Столяр Ю. Д.

К ВОПРОСУ ВЫЯВЛЕНИЯ МОШЕННИЧЕСТВА С ПОДЛОЖНОЙ СТРАНИЦЕЙ 3D-SECURE

Столяр Юлия Дмитриевна, студентка 4 курса Белорусского государственного университета, г. Минск, Беларусь, stoliaryulia@gmail.com

Научный руководитель: канд. юрид. наук, доцент Красиков В. С.

Расследование мошенничества в глобальной сети Интернет на сегодняшний день является одной из основополагающих направлений деятельности правоохранительных органов. Резкий скачок количества киберпреступлений, совершаемых на территории Республики Беларусь, напрямую свидетельствует о низкой правовой культуре и правовом сознании граждан в области информационной безопасности. Для создания действенного механизма расследования преступлений в сфере высоких технологий видится необходимым как реформировать внутреннюю структуру правоохранительных органов, организовав специальные подразделения, деятельность которых будет направлена на выявление, пресечение и предупреждение киберпреступлений; так и ввести тренинги для граждан, цель которых научить последних распознавать признаки мошеннических деяний, защищать свои персональные данные в глобальной сети Интернет, а также, в случае выявления признаков преступления, оперативно реагировать на произошедшее с целью предотвращения негативных последствий.

Ввиду стремительности развития цифровой экономики и глобальной информатизации, общество все чаще сталкивается с такими преступлениями, как фишинг, вишинг, смишинг, кибервымогательство. Но мошенники, как и технологии, не стоят на месте, придумывая все новые способы обмана и манипулирования с целью завладения чужими денежными средствами, либо определенной информацией. Так, среди новшеств можно упомянуть мошенничество с подложной страницей 3D-Secure.

Разработанная платежными системами (Visa, MasterCard) технология 3D-Secure направлена на обеспечение безопасности платежей по картам в глобальной сети Интернет, позволяющая идентифицировать Держателя карты, осуществляющего операцию. Процесс осуществления оплаты посредством технологии 3D-Secure представляет собой введение необходимых реквизитов платежной карточки, после чего происходит соединение с банком посредством переадресации на отдельную безопасную страницу с одновременным отправлением клиенту банком СМС-сообщения с одноразовым паролем, указание которого необходимо на данной странице. После ввода пароля осуществляется автоматический переход на сайт интернет-магазина и оплата покупки.

В настоящее время участились случаи подделывания официальных сайтов интернет-магазинов с имитированием злоумышленниками страниц оплаты, якобы защищенных 3D-Secure. Ввиду снабжения подложных 3D-Secure страниц логотипами международных платежных систем отличить такие страницы от оригинальных крайне затруднительно, что позволяет злоумышленникам не мешкая ввести в заблуждение стремящихся быстро оформить покупку в интернет-магазине покупателей. Именно в этом и заключается опасность такого рода преступления. В частности, для банка-эмитента такие транзакционные операции довольно транспарентны, имеют легальный облик, не вызывая каких-либо подозрений. Таким образом, злоумышленники наносят вред не только лицу, осуществившему транзакцию, а также банку-эмитенту, одобрившему данную операцию, интернет-магазину, чей сайт был подделан, а также платежным системам, чьи логотипы были использованы для достижения корыстных целей.

Реклама, спам-рассылки являются способами привлечения потенциальных жертв мошенничества на фишинговые сайты. Зайдя на поддельный сайт, покупатель производит оплату товара посредством введения необходимых реквизитов банковской карты, впоследствии попадающих на сервер мошенника, откуда происходит обращение к P2P-сервисам различных банков с указанием в качестве получателя одной из карт мошенника (P2P-сервис представляет собой технологию онлайн-переводов денежных средств с одной банковской карты на другую). P2P-сервис выбранного банка, в свою очередь, направляет на сервер мошенника сообщение, содержащее закодированную информацию о банковской карте плательщика, сумме перевода, названии и реквизитах использованного P2P-сервиса. С целью сокрытия от покупателя факта использования P2P-сервиса банка, на сервере мошенника осуществляется подмена реальной информации на подложные данные об данном интернет-магазине, которые впоследствии отображаются на легитимной 3D-Secure странице банка, где покупатель осуществляет ввод платежных данных, подтверждая данную транзакцию паролем из СМС-сообщения, пришедшего на мобильный телефон. После ввода вышеуказанного пароля происходит переадресация на фишинговый ресурс, а деньги перечисляются на счет мошенника.

В целях предотвращения такого рода преступлений банкам необходимо предпринять попытки усиления защиты данных посредством блокирования возможности обращения фишинговых сайтов к легитимному серверу 3D-Secure. Пресечь такого рода киберпреступления возможно лишь в случае, если мошенничество с поддельной страницей ввода кода из СМС осуществляется автоматизированно посредством специально разработанного алгоритма. Введение данных, изменение IP-адреса злоумышленником вручную исключают возможность пресечения преступления ввиду формирования таким образом легитимного запроса в банк.

Таким образом, при осуществлении оплаты на сайтах интернет-магазинов посредством технологии 3D-Secure необходимо обращать внимание на источник платежа, указанный в отправленном банком СМС-сообщении, содержащем код подтверждения транзакции. Указание в полученном СМС-сообщении на инициирование платежа с ресурсов Card2Card или 2P2 свидетельствует об подложности данных.

Подводя итог вышесказанному, необходимо отметить, что такого рода преступления высоколатентны, ввиду чего их общественная опасность относительна велика. Поиск новых механизмов противодействия кибепреступности является на данный момент одной из первостепенных задач, возложенных на правоохранительные органы. Именно посредством анализа причин киберпрестпуности, рисков и угроз кибермошенничества, форм совершения данного вида преступлений возможно достижение положительных результатов в ходе расследования. Благоразумным видится также разработка и создание международных правовых инструментов, направленных на противодействие киберпреступности. Таким образом, только путем взаимного сотрудничества граждан и правоохранительных органов, возможно добиться снижения уровня преступлений, совершаемых в сфере высоких технологий, на территории Республики Беларусь.

Строганова Э. А.

ПЕРСПЕКТИВЫ ИНТЕГРАЦИИ СОВРЕМЕННЫХ ПСИХОЛОГИЧЕСКИХ КОНЦЕПЦИЙ В КРИМИНАЛИСТИКУ

Строганова Элеонора Александровна, студентка 3 курса факультета № 2 Криворожского учебно-научного института Донецкого государственного университета внутренних дел, г. Кривой Рог, Украина, eleonorastroganova@gmail.com

Научный руководитель: канд. юрид. наук, доцент Кубарев И. В.

В течение многих десятилетий криминалистика как наука претерпела качественные изменения, направленные на оптимизацию и увеличение эффективности процесса раскрытия и расследования преступлений. Однако постепенное развитие криминалистики не оказалось бы столь стремительным без активного заимствования достижений в самых различных научных областях. Как справедливо отмечает Р. С. Белкин, одной из главных задач криминалистики остается научное обеспечение практики борьбы с преступностью, для достижения которой тщательно изучаются именно психологические аспекты процесса раскрытия, расследования и предупреждения уголовных правонарушений (Р. С. Белкин, 1999).

Под понятием «концепция» (от лат. conceptio – понимание, система) принято рассматривать подходящий способ понимания (трактовки, восприятия)