Информационно-аналитический материал о профилактике правонарушений, совершаемых с использованием мобильных средств связи и в сети Интернет

САМАРА

2017 г.

СОДЕРЖАНИЕ

Предисловие

27 марта т.г. комитетом по законодательству, законности, правопорядку и противодействию коррупции и комитетом по транспорту, автомобильным дорогам, информационным технологиям и связи Самарской Губернской Думы проведен «круглый стол» на тему «Совершенствование нормативно-правовой базы с целью предотвращения правонарушений, совершаемых с использованием мобильных средств связи и в сети Интернет».

В ходе данного мероприятия представителями надзорных и правоохранительных органов, а также научной общественности была представлена информация о том, что граждане, пострадавшие от действий мошенников, не научились соблюдать элементарные правила финансовой безопасности в Интернете. В 2016 году число интернет-краж с банковских карт из-за халатности их владельцев достигло 107 тыс. случаев – это на 43% и 78% больше, чем в 2015 и 2014 годах соответственно. По экспертным оценкам, в 70% случаев клиенты сами понимают, как именно злоумышленники завладели их деньгами.

Аналитики установили, что мошенники чаще всего атакуют компьютеры с помощью вирусов и получают дубликаты SIM-карт, на которые приходят одноразовые пароли для подтверждения операций. Имеет место и человеческий фактор: иногда клиенты сами открывают страницу интернет-банка, например, в офисе, что увеличивает риски доступа к их персональным данным третьих лиц. Довольно опасно подключать интернет-банк и к социальным сетям, которые не несут никакой ответственности за счета пользователей.

Дополнительные риски, по мнению экспертов, создает и активное использование смартфонов для входа в личный кабинет. Многие для упрощения доступа к мобильному банку предпочитают вводить четырехзначный код вместо полноценных логинов и паролей и тем самым увеличивают степень уязвимости приложения.

Почти треть россиян (31%) становились жертвами преступлений, которые связаны с сотовой связью или интернет-сервисами. Об этом свидетельствуют данные декабрьского опроса, проведенного Всероссийским центром изучения общественного мнения (ВЦИОМ).

Как показали результаты исследования, эта доля выше среди молодежи (36%), москвичей и петербуржцев (37%), активных интернет-пользователей (38%), жителей средних городов (43%).

Ниже – среди людей старше 60 лет (21%), жителей сел (24%) и тех, кто практически не заходит в интернет (17%).

С преступлениями в киберсфере не сталкивались 68% участников опроса.

Больше всего граждане РФ (65%) опасаются кражи денег с банковских карт и утечки персональной информации. 56% боятся ложной информации, распространяемой злоумышленниками через SMS или электронную почту.

55% опрошенных волнует, что кто-то может получить доступ к их страницам в социальных сетях, а 52% опасаются техногенных катастроф, причиной которых может стать доступ злоумышленников к электронным системам управления атомными станциями или баллистическими ракетами.

Только 36% считают себя защищенными от подобных рисков. Опрос проведен в декабре 2016 года среди 1,6 тыс. человек в возрасте 18 лет и старше в 130 населенных пунктах 46 регионов страны. Статистическая погрешность не превышает 3,5%.

Прогнозируется, что в перспективе хакеры усилят атаки на российские банки – на них направлено 30% всех действий интернет-злоумышленников. Чуть менее трети (27%) киберпреступлений по-прежнему совершается в отношении счетов простых граждан. Пусть доход от них будет значительно меньше, но сами атаки по сложности исполнения несопоставимы со взломом корсчетов.

Вероятность того, что мошенники будут проявлять больше изобретательности, достаточно высока: за рубежом технологии мошенников

уже стали на порядок выше – в ход идут профайлы из соцсетей, сбор данных, психологический анализ.

Настоящий информационно-аналитический материал ориентирован на граждан в целях их информирования о существующих криминальных способах завладения чужими финансовыми средствами с использованием мобильных средств связи и в сети Интернет и, соответственно, использования гражданами предлагаемых практических способов защиты электронных сбережений.

I. Мошенничество в сфере использования сотовой сети

Проблема совершения мошенничества в сфере использования сотовой сети сегодня наиболее актуальна. По данным службы Росстат 91 % населения имеет мобильный телефон в собственности и, соответственно, пользуется услугами сотовой связи. Использование сотовой связи стало инструментом в руках преступников. Данные преступления наиболее латентные. Одним из часто встречаемых преступлений, совершаемых с использованием сотовой связи, является мошенничество. К сожалению, действующее российское законодательство не имеет определения таких понятий, как «мобильная связь», «сотовая связь». Это понятие раскрывается в технической литературе. Мобильная связь - вид телекоммуникаций, при котором голосовая, текстовая и графическая информация передается на абонентские беспроводные терминалы, не привязанные к определенному месту или территории. Различаются спутниковая, сотовая, транкинговая и другие виды мобильной связи. Особенности преступлений, совершаемые в сфере использования сотовой связи, заключается в их латентности, недостаточном законодательном урегулировании и в колоссальном причиненном ущербе.

По данным, опубликованным на сайте сотового оператора «Билайн», каждый год мировые убытки, связанные с мобильным мошенничеством в мировом масштабе составляют около 25 млрд. долларов. К сожалению, отечественные сотовые операторы предпочитают не афишировать свои потери от мошенничества. В результате проведенного опроса российских

абонентов установлено, что о мобильном мошенничестве знают 78 % респондентов, а 15 % отметили, что их родственники и друзья пострадали от действий мошенников.

1. Наиболее распространенные виды мошенничества

Мошенничество в сети сотовой связи, связанное с публичным объявлением

Способ обмана очень прост: на сотовый телефон приходит SMS-сообщение о выигранном имуществе и предлагается отправить сообщение, либо позвонить на определенный номер, либо ранее часто показываемое по телевидению рекламное сообщение по торговле мобильного контента. Предлагается также отправить сообщение на номер и получить желаемые абонентом музыкальный файл, картинку. Зачастую абонент ничего не получает, либо с его счета списывается больше чем указана сумма средств. Это возможно, если злоумышленник откроет коммерческий номер, то есть платный номер с целью получения прибыли от звонков или присланных сообщений.

Звонок на номер абонента с использованием коммерческого номера и моментальный сброс вызова, не дождавшись ответа

Ничего не подозревающий абонент перезванивает по данному номеру и с его счета списываются денежные средства. Возможно, что жертве на абонентский номер придёт сообщение, которое в последующем окажется фальшивкой, о пополнении баланса, и далее поступит звонок с просьбой перевести полученные абонентом деньги, так как он их получил по ошибке.

Звонок с сообщением о каком-либо происшествии с родственником, другом абонента или же сотрудником правоохранительных органов

…и так же просьба о переводе денежной суммы для того чтобы все уладить (под наиболее распространенными предлогами «Ваш сын попал в ДТП» либо «розыгрыш призов»). Следует учитывать, что данный вид

мошенничества характерен для преступников, находящихся в исправительных учреждениях (как правило, территориально расположенных в другом регионе по отношению к объекту мошенничества).

2. Примеры уголовных дел

1. У гр. М. из корыстных побуждений возник преступный умысел на совершение хищений чужого имущества путем обмана. Реализуя свой преступный умысел, М. разработал план совершения мошенничеств, согласно которому он с мобильных телефонов должен был путем случайного набора цифр осуществить рассылку составленных им самим коротких текстовых SMS - сообщений на абонентские номера, используемые различными ранее незнакомыми М. лицами, денежные средства которых он планировал похитить путем обмана, **с заведомо для него ложными, не соответствующими действительности сведениями о том, что с кредитной либо зарплатной карты владельца абонентского номера якобы осуществлен перевод денежных средств, и для отмены указанного перевода необходимо связаться с сотрудником банка, представителем которого планировал представляться сам М**. При этом в сообщении в качестве абонентского номера сотрудника банка указывался бы абонентский номер, находящийся в пользовании М., и последний планировал, что после получения указанного выше сообщения пользователь абонентского номера, будучи введенным М. в заблуждение относительно правдивости сведений, содержащихся в сообщении, должен был осуществить телефонный звонок М. После чего М., представившись сотрудником банка, введя в заблуждение позвонившего ему гражданина, желающего отмены перевода денежных средств со счета банковской карты, находящейся у последнего в пользовании, умышленно, из корыстных побуждений, планировал предложить держателю банковской карты пройти к ближайшему банкомату и осуществить ряд операций со своей банковской картой. После получения согласия на осуществление данных действий от потерпевшего, введенного М. в заблуждение относительно его преступных намерений, последний

планировал сообщить в ходе телефонного разговора с потерпевшим алгоритм его действий с банковской картой и банкоматом, в результате которых денежные средства со счета указанного держателя банковской карты переводились на счета абонентских номеров, либо банковских карт, названных М., и находящихся в пользовании последнего. В результате чего М. получал возможность распоряжаться похищенными указанным способом денежными средствами по своему усмотрению, в том числе в качестве платежного средства для осуществления расчетов от своего имени или от имени третьих лиц, не снимая денежных средств со счета, на который они были бы перечислены в результате мошенничества. При этом у М. в отношении каждого отдельного гражданина, в адрес которого он впоследствии отправлял указанные выше сообщения, каждый раз возникал конкретизированный преступный умысел на хищение денежных средств конкретного гражданина общим для всех потерпевших вышеуказанным способом. Вышеуказанным способом путем обмана М. заставил перевести потерпевших в 14 случаях на счета банковских карт и в 6 случаях на счета абонентских номеров денежные средства в сумме свыше 1 млн. руб. За совершение указанных преступлений гр. М. осужден к 3 годам 6 месяцам лишения свободы с отбыванием наказания в колонии строгого режима.

2. У гр. С., отбывающего наказание в виде лишения свободы в местах лишения свободы, из корыстных побуждений возник преступный умысел на совершение хищений, путем обмана, чужих денежных средств у неопределенного количества лиц.

Для реализации преступного умысла, направленного на хищение денежных средств, путем обмана, С. разработал способ хищения, по которому он, путем случайного набора цифр, должен был осуществить рассылку текстовых смс – сообщений на абонентские номера, используемые различными, ранее незнакомыми С. лицами. **Текст смс - сообщения содержал ложные сведения о том, что заявка на перевод с банковской карты 9 000 рублей принята**. При этом в сообщении для получения

информации указывался абонентский номер, используемый С. Гражданин получивший такое смс – сообщение, будучи обманутым относительно правдивости сведений, содержащихся в нем, должен осуществить телефонный звонок С., на указанный номер. С., представившись сотрудником банка, под предлогом отмены операции по переводу денежных средств с банковской карты, планировал предложить держателю банковской карты пройти к ближайшему банкомату и осуществить ряд операций со своей банковской картой в результате которых денежные средства с лицевого счета банковской карты должны были быть перечислены на лицевой счет абонентского номера мобильного телефона, находившегося в распоряжении С. Алгоритм действий потерпевшего с банковской картой и банкоматом, в результате которых денежные средства со счета банковской карты переводились бы на счета абонентских номеров, С. планировал сообщить в ходе телефонного разговора с потерпевшим. После этого С. получил бы возможность распоряжаться похищенными указанным способом денежными средствами по своему усмотрению, а именно при помощи системы международных денежных переводов «Юнистрим» осуществлять переводы денежных средств с лицевых счетов абонентских номеров, находившихся в его распоряжении, в различные банки, для их последующего получения наличными и, в том числе, в качестве платежного средства для осуществления расчетов, не снимая денежных средств со счетов абонентских номеров, на который они были бы перечислены в результате мошенничества, а переводя их, по своему усмотрению, на лицевые счета иных абонентских номеров.

Вышеуказанным способом путем обмана С. заставил перевести потерпевших денежные средства в сумме 97403 руб. на счета абонентских номеров, находящихся в его пользовании.

За совершение данного преступления гр. С. осужден к 2 г. 6 мес. лишения свободы с отбыванием наказания в колонии строгого режима.

3. У гр. В. из корыстных побуждений возник преступный умысел на совершение хищений чужих денежных средств путем обмана.

Реализуя свой преступный умысел, направленный на хищение чужого имущества путем обмана, гр. В. по способу совершения мошенничества, который он узнал от неустановленного в ходе следствия лица, путем случайного набора цифр осуществил рассылку текстовых смс – сообщений на абонентские номера, используемые различными ранее незнакомыми В. лицами, денежные средства, которых он планировал похитить путем обмана, **с заведомо для В. ложными, не соответствующими действительности сведениями о том, что их банковская карта заблокирована**. При этом в сообщении в качестве абонентского номера для получения информации указывался абонентский номер, используемый В., и последний планировал, что после получения указанного сообщения пользователь данного абонентского номера, будучи введенный в заблуждение относительно правдивости сведений, содержащихся в сообщении, должен осуществить телефонный звонок В., где он, представившись сотрудником банка, введя в заблуждение позвонившего ему гражданина, под предлогом корректировки работы банковской карты и получения возможности ее дальнейшего использования гражданином, умышленно, из корыстных побуждений, планировал предложить держателю банковской карты пройти к ближайшему банкомату и осуществить ряд операций со своей банковской картой. После получения согласия на осуществление данных действий от потерпевшего, введенного В. в заблуждение, относительно его преступных намерений, последний планировал сообщить в ходе телефонного разговора с потерпевшим алгоритм его действий с банковской картой и банкоматом, в результате которых денежные средства со счета указанного держателя банковской карты переводились бы на счета абонентских номеров, названных В. В результате этого последний получил бы возможность распоряжаться похищенными указанным способами денежными средствами, по своему усмотрению, в том числе в качестве платежного средства для

осуществления расчетов от своего имени или от имени третьих лиц, не снимая денежных средств со счета, на который они были бы перечислены в результате мошенничества.

На сообщение перезвонила жительница г. Ростова-на-Дону гр. Д. и, не подозревая о преступных намерениях В., выполняя инструкции последнего, осуществила операцию по перечислению денежных средств, со счета находящейся в ее пользовании банковской карты на лицевые счета указанных В. абонентских номеров на общую сумму свыше 15 тыс. рублей.

За совершение данного преступления В. осужден к 1 г. 6 мес. лишения свободы с отбыванием наказания в колонии строгого режима.

II. Хищения, совершаемые с помощью сети Интернет и компьютерной техники

Цель финансовых преступлений, совершаемых в компьютерной сети, – получение дохода с помощью компьютерных технологий.

Убеждение, что если человек не говорит никому PIN-код карты и не расплачивается ею в местах, которые имеют сомнительную репутацию, то деньги никуда не пропадут, не безоговорочно. Случаи мошенничества в Интернете встречаются очень часто. И чтобы их избежать, нужно быть предельно осторожным.

Существует так называемый **фишинг** – разновидность сетевого мошенничества, при котором пользователей заманивают на фальшивые сайты, где получают доступ к данным платежных карт с целью хищения денежных средств. Целью фишингов являются клиенты банков и электронных платежных систем. Так, создается сайт, который очень похож на интернет-магазин, где люди расплачиваются своими карточками. Впоследствии на почту пользователю приходит письмо, в котором «администрация» магазина или другого сервиса просит пройти по ссылке и произвести некоторые манипуляции. Нужно это для того, чтобы подтвердить настройки безопасности, или использовать какой-нибудь другой

благовидный предлог. Пользователь проходит по ссылке, попадает на страницу, которая своим дизайном очень похожа на привычный ему сайт, где он раньше что-то покупал. Затем он вводит там свои личные данные. Теперь мошенники могут совершать покупки в Интернете по карточке пользователя. Заявление о мошенничестве подавать бесполезно: найти того, кто проворачивает подобные схемы, практически невозможно. **Обезопасить себя можно достаточно просто.** Не следует переходить по сомнительным ссылкам. Серьезная организация никогда не присылает своим пользователям подобные письма на почту. Кроме того, следует регулярно обновлять свой браузер. Во всех популярных браузерах стоят качественные антифишинговые программы, которые регулярно совершенствуются.

Оплачивать карточкой покупки или услуги в интернет-магазинах и т. п. небезопасно. Недобросовестные сотрудники, имеющие доступ к данным, которые человек водит на сайте при покупке, могут ими воспользоваться. Для этого создаются фиктивные интернет-фирмы. Незадачливым пользователям однажды приходят новости, что с их счета оплатили неизвестную им покупку, причем, возможно, не на территории Российской Федерации. Иными словами, фиктивная фирма продает «воздух», а деньги со счета за его оплату снимаются самые настоящие. Подобные схемы достаточно распространены, поэтому **расплачиваться в Интернете безопаснее при помощи платежных систем, чем используя данные своей карты.**

Следующим этапом развития киберпреступности стал **фарминг** – перенаправление жертвы на ложный IP-адрес. Как и при фишинге, целью фарминга является получение персональных данных клиентов платежных систем. Разница заключается в том, что атака преследует цель перенаправления трафика к веб-сайту в другое место. В результате механизм перенаправления активизируется, когда пользователь набирает адрес, соответствующий его банку, и жертва попадает на один из ложных сайтов.

Одной из разновидностей фишинга является **кардинг**, то есть род мошенничества, при котором производится операция с использованием банковской карты или ее реквизитов, не инициированная или не подтвержденная ее держателем. Реквизиты пластиковых карт кардеры добывают хакерскими способами. То есть взламывают интернет-магазины, платежные системы, персональные компьютеры, похищая конфиденциальную информацию. Для получения нужной информации кардерами активно используется и фишинг, при котором людей самыми разными способами вводят в заблуждение и заставляют регистрироваться на поддельных сайтах. Иными словами, пользователи добровольно передают третьим лицам конфиденциальную информацию.

Вишинг - это еще один из способов украсть деньги со счета. Схема достаточно проста. Незнакомое лицо звонит клиенту банка и представляется служащим. Далее клиенту предлагается в тоновом режиме телефона ввести личные данные якобы для восстановления системы после «сбоя». Доверчивый человек моментально выкладывает номера своих карт и ПИН-коды. При этом упор делается на то, что сделать это нужно максимально быстро. Мошенники не дают времени для размышления. Это заставляет людей забыть о безопасности и делать то, что просят, на кону ведь деньги. После того как человек раскрывает свои данные, вежливый «сотрудник банка» прощается. И в течение определенного времени, как правило, небольшого, средства с карточки исчезают. Это также подпадает под статью 159 УК РФ «Мошенничество». Но обманутому человеку это мало чем поможет. Подавать в полицию заявление о мошенничестве бесполезно. Найти афериста практически невозможно.

Еще одна разновидность кардинга – **скимминг.** Скиммер – это такое устройство, с помощью которого можно перехватывать нужную информацию с магнитных лент на пластиковых карточках. Официально эти устройства появились в 2002 году в Европе. Возможно, они были созданы

гораздо раньше, но до этого года о скиммерах какая-либо информация отсутствовала. Устройство это состоит из двух частей. Первая – поддельный приемник, принимающий банковские карты. Его крепят на банкомате. Используется он для считывания информации с карточек. Если человек давно пользуется услугами определенного банкомата, то ему легко будет обнаружить появившуюся подделку. Но людям, которые подошли к нему в первый раз, сделать это сложно. Поэтому данный способ популярен в местах, где перемещаются большие массы людей. **Как уберечь себя от такого рода мошенничества? Нужно внимательно изучить терминал для банковских карт.** Если банкомат вызывает сомнения (устаревший, расположен на отшибе, имеет необычную форму клавиатуры для ввода данных и прочее), то разумнее воздержаться от проведения операций.

Вторая часть скиммера – поддельная клавиатура. Она нужна для получения информации о ПИН-коде. В клавиатуру встроена микросхема, благодаря которой на телефон мошенников отправляются СМС-сообщения. Определить подделку не так уж и сложно. Такая клавиатура выделятся на плоскости банкомата. Когда человек вводит там свой ПИН-код, он сразу же отправляется мошенникам через СМС. Что делают кардеры с полученной информацией? После того как нужные сведения поступают к мошенникам, они записывают полученную информацию на другую пластиковую карту. Обычно она не имеет каких-либо логотипов и внешнего оформления вообще. Такие карточки называются «белым пластиком». С их помощью злоумышленники снимают деньги в любом банкомате. В редких случаях изготавливаются полноценные подделки существующих банковских карт, которые применяются для оплаты товара в магазинах. Это одна из схем, которой пользуются мошенники. Пластиковые карты такого рода обычно используются один раз, потом их выбрасывают. **Как в таком случае сохранить свои деньги и не стать жертвой мошенников?** Банки стараются заботиться о своих клиентах и регулярно совершенствуют и обновляют оборудование. Сейчас популярны банкоматы, имеющие встроенную защиту

от скиммеров. Работает она следующим образом. Пластиковая карточка принимается банкоматом, а потом устройство ее частично выталкивает наружу. Затем она принимается банкоматом полностью. Такая последовательность нарушает работу скиммеров, и они не могут полноценно считывать данные. **Рекомендуется использовать банкоматы, которые находятся непосредственно рядом с банком. Желательно, чтобы вокруг было много камер видеонаблюдения**. Как уже упоминалось выше, следует очень внимательно осматривать банкомат снаружи. Если что-то показалось подозрительным, то разумнее пойти в другое место. Самое безопасное время для снятия денег – это с 9 утра до 11 дня. Обычно именно в этом промежутке банкоматы проверяют служащие и работники полиции.

Главное и основное правило безопасности в Интернете - аккуратно хранить свои личные данные. Никогда и никому их не передавать и не пересылать по электронной почте. Также следует воздержаться от введения личных данных на сомнительных сайтах. Серьезная организация или платежная система никогда не попросит у пользователя отправлять или размещать где-либо пароли или ПИН-коды открытым текстом.

III. Рекомендации гражданам (Роспотребнадзор):

Что такое электронные платежи и как обезопасить свои электронные деньги?[1]

Даже исчерпывающая информация на просторах всемирной Сети не дает четкого понимания, какие именно деньги — «электронные», и что принято считать «электронными платежами». По результатам опроса, проведенного РОЦИТ на интерактивной площадке «Голос Рунета», 63% уверены в том, что знают, какие платежи являются электронными. Однако при ответе на вопрос, что можно отнести к электронным платежам, мнения разделились: 22% заявили, что это оплата товаров и услуг с помощью электронного кошелька, 20% — банковской карты, 17% — интернет-

[1] Информация, размещенная на официальном сайте Роспотребнадзора от 9 марта т.г.

банкинга. Лишь 1% пользователей правильно отметил, что это оплата любым способом без использования физических денег.

С информацией о том, что такое банковская карта и зачем она нужна, как пользоваться дебетовой картой, на что обратить внимание при оформлении кредитной карты, что представляет из себя национальная платежная система, каковы основные правила платежной безопасности и о том, как контролировать списание денежных средств Вы можете узнать из материалов, расположенных в Государственном информационном ресурсе в сфере защиты прав потребителей (адрес ресурса zpp.rospotrebnadzor.ru).

Безусловно, у электронных платежей очень много плюсов: простота использования, высокая скорость совершения платежей, отсутствие необходимости всегда носить деньги и банковскую карту с собой. Возможно, поэтому лишь 11% респондентов никогда не пользовались услугой электронных платежей.

Опрошенные отметили, что их друзья и знакомые не совершают электронные платежи в связи с тем, что им не хватает знаний и навыков в том, как это делать (27%), а также они опасаются за сохранность своих денежных средств (19%).

С каждым днем все шире и разнообразнее становится спектр товаров и услуг, которые можно оплатить с помощью электронных денег. По данным опроса, чаще всего пользователи используют свой электронный кошелек для оплаты услуг связи (18%), товаров в интернет-магазинах (17%), а также услуг интернет-провайдера (12%).

Иногда проблемы с электронным кошельком возникают у пользователей на этапе его пополнения. Не дошли денежные средства, не прошел платеж, неправильно указал номер электронного кошелька — вот ряд проблем, с которыми сталкиваются пользователи каждый день. Не удивительно, но самые частые проблемы связаны просто с невнимательностью человека.

Для обеспечения безопасности своих электронных денег очень важно пользоваться лицензионными антивирусами, осторожно пользоваться сетями

в общем доступе, не вводить пароли на чужих компьютерах, не записывать и не хранить пароли офлайн.

Рекомендуется иметь отдельную (возможно виртуальную) карту для оплаты покупок в интернете, переводить туда только фиксированную определенную сумму для оплаты текущих покупок.

Крайне рекомендуется настроить SMS-пароли вместо постоянного пароля. В этом случае кража пароля фактически исключена, так как он действителен только на одну операцию.