КУЛЬТУРОЛОГИЯ

ИНТЕРНЕТ МОШЕННИЧЕСТВО - ЭТО НОВАЯ ИНТЕРНЕТ ТЕХНОЛОГИИ ИЛИ ЖАДНОСТЬ И АЛЧНОСТЬ НЕИСТРЕБИМЫ…?

Дворянкин О.А.
кандидат юридических наук,
старший преподаватель кафедры информационной безопасности
Учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
Москва

IS INTERNET FRAUD A NEW INTERNET TECHNOLOGY OR IS GREED AND CUPIDITY INDESTRUCTIBLE…?

O.A. Dvoryankin
candidate of legal sciences,
lecturer at the chair of information security
of the Moscow Ministry of Internal Affairs
of the Russian Federation Kikot University,
Moscow

АННОТАЦИЯ

В статье представлена информация о видах и формах интернет мошенничества. Осуществлено исследование ситуации, когда проходит интернет мошенничество, а также обстоятельства, когда люди сами очень часто рассказывают преступникам о своих бедах и проблемах, показывают свою алчность, жадность, обозначают быстрое стремление в получении денег, при этом ничего не делая для этого, и тем самым, своими действиями и поступками, провоцируют мошенников на противоправные действия или вразумительные действия для жертвы на будущее.

ABSTRACT

The article provides information on the types and forms of Internet fraud. The study of the situation when Internet fraud takes place, as well as the circumstances when people themselves very often tell criminals about their troubles and problems, show their greed, cupidity, and show a huge desire to get money, while doing nothing for this, and thus, by their actions and deeds, provoke fraudsters to illegal actions or intelligible actions for the victim in the future.

Ключевые слова: информационная безопасность, Интернет, мошенничество, информация, деньги, психология

Keywords: information security, Internet, fraud, information, money, psychology

Современное общество характеризуется развитием информационных технологий и глобализацией информационных процессов. Одним из самых ярких примеров такого процесса – это появление сети Интернет, а также стремительное и постоянное развитие его информационных технологий во всех сферах общественной жизни.

В настоящее время нельзя представить себе жизнь человека без Интернета, он буквально стал неразрывной частью общества.

Первоначальной целью разработки сети Интернет являлось создание надежной системы обмена информацией между компьютерами, а также (что явилось одной из главных целей) для отработки методов поддержания связи в случае ядерного нападения.

При этом по прошествии уже нескольких десятилетий с момента его создания, и не смотря, что проблема ядерной войны уже не является такой актуальной, хотя с повестки дня не снята, информационные технологии из военной сферы были переведены в гражданскую область жизнедеятельности, где получили новое дыхание, приобрели новейшие возможности и стали активно расти с каждым годом в Интернет пространстве.

Среди них можно выделить следующие:

– получение, хранение, обработка, распространение и использование информации и знаний благодаря возрастающим техническим возможностям коммуникации;

– осуществление коммуникации почти мгновенно, что принципиально отличает его от других средств коммуникации;

– функционирование виртуального пространства, повторяющего реальные сферы жизнедеятельности человека;

– проникновение компьютерных технологий в науку, культуру, медицину, образование, экономику, политику, технологии, производство;

– осуществление коммуникации с другим человеком (часто совершенно незнакомым), при этом отсутствует зависимость от местонахождения обоих, а коммуникация может поддерживаться непрерывно.

Растет не только количество интернет-пользователей, но и время, которое они проводят, пользуясь устройствами и сервисами, работа которых зависит от подключения к Интернету и в 2020 году эта цифра составляла в среднем 6 часов в день.

Однако вместе с возможностями сети Интернет для развития и расширения коммуникации между людьми и, также возможности поиска, хранения и обработки большого количества информации, Интернет стал и полем для деятельности мошенников, т.е. обмана людей и выманивания у них на **«добровольных основах»** денежных средств.

Под мошенничеством в Уголовном кодексе Российской Федерации (статья 159) понимается хищение имущества, которое принадлежит третьим лицам. Важным признаком, отличающим мошенничество от других преступлений, направленных против собственности, является то, оно осуществляется посредством обмана потерпевшего или введения его в заблуждение.

В этой связи необходимо отметить, что мошенничество существовало всегда. Всегда были люди, которые обманывали и были другие, которых обманывали. По мере развития общества мошенники всегда старались разнообразить свои навыки и увеличить количество наживы, а с появлением Интернета, мошенники, увидев в нем преимущества для себя и проблемы для жертвы, незамедлительно переместились в его виртуальное пространство.

Таким образом нельзя говорить о том, что мошенничество появилось в Интернете случайно. Люди всегда желали обогащения и получения больших объемов денежных средств. Во все времена в обществе были люди с низким достатком по различным причинам, но жаждущие получать «значительные суммы денег», еще алчные и жадные люди, а также люди, готовые идти на риск ради своей выгоды и, в частности, ради получения денег. Такие люди и становятся приманкой для мошенников, которые играют на чувствах людей, на их желании заработать, получить быструю выгоду и при этом ничего не делая, т.е. находя для себя выгоду в поведении и потребностях пользователей.

В наше время, когда повсеместно применяются компьютерные и информационные технологии, когда люди безоговорочно верят в их непогрешимость и открытость, при этом не думая о своей информационной безопасности, многие способы выманивания денег, которыми пользовались мошенники, преобразились, модернизировались и по-новому обрели свою актуальность. Например, речь идет о предложении покупки «чудодейственных» косметологических препаратах, мошенничестве с недвижимостью, мошенничество гадалок и др. Таким образом в наше время интернет мошенничество становится самой всеохватывающий и масштабной сферой преступности и при этом снова или точнее заново поднимает старые виды мошенничества и ставит их на новые информационные рельсы (технологии).

При этом, одной из отличительных характеристик, нового мошенничества является следующее, в интернет-мошенничестве субъект не входит **в прямой контакт** (непосредственный, личный, совместные встречи) с жертвой, что значительно снижает шансы на разоблачение и такой способ с каждым годом набирает популярность, проникая во все сферы общественной жизни.

Именно отсутствие прямого контакта и применение информационных технологий упрощает получение персональных данных потенциальных жертв. Поэтому многие организации и сервисы используют эту информацию для настройки таргетированной рекламы, запуска кампаний социальной инженерии или влияния на пользователей с помощью других манипулятивных методов, но это они производят не всегда для мошеннических действий, а только для получения дополнительной выгоды.

А вот мошенники они целенаправленно настроены на определение Ваших предпочтений, любимых мест, близких люди и иных подробностей о Вас, чтобы получить о необходимую персональную (личную) информацию, которая позволит или станет тем ключевым инструментом для осуществления преступной деятельности, связанной с передачей добровольно Вами денег мошенникам. Другими словами, личная информация жертвы и не осуществляемая ей информационная безопасность, становится для мошенников самым важным инструментом в его деятельности.

В целом необходимо говорить о том, что мошенники, как правило, люди, обладающие высоким уровнем интеллекта и определенными и иногда очень серьезными познаниями в области психологии, что позволяет им свободно вступать в контакт, располагать к себе, а в большинстве случаев, они являются специалистами в экономике, информационных технологиях и т. д.

При этом, мошенники, несмотря на совершенствование психологических маневров и на то, что новые технологии (фишинг, фарминг и др.) стали более совершенными, общий принцип изъятия денег остался прежним, т.е. мошенники и воры в большинстве случаев в сети Интернет, как и раньше используют определенные способности, т.е. старые проверенные методы и технологии, но при этом и в связи со знанием информационных технологий стали обладать «уникальными способностями и знаниями», которые используют в своем деле.

С приходом Интернета мошенникам приходится постоянно развиваться, совершенствоваться, учиться и в обязательном порядке применять вновь получаемые знания, технологии, но в тоже время с учетом старых, проверенных годами методик отъема денежных средств.

При этом важно отметить, что в основном мошенники полагаются не столько на высокие технологии и уникальные возможности, а на классические психологические методы воздействия на человека, позволяющие ввести жертву в заблуждение. Мошенники чаще всего пользуются доверчивостью своих жертв, когда она сама рассказывает личную и сугубо личную информацию о себе, пренебрегает или не знает основные правила интернет-безопасности (информационной безопасности), используют элемент неожиданности и запугивания потенциальной жертвы, чтобы получить информацию, которую впоследствии используют для совершения кражи или иной противоправной деятельности.

Наряду с этим, мошенники целенаправленно входят в доверие к жертве, а потом им злоупотребляют, т.е. осуществляют обман.

Обман может выражаться в ложном заявлении о том, что оно сознательно не соответствует действительности, или в преднамеренном замалчивании разных фактов, сообщение которых было необходимо. В любой форме обмана и злоупотребления доверием его суть заключается в том, что преступник посредством гарантий или упущений формирует у потенциальной или реальной жертвы наличие недостаточно верного или абсолютно неправильного представления о каком-либо объекте. Подобная ситуация приводит жертву к убеждению в необходимости передачи активов, или так называемого имущественного права. То есть реализуется ключевой принцип мошенничества, при котором преступление совершается на основе введения в заблуждение или обмане.

Неудивительным в современных реалиях является тот факт, что мошенничество в сфере компьютерной информации сегодня по праву вполне можно считать очень быстро развивающимся преступлением, поскольку активное развитие самих информационных технологий создает для этого все больше возможностей.

Мошеннические схемы в области компьютерной информации - это «кража» собственности других лиц или приобретение прав на собственность других лиц незаконным способом путем ввода, удаления, а также блокирования, изменения компьютерной информации или любых других способов вмешательства с операциями, связанными с хранением, обработкой и/или передачей компьютерной информации. Также информационные и телекоммуникационные сети подвержены мошенническим атакам. С реальной точки зрения процессы ввода, удаления, блокировки, любого изменения компьютерной информации или другого вмешательства в операции содержат характерные и вполне очевидные признаки мошеннических действий в области работы с компьютерной информацией. [1].

С учетом изложенного рассмотрим разные виды мошенничества в различных областях жизнедеятельности людей.

В настоящее время банковская сфера является одной из самых популярных среди интернет мошенничества.

Один из самых популярных и распространенных методов ограбления клиентов в Интернете – это фишинг. Слово представляет собой сочетание двух английских слов: пароль и рыбалка. В просторечии это словосочетание переводится как «перехват паролей». Этот метод чаще всего используется для обмана жертв, использующих интернет-банкинг, когда мошенники выдают себя за банк и отправляют поддельное сообщение на сотни случайно выбранных адресов электронной почты с просьбой срочно войти в систему онлайн-банкинга определенного банка. Сообщение содержит ссылку на поддельный веб-сайт. После входа в фальшивую учетную запись покупателя просят ввести одноразовые коды или иную информацию, помогающую мошеннику получить доступ к банковскому вкладу жертвы [2].

В последнее время данный классический вид фишинговых атак претерпел множество изменений в основном из-за того, что все больше и больше банков отправляют одноразовые коды через SMS.

В этой связи мошенники отправляют электронные письма, к которым прикрепляют поддельные вложения, в которых якобы содержатся выписки с историей счета или запросы на оплату. Обычно прикрепленные файлы имеют расширения, аналогичные широко используемым, но с небольшими изменениями. Например, вместо файла «*.pdf» используется файл «*.pif» и когда такой файл открывается, вирус устанавливается на компьютер жертвы.

В последствии, когда пользователь заходит на сайт своего банка и вводит данные для входа, вредоносная программа перехватывает их и отправляет мошенникам.

Кроме того, на странице онлайн-банкинга будет отображаться сообщение с просьбой установить на мобильный телефон специальную антивирусную программу, предположительно рекомендованную банком. По сути, это еще один вирус, на этот раз заражающий смартфон. После его установки SMS-коды, поступающие на телефон клиента, автоматически перенаправляются на номер похитителя. Пользователь даже не знает, что получил авторизационное SMS, потому что мошенники блокируют отображение уведомлений. Благодаря этому мошенники могут осуществлять переводы без ведома клиента.

В настоящее время осведомленность пользователей о фишинговых атаках возрастает. Банки, социальные сети и другие веб-сервисы предупреждают о различных мошеннических схемах, использующих методы социальной инженерии. Все это уменьшает количество откликов в фишинговой схеме. Все меньше и меньше пользователей можно обманным путем заманить на поддельный сайт. Поэтому

злоумышленники придумали механизм скрытого перенаправления пользователей на фишинговые сайты, получивший название «фарминг» («pharming» — производное от слов «phishing» и англ. «farming» — занятие сельским хозяйством, животноводством).

Злоумышленник распространяет специальные вредоносные программы на компьютеры пользователей, которые после запуска перенаправляют обращения к заданным сайтам на поддельные сайты. Это обеспечивает высокую скрытность атак, а участие пользователя сводится к минимуму — достаточно подождать, пока пользователь решит посетить интересующие злоумышленника сайты.

Методов абсолютной защиты от фарминг-атак, возможно, не существует, поэтому необходимо применять превентивные меры:

1. Использование и регулярное обновление лицензионного антивирусного программного обеспечения; Использование защиты электронного почтового ящика (отключение предварительного просмотра); не открывать и не загружать вложения электронных писем от незнакомых и сомнительных адресатов.

2. Еще один метод вымогательства данных у клиентов – это так называемый «вишинг» или голосовой «фишинг». Вор притворяется представителем банка и звонит покупателю с каким-либо предложением, чаще всего запугивая тем, что кто-то получил доступ к его счету и банку необходимо помочь в поиске, блокировке счета. После стандартных вопросов о личных данных он начинает вникать в детали, спрашивая, например, о логине и пароле для онлайн-банкинга, номере платежной карты, кодах проверки карты (CVV) или только что полученных кодах авторизации транзакций. Это пугает пользователя тем, что его учетная запись была взломана, и он соглашается быстро изменить ситуацию по телефону, что в итоге приводит к потере всех денег на счету.

3. Еще одним инструментов для интернет-мошенничества становятся платежные карты. Данные карт клиентов банка – это самый популярный в настоящее время товар на черном рынке. Поэтому воры пытаются получить эту информацию разными способами. Стоит помнить, что во многих банках до сих пор нет дополнительных методов защиты карточных платежей. Таким образом, достаточно знать только номер карты, срок ее действия и трехзначный код на ее обратной стороне, чтобы совершить транзакцию. На самом деле достаточно даже фотографии карты, чтобы произвести платеж в сети Интернет.

4. Еще один способ мошенничества в Интернете – это открытие счета в банке на имя жертвы. В некоторых банках можно открыть счет удаленно, а личность проверяется на основе данных, содержащихся в переводе, поступающем из другого банка. Такой перевод включает в себя всю необходимую информацию об отправителе – имя, фамилию и адрес. Этим пользуются воры, которые подают заявку от имени клиента и пытаются уговорить его сделать перевод на указанный счет. Если он это сделает, вор получит в свое распоряжение банковский счет, оформленный на другого человека. Такой метод могут использовать на сайте объявлений, например, прося внести залог за товар, если покупатель не готов заплатить сразу или просит подождать и придержать товар по выгодной цене. Естественно, залог будет обналичен, а покупатель ничего не получит, при этом виновником будет тот, на чье имя открыт счет. [3].

5. «Кардинг — (от англ. carding) — это еще один вид мошенничества, при котором транзакция совершается с использованием платежной карты или ее реквизитов, не инициированных и не подтвержденных ее держателем.

Данные платежных карт обычно берутся со взломанных серверов интернет-магазинов, платежных и расчетных систем, а также с персональных компьютеров (либо напрямую, либо через программы удаленного доступа, «трояны», «боты» с функцией «form grabber» (шпионская программа, используемая для перехвата введенных паролей и имен пользователей))». Одним из самых масштабных преступлений в области мошенничества с платежными картами считается взлом глобального процессинга кредитных карт «Worldpay» и кража с помощью его данных более 9 миллионов долларов США. В ноябре 2009 года по этому делу были предъявлены обвинения преступной группе, состоящей из граждан государств СНГ.

Наряду с представленными методами мошенничества преступники в сети Интернет используют и иные информационные технологии и работают (нацелены) не только на клиентов банка.

Рассмотрим иные виды интернет-мошенничества в других секторах нашей жизнедеятельности.

1. Самый распространенный метод – это «скимминг» (копирование персональных данных при помощи считывающих устройств на банкоматах), но есть попытки получить эти данные по телефону, или на сайтах частных объявлений или сайтах знакомств. Бывает, что данные с карты могут украсть в магазине или кафе, если клиент передает карту продавцу или официанту, а тот якобы должен отнести ее к платежному терминалу и там выполнить оплату. Скиммингом занимаются группы мошенников, которые имеют специальное оборудование и технические средства, а вот для того чтобы просто скопировать номер карты и CVV код особых знаний не требуется, как и выполнить оплату с использованием таких данных.

2. Также одним из старейших видов интернет-мошенничества является так называемое мошенничество «нигерийского принципа» (нигерийские письма). В этом случае к жертве по почте обращается человек, который имеет огромные активы (чаще всего наследство), но по каким-то причинам не может их формально получить и нуждается в партнере, который,

конечно же, получит минимум половину или даже всю сумму, в зависимости от договоренности при подготовке к сделке. Для подтверждения ваших данных получателю письма следует отправить отсканированные документы и небольшую сумму для выполнения формальностей. После отправки денег связь с предполагаемым «партнером», конечно же, прерывается, а переведенные деньги теряются или если работа с вами продолжается, если мошенник уверен в своей безнаказанности.

««Нигерийские письма» (англ. «Advance-fee scam», буквально «Мошенничество с предоплатой») — распространенный вид мошенничества, который получил наибольшее развитие с появлением массовых рассылок по электронной почте (спам). [4].

Письма названы так, потому, что этот вид мошенничества был особенно распространен в Нигерии, причем еще до распространения Интернета, тогда такие письма распространялись обычной почтой. Однако нигерийские письма приходят и из других африканских стран (Того), а также из городов с большой нигерийской диаспорой (Лондон, Амстердам, Мадрид, Дубай). Рассылка писем началась в середине1980-х гг. Как правило, мошенники обращаются к получателю письма за помощью в многомиллионных денежных операциях, обещая солидные проценты на полученные суммы. Если получатель соглашается участвовать, то постепенно у него, раз за разом (денежная операция за денежной операцией) выманивают все более крупные суммы денег (начинают, например, сначала 100 долларов США, потом 300, затем 500 и т.д.) якобы для совершения сделок, уплаты пошлин, подкупа должностных лиц и т.д. Нигерийские письма — один из самых распространенных видов мошенничества в Интернете, ему присвоен специальный код № 419.

3. «Фарминг (англ. «pharming») — это процедура скрытного перенаправления жертвы на ложный IP-адрес. В классическом фишинге злоумышленник распространяет письма по электронной почте среди пользователей социальных сетей, интернет-банкинга, почтовых веб-сервисов, заманивая пользователей, ставших жертвами мошенничества, на поддельные сайты с целью получения их имен пользователей и паролей. Многие пользователи, активно пользующиеся современными веб-сервисами, уже не раз сталкивались с подобными случаями фишинга и настороженно относятся к подозрительным сообщениям. В классической фишинговой схеме главным «слабым» звеном, определяющим эффективность всей схемы, является зависимость от пользователя.

При этом хочу отметить, это только некоторые наиболее ярко проявившие себя в последнее время формы интернет мошенничества. В ближайшее время будут появляться новые и мы он них так же обязательно узнаем и будем, вероятно, принимать необходимые меры информационной защиты.

Таким образом, делая предварительный вывод, можно сказать, что технологии интернет-мошенничество распространяется по всем каналам связи в сети Интернет: через форумы, чаты, обмен мгновенными сообщениями, социальные сети, электронная почта и другими способами ознакомления аудитории или посредством размещения информации на веб-сайте, что способно сделать ее доступной для всего мира.

Кроме этого у них постоянно совершенствуются и изменяются методы совершения преступлений, модернизируются «инструменты» (создаются новые программы), появляются новые схемы обмана и как результат от таких действий страдают люди и компании, которым приносится значительный ущерб. Эту тенденцию хорошо показывают различные статистические отчеты, отмечая, что правоохранительные органы еще недостаточно эффективно противодействуют интернет мошенничеству.

Также важно учитывать, что в настоящее время из-за пандемии коронавирусной инфекции (COVID-19) человечество в мировых масштабах вполне закономерно столкнулось с этим явлением, так как люди сидят дома, хотят общения и заработка дополнительных денег, что в полном объеме дают им интернет мошенники, только в противоположном виде.

Так, в новой жизни отмечается глобальный переход к онлайн-системам и удаленному формату работы и/или обучения. Наблюдается тенденция роста аудитории Интернет-пространства за счет пожилых людей, включая аудиторию в возрасте 65 лет и старше. В начале появления электронной коммерции, интернет-магазинов пользователей недостаточно сильно волновала возможная потеря учетной записи на веб-сайте интернет-магазина, поэтому ими выбирались предельно простые учетные записи и зачастую использовали одни и те же пароли для самых разнообразных веб-сайтов.

Оплата производилась не в онлайн-формате, а наличными денежными средствами на почте или непосредственно при доставке заказа. Как только появилась возможность связывать банковские карты и платежи в Интернет-среде, онлайн-мошенничество начало активно и быстро процветать. К примеру, стали появляться базы паролей с открытым доступом и мошенническое фишинговое программное обеспечение.

В течение последнего времени многократно увеличилось общее количество интернет-мошенничества с использованием рассылок и рекламы в виртуальной сети, целью которых по-прежнему является вымогательство денежных средств у пользователей сети.

В случае применения мошеннических схем пользователям обещают получение очень солидного вознаграждения, если они пройдут специальный интернет-опрос или примут непосредственное участие в конкретной акции.

Чтобы получить деньги, пользователь должен первоначально заплатить небольшой «комиссионный сбор», размеры которого обычно не превышают 200-300 рублей. В результате

пользователь не получит обещанную оплату, а «комиссионный сбор» уйдет злоумышленникам. В этом отношении наиболее распространенными в современных реалиях являются опасные виды мошенничества, такие как поддельные онлайн-опросы от имени крупных компаний, социальные выплаты из фиктивных финансовых средств и мошенничества с досками объявлений или службами доставки [5].

Кроме этих видов интерне мошенничества в последние годы россияне довольно часто сталкиваются с телефонным спамом или новым форматом мошенничества. Например, мошенники звонят, к примеру, из «банковского отдела службы поддержки клиентов». По этой причине многие владельцы гаджетов предпочитают в последнее время не отвечать на звонки с незнакомых номеров. Руководители отделов кибербезопасности мобильных операторов, как правило, очень внимательно отслеживают такие события и предоставляют оператору черный список номеров, с которых чаще всего совершаются мошеннические звонки. Потом указанные номера бывают заблокированы. В любом случае оператору не разрешается прослушивать звонки, что в некоторой степени облегчает работу мошенникам [6].

В этой связи необходимо сказать, что службы безопасности коммерческих организаций и государственных органов постоянно выявляют эти схемы, но интернет мошенники придумывают новые. Простые и примитивные виды интернет-мошенничества остались далеко в прошлом с момента появления Интернет-пространства. Новое поколение мошеннических систем разработали и разрабатывают не «школьные» хакеры, а профессиональные преступники, поэтому абсолютно все недостатки устаревших систем постоянно учитываются и устраняются при разработке.

Таким образом, раскрыть мошеннические схемы, доказать их существование и уничтожить все системы злоумышленников «под корень» в современных реалиях является практически невозможным. Зачастую пользователи переключаются со страницы, где упоминается любимый бренд, на страницу злоумышленника и не замечают, что этот бренд больше не упоминается на последующих веб-сайтах, где просят заплатить или оставить свою персональную, личную информацию. Безусловно, указанные страницы вполне могут находиться в совершенно другом домене и исходить от другого провайдера.

В заключение необходимо отметить, что схемы интернет-мошенничества становятся с каждым годом все более и более изощренными.

Раньше использовались классические методы для привлечения трафика на мошеннические сайты или электронный спам, всплывающая и баннерная реклама, поисковая оптимизация. Сегодня социальные сети и социальная инженерия не только расширили, но и упростили, расширили масштабы для деятельности мошенников, так как теперь они являются стандартным и традиционным методам личного и конфиденциального общения.

Таким образом можно сделать вывод, что, мошенники в настоящее время - это не отдельные хакеры-любители (такие тоже существуют), а крупные организованные криминальные группировки со значительными ресурсами (финансовыми, информационными и техническими) начали конкретно и достаточно активно атаковать людей на изъятие мошенническими способами денежных средств

В результате количество случаев онлайн-мошенничества растет с каждым годом, причем намного быстрее, чем количество простых случаев обычного фишинга. При этом растут масштабы мошенничества и количество обманутых людей, даже из числа тех, кто считает себя подкованным на уловки преступников. Все это говорит о формировании негативной тенденции к дальнейшему развитию интернет-мошенничества.

Однако важно сделать вывод о том, что интернет-мошенничества не было бы, если бы не существовало алчности и жадности простых людей.

Мошенники только отвечают на поведение людей, на их потребность и желание рисковать, ради получения выгоды и при этом для достижения своих целей и задач, при необходимости, совершенствуют использование психологических уловок в отношении потенциальных жертв.

В завершении хочу сказать, что с интернет мошенничеством можно бороться, в первую очередь, путем повышения бдительности самих людей, а также путем противодействия жадности и неоправданными рискам, которые свойственны простым людям.

В этой связи надо больше, активней говорить о таких явлениях и может быть тогда из-под преступников будут выбита противоправная платформа, а люди задумаются и себя информационно обезопасят (информационная безопасность - это как личная гигиена).

ЛИТЕРАТУРА

1. Заплатина Е. А., Калинина Ю. В., Еремина Е. А., Лопатин Д. В. Интернетмошенничество. Старые и новые угрозы / Е. А. Заплатина, Ю. В. Калинина, Е. А. Еремина, Д. В. Лопатин // Гаудеамус. – 2012. – № 20. – С. 36–42.

2. Радевич, В. В. Этапы и виды манипуляции как коммуникативной стратегии в неискреннем дискурсе на материале жанра «Нигерийские письма» / В. В. Радевич. — Текст: непосредственный // Вестник КемГУ. — 2012. — № 4. — С. 121.

3. Атаманов Р. С. Некоторые вопросы расследования мошенничества в сети Интернет / Р. С. Атаманов // Государство и право. – 2010. – № 4. – С. 44–51.

4. Что такое фишинг (phishing) атака и как ее избежать?. — Текст: электронный // Яндекс Кью: [сайт]. — URL: https://yandex.ru/q/question/computers/chto_takoe_fis

hing_phishing_ataka_i_kak_94997200 (дата обращения: 18.01.2020).

5. Никитина И. А. Финансовое мошенничество в сети Интернет / И. А. Никитина // Вестник Томского гос. университета. – 2010. – № 337. – С. 122–124.

6. Журавлева Е. Ю. Основные категории пользователей среды сети Интернет/ «Социология и Интернет: перспективные направления исследования», 2014-2015. С. 29.