Общероссийская общественная организация
"Российская академия естественных наук"

ФИНАНСОВОЕ МОШЕННИЧЕСТВО В СЕТИ ИНТЕРНЕТ

Лекция подготовлена в рамках социально значимого Президентского проекта по Созданию системы распространения знаний по вопросам экономической и финансовой безопасности России, борьбы с теневыми доходами, противодействию финансирования терроризма, экстремизма, антигосударственной и деструктивной деятельности и ее апробации в четырех пилотных регионах (№ 244/79-3).

INTERNET FRAUDS

The lecture created within socially important President Project to establish knowledge system in economical and finance safety in Russia, to confront shadow gains, terrorism, extremism, anti-governmental activity and its approbation in four pilots regions (№ 244/79-3).

Москва
2016

УДК 37.032

Волков С.Е., Глотов В.И. под общей редакцией Каратаева М.В.

Финансовое мошенничество в сети Интернет / редкол.: Каратаев М.В (отв. ред) [и др.] – Москва. – 20 стр.

Лекция посвящена вопросу мошенничества в сети Интернет. Рассмотрены основные методы, используемые мошенниками, такие, как фишинг, псевдо-акции брендов, «заливы» на кошельки и банковские карты, обналичивание, обмен валют, краудфандинг, письма счастья, нигерийские письма, брачная афера, опросы, розыгрыш призов, авторитетная личность, прогноз на исход события, покупки в интернет-магазинах, интернет-аукционы. Для каждого метода рассмотрены основные методы избежать встречи с мошенниками в сети Интернет.

Адресована широкому кругу читателей для повышения уровня финансовой грамотности по вопросам мошенничества в сети Интернет.

УДК 37.032

The lecture is devoted to Internet Fraud. The common methods of frauds are examined: fishing, brand fake-shares, wallets nad credit cards refillings, cashing-out, currency excnahge, crowdfunding, chain mail, Nigerian scam, marriage fraud, surveys, prize drawing, bookmaking, internet purchasing, internet auction. The common ways of avoiding the fraud are examined.

It is addressed to a wide specter of readers to enlight them in Internet fraud issue.

Аннотация. В лекции проведен анализ основных способов обмана граждан в сети Интернет, который используют мошенники. На основе результатов сформулированы способы избежать встречи с мошенниками.

Ключевые слова: финансовое мошенничество, финансовая безопасность, Интернет.

Abstract. The lecture analyzes the common fraud methods via Internet used by the criminals. The results are the ways of avoiding the criminal actions.

Keywords: financial fraud, financial security, Internet.

Рынок электронных платежей в России растет примерно на 30 процентов ежегодно, и вместе с ним увеличивается число интернет-махинаций. Тысячи людей ежедневно становятся жертвами сетевых аферистов, которые изобретают все новые и новые способы отъема денег у населения.

Согласно обзору Банка России, за 2014 год со счетов граждан незаконно списывали деньги 300 тыс. раз, общая сумма ущерба составила 3,5 млрд. руб. С карточек мошенники списали 1,58 млрд. руб., причем в 68% случаев для проведения транзакций мошенники использовали реквизиты чужих карта, в 21% случаев злоумышленники изготавливали поддельные карты, 11% несанкционированных списаний произошли по утерянным и украденным картам.

Большую часть суммы (свыше 1 млрд. руб.) мошенники украли через интернет-банк и мобильное приложение. Объем неправомерных транзакций, совершаемых через дистанционные каналы обслуживания, вырос на 44,8%[1].

По статистике, наиболее частой причиной преступлений в интернете становится банальная невнимательность пользователей, либо недостаток знаний о правилах безопасности. Большинство случаев мошенничества построены на использовании человеческой жадности и желании заработать легких денег. И сколько бы ни говорили о том, что обогатиться моментально невозможно, все новые и новые соискатели попадаются на удочку злоумышленников.

В связи с этим необходимо рассмотреть наиболее часто встречающиеся схемы мошенничества в сети интернет.

Фишинг**.** Данный вид мошенничества направлен на получение у пользователя секретных данных (PIN-коды кредитных карт, пароли от социальных сетей и учетных записей и пр.).

Фишинг-сообщения, в большинстве случаев, выглядят внешне похожими на уведомления от платёжных систем, банков, популярных веб-сервисов, и в них пишется о необходимости предоставить данные для входа на сайт, ввиду проблем на сервере или сбоем системы, активировать свою учетную запись путем отправки SMS на короткий номер, за которое пользователь заплатит деньги, ввести на предоставленном по ссылке сайте свои данные, которые мошенники легко могут скопировать и т.д. Ссылка, естественно, ведёт не на сайт настоящего веб-сервиса, а на его клон, созданный интернет-мошенниками.

Фишинговые сайты, которые используются мошенниками для обмана людей, как правило, имеют дизайн, схожий с дизайном официального сайта платёжных систем, банков, интернет-бирж и прочих веб-сервисов, где водятся электронные деньги. Отличить такой клон можно по доменному имени, которое будет разниться с оригинальным, правда, часто всего лишь одной какой-то буквой. Введите на сайте http://www.odnoklassniki.ru/ свой логин и пароль от одноклассников и его сразу узнают мошенники.

Воровство аккаунтов социальных сетей, различных интернет-бирж, сайтов знакомств, Skype, ICQ и прочих интернет-мессенджеров – вещь неприятная. Однако с куда большими неприятностями можно столкнуться в случае воровства денег с электронных счетов. Счета систем онлайн-банкинга и кошельки платёжных систем серьёзно защищены. И вряд ли мошенники могут справиться с системой безопасности банков и платёжных систем. Потому проще конфиденциальные данные доступа к электронным деньгам – логины, пароли, PIN-коды и прочее – выведать у самих пользователей. Для этих целей и придуманы различные схемы интернет-мошенничества.

В качестве мотивации пользователя используются различные психологические трюки, например «Зафиксирована попытка несанкционированного входа в ваш аккаунт, вам нужно подтвердить свои данные». Главная задача мошенников – вызвать чувство страха в человеке или заставить его любым иным обманным способом выложить свои данные доступа к электронным деньгам.

Фишинг находится в постоянном развитии, и мошенники оттачивают своё мастерство, изучая принципы работы финансовых онлайн-систем, изобретая всё новые психологические подходы к доверчивым пользователям Интернета. Если ранее интернет-мошенники для фишинга использовали в основном электронную почту, то сегодня по количеству фишинговых предложений лидируют социальные сети.

Псевдо-акции брендов. Разновидностью фишинга являются так называемые псевдо-акции брендов. При этой схеме интернет-мошенничества у пользователей их

конфиденциальные данные выведываются с использованием имени известного бренда, которому доверяют массы.

Например, несколько лет назад от имени McDonald's мошенники разослали пользователям Интернета предложение поучаствовать в социальном опросе касательно качества обслуживания в точках McDonald's. За участие в таком опросе обещалось вознаграждение в размере $80. Электронный адрес мошенников был схож с настоящим - mcdonalds@mcdonaldss.com. Одна лишняя буква «s» практически незаметна.

Веб-опросник содержал, помимо стандартных вопросов о качестве обслуживания в точках общепита, дополнительную графу о необходимости указания номера банковской карты и кода доступа к ней в целях перечисления обещанной платы за участие в опросе. Все те, кто попали на удочку мошенников, конечно же, не получили никаких $80. Жертвам пришлось расстаться со всеми своими деньгами, причём в некоторых случаях и с кредитными.

«Заливы» на кошельки и банковские карты**.** Этот способ выманивания денег сегодня набрал неимоверные обороты. На различных досках объявлений и в социальных сетях можно увидеть такие предложения «Залив на карту (кошелек) любой суммы. Деньги из игорного бизнеса. Вывожу через посторонних лиц, за что плачу 50%». Как и в большинстве случаев, злоумышленники предлагают получить круглую сумму денег всего за один клик.

«Залив на карту» - сленговое название мошеннической операции по отмыванию украденных денег. На самом деле, под этим термином понимают два вида мошенничества: действительный «залив» (встречается редко) и обман принимающего платеж «так называемая «предоплата» или «проверка баланса».

В обоих случаях неизвестный человек предлагает очень выгодную операцию. По его словам, на банковский счет получателя поступит некая, обычно довольно крупная сумма денег (несколько сот тысяч рублей), которую надо снять в банкомате и разделить на две части (обычно пополам). Первую часть отправить на другой счет (или на электронный кошелек), а вторую – оставить себе в качестве вознаграждения.

Удержаться от того, чтобы не несколько минут «заработать» пару-тройку сотен тысяч рублей, крайней сложно, особенно если у человека есть проблемные кредиты или просто сложности с деньгами. Поэтому многие соглашаются, не понимаю, что и зачем делают.

Смысл этой операции – в «отмывании» ранее украденных средств. Деньги жертве перечисляются с взломанного счета или с использованием украденных данных банковской карты. Пропустив их через свой счет, жертва становится главным,

подозреваемым в этих преступлениях, а реальный преступник получит уже «отмытые» деньги, скорее всего на анонимный электронный кошелек или безопасный счет.

В этом «криминальном бизнесе» роли четко распределены: одни преступники незаконно получают доступ к счетам, другие непосредственно проводят переводы, третьи находят лиц, согласных принять деньги на свои счета, и т.д., они не знакомы между собой и часто живут в разных странах.

Однако наиболее распространен другой вид мошенничества, своего рода производная от настоящего «залива». В данной схеме жертве предлагается сделать «предоплату» в счет будущего дохода около 5-10% от суммы. При этом для большего доверия жертва проводит предоплату якобы не самому преступнику, а «гаранту», посреднику. Естественно гаранта не существует или он в сговоре с преступником. Как только жертва перечисляет несколько десятков тысяч рублей операция заканчивается.

Второй вариант этого типа мошенничества – получение доступа к карте самой жертвы. Человеку предлагается получить новую банковскую карту и положить на нее некую относительно небольшую сумму (5-10 тысяч рублей) под предлогом того, что для приема крупного платежа на карте должен быть положительный баланс. После чего жертву вводят в состояние стресса и выманивают секретные данные этой карты «для проверки баланса», включая коды, которые приходят на сотовый телефон. Понятно, что как только доступ к карте и кодам получен, она обнуляется, а жертва будет очень долго ждать крупного перевода.

Обналичивание PayPal через QIWI. В интернете часто можно найти объявления по типу «Срочно нужны «обнальщики» PayPal через QIWI. Без предоплат, без выставленных счетов, без оплаты комиссий за перевод. Прибыль делим поровну - 50/50, возможно до 200 000 руб. От вас требуется адекватность и умение пользоваться QIWI. Все вопросы e-mail, vk, Skype».

Суть данной схемы мошенничества заключается в следующем.

С целью притупить бдительность мошенники в разговоре с жертвой объясняют схему заработка, используя при этом многочисленные финансовые термины, которая сводится к следующим простым действиям:

1. завести кошелек в системе QIWI;
2. положить на кошелек определенную сумму денег;
3. установить на кошелек специальный скрипт.

При этом жертву убеждают в необходимости совершить действия под пунктами 2 и 3, объясняя это необходимостью «автоматизации операций обмена» или тем, что «PayPal не будет автоматически работать с пустым кошельком».

В итоге, деньги с кошелька QIWI воруются мошенником с помощью установленного жертвой скрипта, который был разработан исключительно с этой целью.

В подобных ситуациях всегда выручает логика. Схемы, системы и методы переводов электронных «валют» друг в друга, включая их обналичивание, уже давно разработаны и действуют долгие годы. Искать специальных людей и платить им за совершение подобных операций, это примерно то же самое, как искать человека, который сможет обменять рубли на какую-либо другую валюту по курсу какого-либо банка, учитывая, что это вполне можно сделать самостоятельно.

Обмен валют. В продолжение темы обмена валют друг на друга, существуют, также, и другие схемы мошенничества. В данном случае речь не пойдет о биржах по типу Forex.

Ни для кого не секрет, что валюты обмениваются друг на друга где-то по одному курсу, где-то по другому, в том числе и электронные «валюты» не всегда обмениваются по курсу один к одному. Кажется, что на этой разнице обмена можно заработать, и именно на этом построены схемы мошенничества, речь о которых пойдет ниже.

Существует несколько видов схем:

1. Жертве предлагают заработок, основанный на обмене валют. Для этого необходимо зарегистрировать кошелек, через который будут проходить некоторые сделки, а жертве начисляться определенный процент с этих сделок. Целью данный схемы мошенничества является получение в свое распоряжение кошелек, зарегистрированный на реального человека, через который можно проводить сомнительные операции, подтверждаемые жертвой, и которые однажды могут стать объектом пристального внимания, в том числе и правоохранительных органов.

2. Жертве предлагают установить некое программной обеспечение, осуществляющее мониторинг курсов обмена валют и подбирающее наиболее выгодное предложение по интересующему запросу. Чаще всего данное программное обеспечение содержит в себе вирусы. После установления программы на компьютер жертвы мошенник может действовать несколькими способами:

    1) воспользоваться программой как вирусом и украсть все пароли и иные личные данные, необходимые для кражи денежных средств со счетов и электронных кошельков;
    2) использовать компьютер жертвы в иных своих интересах;
    3) использовать программу в соответствии с ее прямым назначением: через какое-то время программа демонстрирует, что нашла очень выгодный курс для обмена валюты, как правило предложение ограничено по времени.

Разумеется, предложение ведет на сайт и кошелек мошенников, и в обмен на денежные средства жертва не получает ничего;

4) сочетание вышеуказанных способов.

3. Вариации вышеуказанных способов. Жертве могут предложить поменять валюту по определенному курсу, или просят помочь обменять WebMoney на Яндекс.Деньги. При переводе средств на указанный кошелек, обратного обмена не происходит.

Мошенники представляются работниками банка. Жертва размещает объявление о продаже какого-либо товара на одном из популярных сайтов объявлений и становится прицелом для мошенников.

Звонит покупатель и говорит, что готов приобрести продаваемую вещь. Далее он сообщает, что находится в другом городе и готов произвести оплату на карту, а за покупкой отправит курьера из транспортной компании. Жертва пересылает мошеннику номер своей банковской карты, а также все паспортные данные, так как они нужны транспортной компании.

Через некоторое время на телефон жертвы поступает звонок с официального номера банка, в котором он обслуживается, звонивший представляется сотрудником службы безопасности банка и сообщает примерно следующее: «На ваш счет поступил перевод в размере (называет сумму). Так как сумма большая, требуется подтверждение. Вам на телефон была отправлена SMS с кодом подтверждения. Если вы мне её назовете, то сумма сейчас зачислится на ваш счет». В случае, если жертва поверила, то она предоставляет всею информацию мошеннику, после чего все деньги с карты исчезают.

На вопрос, может ли мошенник позвонить, прикрываясь номером банка, да так, чтобы и при обратном звонке, и в детализациях звонков был указан именно официальный номер, представители сотовых компаний не скрывают, что такое технологически сделать можно.

Краудфандинг**.** В Интернете могут появиться объявления от благотворительной организации, детского дома, приюта с просьбой о материальной помощи больным детям. Злоумышленники создают сайт-дублер, который является точной копией настоящего, меняют реквизиты для перечисления денег. Часто для перевода денежных средств используются современные системы платежей, такие как электронные кошельки, платежные терминалы, мобильные платежи и др. способы оплаты.

Для того, чтобы не оказаться вовлеченным в данную мошенническую схему стоит проверить организацию, занимающуюся собором средств, уточнить номер расчетного счета, либо посетить организацию лично, убедиться в достоверности размещенной

информации, выяснить все подробности дела и только после этого принимать окончательное решение о пожертвовании средств.

Письма счастья**.** Потенциальной жертве приходит письмо, как правило, составленное на английском языке, о том, что она выигрывала в лотерею или у нее умер дальний родственник, у которого не было ни жены, ни детей и жертва является ближайшим наследником и т.д. Пишущий чаще всего представляется адвокатом из США, Великобритании и т.д. Однако для того, чтобы получить деньги необходимо выслать свои данные, заполнив простую анкету – ФИО, год рождения, номер паспорта, адрес, семейное положение, место работы, номер карты/счет, куда можно перевести деньги и т.д. После отправки данных жертве приходит письмо-подтверждение их получение, а также с известием о том, что в настоящее время оформляется перевод денежных средств, однако для завершения процедуры перевода необходимо внести $100, $500 и т.д. для покрытия расходов по переводу денег, оплаты комиссии банку и пр. При этом, взять деньги из «причитающейся» суммы они не могут. В качестве варианта предлагают самостоятельно забрать денежные средства в США, Великобритании (в зависимости от того, адвокатом из какой страны представился мошенник), что, по понятным причинам, сложнее и дороже, чем просто перевести небольшую сумму в счет покрытия издержек, связанных с оформлением перевода. После перевода указанной «адвокатом» суммы никакие денежные средства на счет жертвы не поступают.

Нигерийские письма. Нигерийские письма – распространенный вид мошенничества, получивший наибольшее развитие с появлением массовых рассылок по электронной почте (спама). Письма названы так потому, что особое распространение этот вид мошенничества получил в Нигерии, причем еще до появления Интернета, когда такие письма распространялись по обычной почте.

Так, с целью отнять электронные деньги у жертвы мошенники присылают письмо с витиеватой историей о том, что они являются бывшими высокопоставленными чиновниками/весьма состоятельными людьми и т.д., которые из-за финансовой нестабильности в Нигерии не могут обналичивать денежные средства. Просьба помочь обналичить деньги сопровождается довольно заманчивым предложением получить вознаграждение за сделку в размере 10-30% от суммы, которую жертва нигерийского письма обналичит. Для этого жертве необходимо предоставить доступ ко счету в банке или электронному кошельку. Если жертва сделает такой опрометчивый поступок, естественно, все её электронные деньги вместе с «нигерийскими богачами» бесследно исчезнут.

Существуют также и другие сюжеты данного вида мошенничества. Распространенным вариантом, также, являются письма, якобы, от работника банка или чиновника, узнавшего о недавней смерти очень богатого человека «с такой же фамилией», как у получателя письма, с предложением оказать помощь в получении денег с банковского счета умершего человека.

Речь в письмах обычно идет о суммах в миллионы долларов, и получателю обещается немалый процент от суммы – иногда до 40%. Мошенничество организовано профессионально: у мошенников есть офисы, работающий факс, собственные сайты и попытка получателя письма провести самостоятельное расследование не обнаруживает противоречий в легенде.

Если получатель письма отвечает мошенникам, ему посылают несколько документов. При этом используются подлинные печати и бланки крупных фирм и правительственных организаций. Затем у жертвы просят деньги на сборы, постепенно увеличивая суммы сборов для обналичивания, или на взятки должным лицам, или могут, например, потребовать положить 100 тысяч долларов в нигерийский банк, мотивируя от имени сотрудников банка, что иначе перевод денег запрещен.

Часто в ходе вымогательства мошенники используют психологическое давление, уверяя, что нигерийская сторона, чтобы заплатить сборы, продала все свое имущество, заложила дом и т.д.

Разумеется, обещанных денег жертва в любом случае не получает: их просто не существует.

Сравнительно недавно появились и российские аналоги «нигерийских писем», в которых переписка ведется от лица несуществующего «российского бизнесмена», якобы нуждающегося в помощи адресата в переводе своего огромного состояния из России в другую страну за щедрое вознаграждение.

Брачная афера. Не встретив в реальной жизни свою половину, многие мужчины продолжают искать ее в Интернете. Поиски начинаются на сайтах знакомств и дневниках, где будущие избранницы размещают свои фотографии.

Этим пользуются злоумышленники, используя фото девушек, привлекая психологов, программистов, переводчиков и посредством этих сайтов завязывают переписку с доверчивыми иностранцами.

Западные женихи «клюют» на объявления, где нетребовательные русские красавицы говорят о том, что нуждаются в серьезных отношениях. А взамен вечной любви, порой после месяцев переписки, просят решить их финансовые проблемы - помочь

обеспечить сиделкой больных родителей, расплатиться с кредитом, перевести деньги на перелет к жениху в дальнее зарубежье и т.д.

После получения денег невесты перестают выходить на связь. Пылкие иностранные поклонники, поняв, что их обманули, обращаются в полицию. Злоумышленники рассчитывают только на женихов из дальнего зарубежья, т.к. представители ближнего зарубежья предпочитают приехать в гости к невесте сами, что невыгодно для мошенников.

Женская половина также нередко страдает от подобных схем мошенничества. В данном случае войдя в доверие «зарубежный» поклонник высылает девушке небольшой сувенир, однако для того, чтобы его получить нужно оплатить доставку. Деньги, как уверяется, будут возвращены. На почту жертве даже приходит письмо от службы доставки с подтверждением получения посылки, однако для ее получения нужно перевести сумму на указанный счет. После оплаты указанной суммы могут потребовать оплатить еще и место на складе, так как отправитель этого не сделал. Итог у этой истории один – ни денег, ни подарка, ни возлюбленного девушка так и не дожидается.

Набор текстов или иная несложная удаленная работа. В интернете периодически появляются предложения об удаленной работе, связанной с набором текста, каких-либо специальных требований к кандидату не предъявляется, кроме наличия доступа в интернет. Работа заключается в перенесении текста с бумажного носителя в электронный вид, при этом предлагается заманчивое денежное вознаграждение за выполненную работу. Стандартное недоумение почему не отсканировать и не распознать, или, хотя бы, не отсканировать и не прислать текст в электронном виде парируются многозначительным «там же сложные формулы, вдруг при сканировании что-то недосканируется» и пр.

После согласия выполнить данную работу жертве предлагается оплатить доставку бумажных документов или внести залог в качестве гарантии выполнения работы, который по окончании обещают вернуть, путем перечисления денежных средств на указанный счет/кошелек. Как и следовало ожидать, никакие документы после внесения средств не приходят.

В настоящее время ввиду распространенности специальных программ по распознаванию текста неплохо справляющихся со своей задачей работа по набору текста потеряла свою актуальность. Такая хорошая программа обойдется дешевле не очень хорошего «наборщика текстов». Также, существует вполне реальная вакансия «синхронистов», распознающих тексты с аудиофайлов, высылаемых в формате .mp3 или ином формате аудиозаписи, за пересылку которых никто никаких денег не берет.

Подобная схема может быть применена и с другими видами удаленной работы, как, например, сборщик ручек, фасовка каких-либо предметов или иной другой несложной работы.

Другим вариантом мошенничества может стать выполнение простой работы удаленно на каком-либо сайте. Например, жертве поступает предложение заработать, для этого нужно просто пройти по указанной ссылке, зарегистрироваться на сайте и выполнить несложную работу, к примеру, заполнить вымышленными данными (ФИО, пол, возраст, место проживания и другие возможные данные) около 100-150 форм, похожих на регистрационные. По заполнению указанных форм в профиле жертвы отображается приличная сумма. Каждая из форм приносит небольшой заработок, который можно выводить с сайта каждый день, однако на сайте стоит наподобие защиты, которая активируется при попытке вывести денежные средства. После ввода всех необходимых данных и оформления способа вывода сайт предлагает внести $100 на указанный счет для разблокировки «защиты». В случае, если пользователь все-таки это сделает, «защита» не снимается и все так же просит внести $100.

Опросы. Для участия в опросах необходимо заполнить анкету с определенным количеством вопросов, по заполнении которой выплачивается вознаграждение. Опросы давно являются инструментом маркетингового исследования, а с помощью Интернет еще и довольно недорогим. Важным фактором для возможности прохождения опросов является принадлежность к определенной фокус-группе, т.е. нужно владеть автомобилем, быть домохозяйкой или студентом, владельцем определенно марки телефона и т.д., в зависимости от тематики опроса. Кроме того, опросник составлен таким образом, что школьник вряд ли сможет выдать себя за домохозяйку. В итоге, сделать участие в опросах своим постоянным источником доходов представляется проблематичным.

Именно здесь и рождается следующая схема мошенничества. Создается сайт, на котором любой желающий может проходить, например, два опроса в день вне зависимости от принадлежности к той или иной социальной группе. При условии доплаты, можно пройти еще несколько опросов, а если заплатить еще больше – откроются новые. Причем сами вопросы, как правило, короткие и составлены явно неграмотно, начиная с впечатлений от просмотренного видеоролика, до околопсихологических вопросов с парой контрольных, например, «какого оператора сотовой связи предпочитаете?».

На подобных сайтах чаще всего довольно серьезный минимальный порог для вывода денежных средств, который набирается только после прохождения нескольких десятков опросов, что является стимулом для оплаты опросов (на действительно

работающих сайтах по данной тематике минимум к выводу набирается уже после прохождения 1-3 опросов), или же вознаграждение можно получить через определенное время, например, через месяц, так как «рекламодатель должен проверить» анкету.

Не менее важной чертой является привлекательная система дохода с приведенных партнеров (рефералов[1]), т.е. пользователь получает внушительный процент от дохода человека, которого он позвал проходить опросы на данном сайте.

Естественно по факту никаких выплат не происходит, а через какое-то время в интернете начинают появляться возмущенные отзывы пользователей сайта. Как только негативных отзывов становится слишком много, открывается новый сайт – и данная схема начинает работать заново.

Резюмируя вышесказанное можно выделить следующие признаки мошеннических сайтов, предлагающих заработок на опросах:

1. минимальный порог для вывода денежных средств достигается только при условии прохождения нескольких десятков опросов;
2. возможность прохождения вопросов вне зависимости от возраста/профессии/социального положения/предпочтений и т.д.
3. необходимость внести оплаты для получения возможности проходить больше опросов в день;
4. высокий процент вознаграждения от дохода реферала.

Работа в онлайн играх. Наиболее уязвимой группой в данной схеме мошенничества являются школьники.

Суть схемы заключается в следующем. В интернете появляется рекламное объявление по типу: «ищутся тестеры онлайн игр» или «набирается группа для тестирования новых игрушек» и иные рекламные объявления суть которых сводится к тому, что ищут кого-то, кто мог бы поиграть, и готовы платить за это деньги.

При переходе по объявлению посетитель попадает на сайт тестировщиков, на котором рассказывается, что именно сейчас тестируется, сколько людей работает. Часто указывают игры, названия которых на слуху, а патчи[2] к которым требуют тестеров.

За тестирование предлагают хорошее вознаграждение, но для этого нужно зарегистрироваться на сайте и внести денежные средства в качестве членского взноса, залога за доступ к еще не вышедшей игре или за какие-либо материалы/инструкции и т.д.

[1] Реферал - участник партнёрской программы, зарегистрировавшийся по рекомендации другого участника. Рекомендация сопровождается «реферальной ссылкой», содержащей информацию об учётной записи участника, который получит вознаграждение за привлечение новичков.

[2] Патч – часть программы, или небольшая отдельная программа, используемая для устранения проблем в программном обеспечении.

В крайнем случае просят подтвердить телефон, на который в дальнейшем подключается платная подписка.

Кастинг на участие в сериале, фильме, съемке в рекламе, массовке, ток-шоу. Данная схема в основном направлена на молодых людей. В социальных сетях девушке или парню приходят сообщения с приглашением принять участие в кастинге на роль в каком-нибудь известном сериале или ток-шоу, или, например, просто: «для участия в ток-шоу требуется Ваш типаж». Наиболее важным элементом в данной схеме мошенничества является убедительно оформленная страница приглашающего лица в социальных сетях. В профиле могут быть выложены фотографии с известными лицами, в должности указано – директор по кастингам или что-то похожее, место работы – Останкино, Мосфильм и др. И что не мене важно, девушка или парень или и не огромные любители сериала/ток-шоу, то как минимум интересуются информацией о нем, состоит в соответствующих сообществах в социальных сетях, или же просто интересуется кастингами в целом.

В дальнейшем происходит обсуждение роли и перспектив. Роль не главная и даже не второстепенная, а просто предполагает появление в паре эпизодов, оплата символическая. И, конечно, возможность быть замеченным (-ой). Главным условием участия в кастинге является перечисление определенной суммы денежных средств на телефон/счет/кошелек в качестве залога. После перечисления залога, аккаунт, организовывающий кастинги, удаляется из социальных сетей.

Стоит обратить внимание, что «на улице» и, тем более, в социальных сетях актеров не ищут, про открытые кастинги лучше узнавать на официальных сайтах или сообществах в социальных сетях кинокомпаний и телеканалов, и, тем более, организаторы этих кастингов не будут требовать денежные средства в качестве залога.

Розыгрыш призов. Жертве сообщают, что она выигрывала в розыгрыше, лотерее и т.д. Это может быть сказано напрямую, например, «Поздравляем! Вы стали 100000-м посетителем нашего сайта! Чтобы забрать приз нажмите сюда.» или применена двухступенчатая схема, где изначально предлагается поучаствовать в розыгрыше и ответить на несколько вопросов, после чего жертве сообщается, что по результатам опроса она выиграла приз. Для получения приза необходимо заполнить анкету, одним из пунктов которой вероятнее всего будет являться номер мобильного телефона, который нужно подтвердить с помощью SMS, после чего жертве подключается платная услуга. Возможен вариант и с оплатой пересылки приза. Так или иначе получить приз без дополнительных финансовых затрат не предполагается возможным.

Во избежание возможности быть вовлеченным в мошенническую схему стоит понимать, что невозможно выиграть приз без выраженной воли принять участие в розыгрыше, а также стоит внимательно изучить отзывы и условия проведения розыгрыша.

Авторитетная личность. Здесь речь пойдет об авторитетных личностях в определенных профессиональных кругах. Нередко можно натолкнуться на форумы, посвященные той или иной тематике, в которых участвуют пользователи, предоставляющие услуги, например, по продаже рекламных мест на качественных ресурсах, и пользующиеся определенным уважение среди других участников форума. Потенциальная жертва также является участником данных форумов, а главное – интересующимся лицом.

Мошенническая схема заключается в том, что потенциальной жертве на почту/Skype и др. способы связи приходит сообщение от якобы авторитетного участника форума с предложением услуги, к примеру, размещения рекламы на тематическом сайте со скидкой. В данном случае срабатывает психологический фактор: пользователь с таким никнеймом[3], как и форум, действительно существует, и он действительно оказывает услуги по размещению рекламы. И жертва соглашается. После перечисление денежных средств «авторитетный пользователь» пропадает. При попытке выяснить на самом форуме у пользователя, который якобы предлагал свои услуги, причину неисполнения своей части договора выясняется, что он ничего об этом не знал и контактные данные у него совсем другие.

Для того, чтобы не быть обманутым данным способом в случае подобного обращения стоит написать человеку непосредственно на самой площадке, в рассматриваемом случае написать личное сообщение на форуме, а также дополнительно проверять сайты, правильность написания e-mail, номеров ICQ, имени в Skype, так как лишний пробел, русская «с» вместо латинской «с» визуально почти не отличаются. Данную информацию необходимо проверять на самом ресурсе, с которого пришел обращающийся, по собственным ссылкам, а не тем, что были предоставлены мошенником, так как они могут вести на специально созданный клон нужного ресурса.

Прогноз на исход события**.** Наиболее уязвимой категорией являются азартные лица, увлеченные футболом или, к примеру, бинарными опционами. Данной категории лиц приходит бесплатный прогноз с указанием исхода какого-либо события, например, «в завтрашнем матче Барселона выиграет». Как правило, событие предполагает исход с вероятностью 50/50 (либо да, либо нет). В случае, если прогноз сбывает, жертва получает

[3] Никнейм – псевдоним, используемый в сети Интернет, обычно в местах общения (в блогах, форумах, чатах).

письмо со следующим прогнозом. При положительном исходе, приходит и третье письмо. Если же и третий прогноз сбывается жертве предлагают купить четвертый прогноз за определенную сумму. В данном случае опять же играет роль психологический фактор: если три раза прогноз сбылся, то и на четвертый раз тоже сбудется. Однако стоит отметить, что, если на каком-то из этапов исход события был неверно спрогнозирован, направление писем с прогнозами прекращается.

Схема мошенничества: берется база контактов людей, увлекающихся, например, Forex и делится на две равные части. Половине высылается прогноз с исходом «да», другой половине – прогноз «нет». Вполне очевидно, что один из прогнозов сбывается, тогда «удачная» половина опять делится на две части по схеме «да»/«нет». И снова половина получает уже второй раз подряд верный прогноз и так далее, только на четвертый раз за предсказание исхода события жертве будет предложено заплатить. За деньги выигравшей половине можно писать опять. Таким образом, жертва не покупает верный прогноз, а ей просто «повезло» оказаться в «удачной» половине, и всегда стоит помнить, что человек, знающий исход, вряд ли будет готов делиться этим знанием.

Покупка авиабилетов. Сегодня существует огромное количество сайтов, на которых можно купить авиабилеты на интересующие направления. В поисках дешевых билетов можно наткнуться на сайты, предлагающие цены на билеты существенно ниже цен, указанных на официальном сайте авиаперевозчика. В этом случае стоит быть осторожнее – вероятнее всего это еще одна разновидность мошенничества. Для получения маршрутной квитанции необходимо оплатить билеты, переведя деньги на указанный счет/кошелек. После проведения оплаты билеты так и не приходят. При попытках позвонить по номерам, указанным на сайте, жертву сначала успокаивают обещаниями во всем разобраться, а после и вовсе перестают отвечать на звонки.

Покупки в интернет-магазинах. Нарастание популярности интернет-магазинов привело к появлению новых схем мошенничества и появлению интернет-магазинов, продающие некачественные товары или не осуществляющие доставку товаров в принципе.

Данные интернет-магазины обладают рядом отличительных признаков:

1. Очень большие скидки и низкие цены на весь ассортимент, представленный в интернет-магазине.

2. Не указана контактная информация (номер телефона, фактический и/или юридический адрес продавца). Раздел «Контакты» либо полностью отсутствует, либо предлагается заполнить контактную форму для связи с продавцом.

Кроме того, одним из показательных признаков может служить наличие возможности оплаты товаров только посредством электронных кошельков или денежных переводов по типу Western Union.

Прежде чем совершить покупку в интернет-магазине стоит навести справки о продавце, изучить отзывы о его работе, а также оплачивать стоимость товара по факту его получения.

Интернет-аукционы. В качестве примера будет рассмотрен аукцион по продаже сайтов. Суть схемы заключается в том, что мошенник ищет на форумах предложения о продаже сайтов и настраивает купленные ICQ или страницу в социальных сетях в соответствии с данными о продавцах сайтов. Затем с них он пишет людям, выразивших интерес в покупке сайта, предлагая не затягивать сделку, а приобрести сайт за предложенную ими сумму. На следующем этапе происходит поиск мошенником человека, обладающего электронным кошельком в WebMoney с высокими показателями бизнес-уровня и уровня доверия и оказывающим какие-либо услуги. У пользователя WebMoney уточняется номер кошелька, который затем передаются заинтересованному в покупке сайта лицу для осуществления перевода. Получив от покупателя подтверждение о совершении платежа, мошенник пишет владельцу кошелька об оплате услуги, однако случайно заплатил больше и просит вернуть разницу, оплатив выставленный счет. Как правило владелец кошелька не замечает, что выплачивает разницу вовсе не на тот кошелек, с которого изначально пришла сумма. Таким образом, мошенник получает денежные средства, практически не вызвав подозрений ни у одного участника сделки.

Вовлечение населения в подобные схемы мошенничества приводит не только к потере их денежных средств. Украденные денежные средства могут быть использованы в целях финансирования терроризма, в частности, международной исламистской террористической организации «Исламское государства Ирака и Леванта», действующей по большей части на территории Сирии (частично контролируя ее северо-восточные территории) и Ирака (частично контролируя территорию к северу и западу от Багдада). В Российской Федерации организация ИГИЛ признана экстремисткой. Ее деятельность запрещена.

Террористические организации сегодня активно используют интернет-технологии для вербовки населения и выманивая денежных средств для собственного финансирования.

Бывший госсекретарь и нынешний кандидат в президенты США Хиллари Клинтон (Hillary Clinton), выступая 6 декабря 2015 г. в Брукингском институте (The Brookings Institution), охарактеризовала группировку ИГИЛ как «как самого эффективного

вербовщика в мире»[2], активно использующего в этих целях возможности сети Интернет. По этой причине она призвала ИТ-компании оказывать госструктурам максимальное содействий в борьбе с ИГИЛ в виртуальном пространстве.

Согласно исследованию «ИГИЛ в Америке. От ретвиттов до Ракки» (ISIS in America. From Retweets to Raqqa), проведенному в Университете им. Дж. Вашингтона (George Washington University), Twitter является сегодня основной интернет-платформой, которую исламисты применяют в вербовочных целях. По оценкам экспертов, только в 2015 г. боевикам ИГИЛ с помощью Всемирной паутины удалось привлечь на свою сторону и склонить к переезду в Сирию и Ирак приблизительно 250 американцев, несмотря на активную работу спецслужб, по результатам которой было возбуждено примерно 900 уголовных дел за пособничество террористам. Средний возраст выявленных американцев – адептов «Исламского государства» составляет 26 лет, т.е. это молодые люди, которые используют в своей повседневной деятельности различные социальные медиа.

Специалисты из Университета им. Дж. Вашингтона отмечают, что в Twitter сторонники ИГИЛ в зависимости от выполняемых функций делятся на три категории: генерирующие основной контент (nodes), осуществляющие распространение информации (amplifiers) и «продвигающие» исламские аккаунты (shout-outs) путем искусственного повышения их рейтингов и создания таким образом популярности среди пользователей.

Кроме того, задействованы и другие интернет-сервисы, например, Instagram, в котором деятельность вербовщика внешне выглядит менее навязчивой и более тонкой, чем в Twitter. Данный ресурс нужен в основном для пропаганды «достойной жизни в халифате» и основывается на фото- и видеоматериалах, снабженных хэштегами и принятыми в среде джихадистов символами поддержки ИГИЛ.

В исследовании «ИГИЛ в Америке. От реттвитов до Ракки» отмечается, что по меньшей мере 300 граждан США, почти треть которых составляют женщины, занимаются в социальных медиа активным привлечением граждан в экстремистские организации. В большинстве случаев «обработка» потенциальных боевиков начинается на различных интернет-форумах, а затем продолжается уже в процессе скрытого от других пользователей личного общения с кандидатами.

Так, внимание американских экспертов привлекла учетная запись, которая предположительно принадлежала молодой женщине, проживавшей, судя по селфи и геометкам, сделанным к ним, в Великобритании. Она использовала хэштег #taqwa, что означает «благочестие», и пыталась сформировать у интернет-аудитории представление об «Исламском государстве» как о воплощенном единстве «истинно мусульманского

общества». В сообщениях гипотетической вербовщицы также присутствовали знаки «эмодзи» (emoji), которые символизируют небо и Аллаха и часто используются сторонниками исламистов.

В текстах на странице другого пользователя употреблялось слово «coconuts» (кокосы), которым в игиловской онлайн-среде обозначают людей, не разделяющих ценностей «чистой веры», и слово «ukhtis» (сестры), применяющееся для повышения внимания аудитории и вовлечения в беседу в индивидуальном порядке.

Последователи ИГИЛ создали во Всемирной паутине собственные стиль и линейку образов, понятные участникам конкретных групп. Например, изображение зеленой птицы или сочетание «эмодзи» в виде птицы и зеленого сердца или круга используются для обозначения мучеников, а часто публикуемое сторонниками «Исламского государства» на своих интернет-страницах изображение льва обозначает в исламе храбрость.

Эксперт Университета им Дж. Вашингтона Сара Гилкс (Sarah Gilkes) подчеркивает, что практически все американцы, осужденные в США за связь с ИГИЛ, проводили значительное время в экстремистских онлайн-сообществах. Многие завербованные террористами пользователи Интернета являются выходцами из неблагополучных семей и испытывают трудности с социализацией, тогда как виртуальные площадки дают им чувство общности и сопричастности к «великому делу».

Психологическое давление и использование человеческих слабостей и трудностей, с которыми столкнулся конкретный человек, позволяет террористам доносить пропаганду своих ценностей и идей до конечной «целевой аудитории», после чего жертва, в лучшем случае, будет готова добровольно пожертвовать террористическим группировкам денежные средства.

Американские специалисты утверждают, что часть этих людей вряд ли решится на преступление: скорее всего, они сумеют преодолеть возникшие проблемы в общении, обусловленные возрастными изменениями и личностными особенностями, и вернуться к нормальной жизни. При этом неизбежны аресты отдельных лиц, которые только теоретически рассуждали о возможности реализации каких-либо противоправных действий и делились своими мыслями на страницах соответствующих интернет-ресурсов.

Резюмируя вышесказанное, хочется еще раз обратить внимание, что мошенничество в сети интернет становится новой угрозой не только для имущественного благосостояния физических лиц, но и для безопасности всего общества в целом. Именно поэтому при пользовании интернет-технологиями стоит проявлять бдительность, не давать свои личные данные незнакомым людям не будучи уверенным, что этот человек не

является злоумышленников, ни при каких обстоятельствах не сообщать коды подтверждения операций и иные сведения, позволяющие получить доступ к счетам и электронному кошельку. Кроме того, следует помнить, что «если кто-то хочет получить от вас хоть какие-то деньги, предлагая заработок – это мошенничество. Всегда. Исключений – нет».

Список использованных источников:

1. РосБизнесКонсалтинг [электронный ресурс]. – Режим доступа: http://www.rbc.ru/finances/23/06/2015/558936aa9a79477bdc5736ec

2. Lecher C. Hillary Clinton asks “great disruptors” of Silicon Valley to “disrupt ISI”/ The Verge. 2015. December 7. – http://www.theverge.com