной жизни каждого человека и значительно упрощает ее, но следует помнить и о том, что следует соблюдать правила безопасности в интернете, внимательнее читать соглашения, которые заключаются при установке приложений, не доверять подозрительным сайтам и сообщениям и т.д.

Библиографический список

1. Арбатова, М.И. Мобильные связи / М.И. Арбатова. - М.: АСТ, 2016. - 558с.
2. Информационная безопасность. Защита информации [Электронный ресурс] // Мобильное мошенничество.- URL: http://uspehmoney.ru/mobilnoe-moshennichestvo/ (дата обращения 31.03.2017).
3. Безопасность Информационных Технологий [Электронный ресурс] // Концепция обеспечения информационной безопасности предприятия.- URL: http://asher.ru/security/book/its/17 (дата обращения 31.03.2017).

THE DANGER MOBILE INTERNET

Shiryakova V. O.

Keywords: *mobile Internet, threats, gadgets, Internet resources, user, fraud, banking.*

Abstract: the article discusses the threats and risks that may face the user of the mobile Internet and how are fraud in the field of mobile Internet.