ISSN 2304-120X
КОНЦЕПТ
научно-методический электронный журнал

Сыпачев А. Ю. Основные способы хищений с использованием сети Интернет // Концепт. – 2015. – № 10 (октябрь). – ART 15349. – 0,4 п. л. – URL: http://e-koncept.ru/2015/15349.htm. – ISSN 2304-120X.

ART 15349 **УДК 344.633**

Сыпачев Андрей Юрьевич,
кандидат юридических наук, старший преподаватель кафедры оперативно-разыскной деятельности и оперативно-технических мероприятий органов внутренних дел ФГКОУ ДПО «Тюменский институт повышения квалификации сотрудников МВД России», г. Тюмень
brig094@mail.ru

Основные способы хищений с использованием сети Интернет

Аннотация. *В статье рассматриваются наиболее распространенные виды хищений чужого имущества или приобретения прав на чужое имущество путем обмана или злоупотребления доверием с использованием сети Интернет, а также указаны причины недостаточно высокой эффективности деятельности подразделений органов внутренних дел по раскрытию и расследованию указанных видов преступлений.*
Ключевые слова: *компьютерные преступления, интернет мошенничество, обман или злоупотребление доверием.*
Раздел: *(03) философия; социология; политология; правоведение; науковедение.*

Качественные показатели, характеризующие современную преступность в Российской Федерации, говорят о том, что она активно осваивает и использует достижения технического прогресса и новых информационных технологий. Наибольшей распространенностью в последнее время пользуется интернет-мошенничество и хищение денежных средств с банковских счетов физических лиц с помощью компрометации систем дистанционного банковского обслуживания[1].

Рассмотрев ряд вышеуказанных преступлений, можно сделать вывод о том, что в большинстве случаев данные преступления остаются незаявленными, так как преступники, совершая хищение денежных средств, в основном похищают не значительные для граждан суммы. Поэтому в каждом втором случае граждане просто не замечают пропажу денежных средств со своей банковской карты, а даже если и обнаруживают таковую, то только двое из десяти обращаются в полицию или банк. Также необходимо отметить, что каждое четвертое преступление совершено лицами, не достигшими двадцатипятилетнего возраста, так как они активно изучают информационные технологии и компьютерные программы, пользуются мобильными телефонами с различными операционными системами, планшетными и портативными компьютерами.

Такое состояние дел в очередной раз поднимает вопрос об эффективности российской правоприменительной системы в отношении преступлений в сфере компьютерной информации, поэтому в данной статье мы рассмотрим отдельные виды хищений чужого имущества или приобретения прав на чужое имущество путем обмана или злоупотребления доверием с использованием сети Интернет.

К наиболее распространенным видам указанного мошенничества можно отнести:

– использование потерянных/украденных банковских карт, когда владелец или банк своевременно их не блокирует;

[1] Компрометация – факт доступа постороннего лица к защищаемой информации, а также подозрение на него. Чаще всего рассматривают компрометацию закрытого ключа, закрытого алгоритма, цифрового сертификата, учётных записей (паролей), абонентов или других защищаемых элементов, позволяющих удостоверить личность участника обмена информацией.

– запись полученной незаконным путем информации о чужой карте на магнитную полосу поддельной или подлинной карты;

– заказ различных товаров и услуг с использованием данных банковской карты, лицом, не являющимся ее владельцем;

– использование чужого банковского счета кредитной или дебетовой карты лицом, получившим доступ к этому счету незаконным путем;

– использование банковских карт, не полученных ее владельцами (например, хищение новой или повторно выпущенной карты при пересылке ее законному держателю);

– указание ложных данных в заявлении на получение карты;

– двойную прокатку карт (сговор торгово-сервисных предприятий, предусматривающий многократную прокатку платежной карты с получением дополнительных копий слипов[2], используемых впоследствии в мошеннических целях);

– использование реквизитов карты, полученных незаконным путем, для транзакций в виртуальной среде. Номер карты мошенники получают различными путями, включая кражу из компьютерной системы торговой точки в сети Интернет, не имеющей необходимых средств безопасности для предотвращения несанкционированного доступа.

Также необходимо отметить и такой вид мошенничества, как фишинг[3]. Его целью является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Он достигается путём проведения массовых рассылок электронных писем от имени популярных торговых марок, которые в представлении потребителя имеют определенные характерные ценные свойства и атрибуты, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом[4]. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам[5] и банковским счетам.

Самым распространенным видом фишинговых сайтов является создание копий банковских сайтов. Схемы преступлений в таких случаях выглядят следующим образом:

1. Клиент банка, пытаясь зайти на сайт онлайн-банка, как правило, попадает на страницу, на которой указано, что в данный момент на сайте ведутся технические работы и его просят ввести свой номер телефона вместо SMS-подтверждения.

После этого ему начинают приходить SMS-сообщения о переводе средств с его банковской карты, затем звонят якобы из технической поддержки данного банка и сообщают о том, что произошли ошибочные операции, и просят продиктовать логин, пароль и SMS-код для отмены операции. Клиент предоставляет необходимую информацию, и мошенники получают доступ к его банковскому счету.

---

[2] Слип – документ (чек), подтверждающий проведение по банковской карте операций, совершенных с помощью механического устройства. Обычно представляет собой трехслойные самокопирующиеся бланки.

[3] Фишинг – одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности: в частности, многие не знают простого факта: сервисы не рассылают писем с просьбами сообщить свои учётные данные, пароль и т. п.

[4] Редирект – автоматическое перенаправление пользователей с одного сайта на другой. Выглядит это следующим образом: пользователь набирает в адресной строке браузера один адрес, а оказывается на сайте, адрес которого совсем другой.

[5] Аккаунт – хранимая в компьютерной системе совокупность данных о пользователе, необходимая для его опознавания и предоставления доступа к его личным данным и настройкам.

ISSN 2304-120X
КОНЦЕПТ
научно-методический электронный журнал
Сыпачев А. Ю. Основные способы хищений с использованием сети Интернет // Концепт. – 2015. – № 10 (октябрь). – ART 15349. – 0,4 п. л. – URL: http://e-koncept.ru/2015/15349.htm. – ISSN 2304-120X.

2. Клиент банка, находясь на копии сайта, выполняет различные операции (например, пополнение счета абонентского номера, оплата различных услуг, перевод денежных средств на другой счет и т. п.). После ввода своих логина и пароля, которые он использует для доступа, они становятся известны мошенникам, последние же, в свою очередь, получают возможность списания денежных средств с банковской карты.

Рассмотрим несколько вариантов совершения хищений денежных средств с использованием сети Интернет:

Вариант 1

Злоумышленник совершает ряд звонков на мобильные либо стационарные номера (обычно данные действия совершаются путем случайного набора номеров, выбирается код города, например 8-3452, далее следует ряд номеров 22-22-22, 22-22-23, 22-22-24 и т. д.). Далее мошенник представляется сотрудником полиции и сообщает, что родственник потенциальной жертвы совершил какое-либо правонарушение или преступление и для того, чтобы решить вопрос, срочно нужны деньги. Также он может представляться сыном или дочерью потерпевшего и сообщить, что у него (ней) неприятности и ему (ей) срочно нужны деньги. В основном злоумышленник, учитывая психологию человека, совершает звонки в ночное время, так как человек, получив в такое время информацию о том, что близкий человек попал в беду, начинает сразу же совершать действия по перечислению либо физической передаче денежных средств и ценностей.

В данном преступлении у преступника есть два варианта хищения денежных средств:

– злоумышленник предлагает потенциальной жертве отправить денежные средства через банкомат либо терминал оплаты на указанный им абонентский номер, номер лицевого счета, номер онлайн-кошелька;

– злоумышленник предлагает передать ему денежные средства в указанном месте.

Как правило, совершая транзакцию[6] денежных средств, злоумышленник пытается скрыть данные денежные средства на зарубежных лицевых счетах. Например, похищенные денежные средства были направлены потерпевшим на абонентский номер 8-908-999-22-33, с данного абонентского номера денежные средства направлены злоумышленником с использованием мобильного банка на онлайн-кошелек или банковский счет 2222 3333 4444 5555. После этого на каком-либо сайте приобретен товар на похищенную сумму; далее злоумышленник со счета 2222 3333 4444 5555, на который ранее были переведены денежные средства, переводит их на счет сайта, с которого они переходят продавцу. Однако согласно условиям такого приобретения товара в течение указанного времени покупатель вправе отказаться от него, чем и пользуется злоумышленник, отказываясь от товара. Затем он указывает счет, на который необходимо перевести денежные средства, перечисленные им ранее за товар 5555 6666 7777 8888.

Таким образом, преступник может получить похищенные денежные средства в виде банковского перевода на свой счет либо повторив данную операцию с подставными счетами два раза и более.

Во втором рассматриваемом варианте данного преступления действия злоумышленника не изменяются за исключением того, что похищенные денежные сред-

[6] Транзакция – операция держателя банковской карты с использованием электронного счета. Транзакция осуществляется держателем электронной карты и предполагает процесс оплаты счета, перевода денежных активов или получения наличных денег.

ства потерпевший передает посреднику (например, когда отказывается лично перечислять денежные средства, мотивируя тем, что не умеет пользоваться банкоматом либо терминалом, или их отсутствием). В данном случае мошенник заказывает такси на указанный жертвой адрес, после чего водитель такси, получив денежные средства, увозит их в указанное злоумышленником место и совершает операцию по перечислению денежных средств за отдельное вознаграждение либо без такового.

Вариант 2

Прежде чем рассмотреть преступления, связанные с хищением денежных средств с банковских карт, необходимо отметить, что сотрудники различных организаций, а также держатели банковских карт сами создают благоприятные условия для преступника (например, во многих организациях существует бесплатное подключение к сети Интернет, не требующее регистрации, также наблюдается небрежное отношение и несоблюдение мер безопасности при использовании гражданами банковских карт). Поэтому в ряде случаев при проведении мероприятий, направленных на раскрытие и расследование данного вида преступлений, сотрудник полиции зачастую может получить ответ, что злоумышленник совершал выход в сеть Интернет с использованием Wi-Fi-соединения в каком-либо кафе или в непосредственной близости от него на расстояний сигнала Wi-Fi-роутера[7]; в данных случаях приходится проводить дополнительные мероприятия, при этом, как мы уже отмечали ранее, время работает на преступника.

Рассмотрим вариант хищения денежных средств с банковской карты, которая имеет привязку к абонентскому номеру, с участием потенциальной жертвы и без таковой.

Для хищения денежных средств с банковской карты злоумышленник, как и в любых других случаях, будет вынужден воспользоваться Интернетом. У преступлений данного типа имеется особенность: злоумышленнику необходимо знать лицевой номер банковской карты, в данном случае, как и было нами отмечено ранее, благоприятные условия создают сами содержатели банковских карт (например, утраченная, но незаблокированная банковская карта, оставленная в магазине или в банкомате и т. д.). Последующие действия злоумышленника настолько просты, что хищение он может совершить в течение пяти минут после того, как получил номер банковской карты.

Злоумышленник осуществляет покупку товаров в сети Интернет, указывая при этом номер банковской карты (PIN-код для выполнения данной операции не требуется), в последующем он отказывается от товара и начинает транзакцию денежных средств по фиктивно созданным счетам или мобильным счетам, которые в сети не зарегистрированы.

При совершении хищения напрямую через онлайн-магазины владельцу банковской карты поступает SMS-уведомление, о том, что заказ оплачен на сайте.

Необходимо отметить, что именно подключение абонентского номера к банковской карте является уязвимым местом, чем в большинстве случаев и пользуется злоумышленник.

Например, мошенники моделируют звонок автоинформатора, получив который держатель карты получает информацию о том, что с его картой производятся мошеннические действия и необходимо немедленно перезвонить по определенному номеру. Злоумышленник, принимающий звонки по указанному автоинформатором номеру, представляется сотрудником какой-либо финансовой организации, просит пройти сверку данных и ввести 16-значный номер карты с клавиатуры телефона. Как только

[7] Роутер – специализированный сетевой компьютер, имеющий два или более сетевых интерфейса и пересылающий пакеты данных между различными сегментами сети.

номер введен, злоумышленник становится обладателем всей необходимой информации (номер телефона, полное имя, адрес), затем, используя этот звонок, можно собрать и дополнительную информацию, такую как PIN-код, срок действия карты, дата рождения, номер банковского счета и т. п.

В последнее время, используя базы данных компаний мобильной связи, злоумышленники массово рассылают SMS примерно следующего содержания: «Ваша карта заблокирована. Для разблокировки необходимо позвонить по номеру....», естественно, указывается номер телефона мошенника. Некоторые граждане, вместо того что бы сразу обратиться в ближайший офис своего банка для проверки поступившей информации либо позвонить в службу клиентской поддержки, перезванивают по указанному в SMS номеру.

Мошенник представляется «сотрудником банка» или «отдела безопасности банковской системы платежей и переводов». Под предлогом разблокирования карты злоумышленник выясняет у гражданина, подключена ли к его счету услуга «Мобильный банк», и, если такая услуга подключена, мошенник обманным путем получает у владельца номер банковской карты, срок ее действия и персональный код. Затем под предлогом разблокирования и «с согласия» владельца на осуществление операций по карте и через Интернет похищает деньги с его счета путем безналичного перевода на другие счета.

Если же услуга «Мобильный банк» не подключена, мошенник в ходе телефонного разговора предлагает гражданину подойти к ближайшему банкомату и осуществить ряд неких операций, вводя его в заблуждение и переводя деньги на абонентские номера телефонов сотовой связи либо на другие банковские счета.

Такое мошенничество становится возможным только из-за того, что многие граждане не знают, что ни одна организация, включая банковские, не вправе требовать PIN-код или реквизиты банковской карты.

Раскрытие рассматриваемых нами преступлений невозможно без проведения комплекса оперативно-разыскных мероприятий [1], большинство из которых требует судебного санкционирования [2, 3].

В заключение хотелось бы отметить, что, на наш взгляд, причинами недостаточно высокой эффективности деятельности подразделений органов внутренних дел по раскрытию и расследованию указанных видов преступлений, являются:

– некомпетентность сотрудников полиции в юридической и технической стороне таких преступлений;
– слабая научно-техническая оснащенность полиции;
– низкая эффективность проведения отдельных мероприятий в сети Интернет.

Ссылки на источники

1. Алгазин И. И., Бакланов Л. А., Бражников Д. А., Бычков В. В., Панюшин Д. Б., Сайфиев М. Д., Сыпачев А. Ю. Правовые основы оперативно-розыскной деятельности: курс лекций. – Тюмень, 2012.
2. Бакланов Л. А. Получение судебного разрешения на гласное обследование жилища // Юридическая наука и правоохранительная практика. – 2011. – № 4. – С. 86–90.
3. Бакланов Л. А. Гласное обследование жилища в случаях, которые не терпят отлагательства // Современное право. – 2011. – № 8. – С. 124–127.

Andrew Sypachev,
Candidate of Law Sciences, senior lecturer at the chair of Investigative and Special Technical Action, Tumen Advanced Training Institute of the Interior Ministry of the Russian Federation, Tumen
brig094@mail.ru
The main methods of theft using the Internet

ISSN 2304-120X
КОНЦЕПТ
научно-методический электронный журнал

Сыпачев А. Ю. Основные способы хищений с использованием сети Интернет // Концепт. – 2015. – № 10 (октябрь). – ART 15349. – 0,4 п. л. – URL: http://e-koncept.ru/2015/15349.htm. – ISSN 2304-120X.

Abstract. The paper discusses the most common types of theft of another's property or buying another's property by deception or abuse of trust using the Internet, as well as the reasons for not sufficiently high efficiency of the law-enforcement bodies to disclose and investigate these types of crimes.

Keywords: computer crimes, internet fraud, deception or abuse of trust.

References

1. Algazin, I. I., Baklanov, L. A., Brazhnikov, D. A., Bychkov, V. V., Panjushin, D. B., Sajfiev, M. D. & Sypachev, A. Ju. (2012) *Pravovye osnovy operativno-rozysknoj dejatel'nosti: kurs lekcij*, Tjumen' (in Russian).
2. Baklanov, L. A. (2011) “Poluchenie sudebnogo razreshenija na glasnoe obsledovanie zhilishha”, *Juridicheskaja nauka i pravoohranitel'naja praktika*, № 4, pp. 86–90 (in Russian).
3. Baklanov, L. A. (2011) “Glasnoe obsledovanie zhilishha v sluchajah, kotorye ne terpjat otlagatel'stva”, *Sovremennoe pravo*, № 8, pp. 124–127 (in Russian).

Рекомендовано к публикации:
Горевым П. М., кандидатом педагогических наук,
главным редактором журнала «Концепт»

ISSN 2304-120X

Поступила в редакцию *Received*	14.08.15	Получена положительная рецензия *Received a positive review*	17.08.15
Принята к публикации *Accepted for publication*	17.08.15	Опубликована *Published*	30.10.15

www.e-koncept.ru