УДК 343.72

ФИШИНГ КАК ОСНОВНОЙ МЕТОД СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

А.С. ПЕТРОВСКАЯ
(Представлено: канд. юрид. наук, доц. Ю.Л. ПРИКОЛОТИНА)

Цифровизация сделала нашу жизнь более комфортной, но и более уязвимой. В статье дается характеристика информации как основной ценности и объекта неправомерных действий, представлено законодательное регулирование информационной безопасности, а также способы совершения преступлений, основанные на социальной инженерии и фишинге как основном ее методе.

Стремительный рост и масштабное распространение новых компьютерных технологий создали предпосылки для увеличения интенсивности информационного обмена до невиданного ранее в истории уровня. Накопленные массивы электронной информации создают широкие возможности для содействия всеобщему доступу к образованию, самовыражению и саморазвитию в соответствии с индивидуальными и социальными запросами. Все это позволяет человечеству, а именно физическим, юридическим лицам и индивидуальным предпринимателям шире реализовывать свои устремления и использовать личностный потенциал. В условиях информационного, цифрового общества владение информацией и доступ к ней становятся не только социальным, но и экономическим ресурсом. Именно потому информация в настоящее время может быть признана одной из основных ценностей и как ценность неизбежно оказывается объектом неправомерных действий.

Несмотря на нарастающую тенденцию предоставления доступа к информации согласно принципам открытости и доступности, все же отдельные ее виды требуют некого «утаивания» и потому защиты – технической, программной и юридической.

В зависимости от категории доступа информация делится на общедоступную и информацию, распространение и (или) предоставление которой ограничено. К информации, распространение и (или) предоставление которой ограничено, относится: информация о частной жизни физического лица и персональные данные; сведения, составляющие государственные секреты; служебная информация ограниченного распространения; информация, составляющая коммерческую, профессиональную, банковскую и иную охраняемую законом тайну; информация, содержащаяся в делах об административных правонарушениях, материалах и уголовных делах органов уголовного преследования и суда до завершения производства по делу; иная информация, доступ к которой ограничен законодательными актами Республики Беларусь. Такого рода информация имеет статус конфиденциальной, так как в отношении нее действует требование недопущения ее распространения и (или) предоставления без согласия ее обладателя или иного основания, предусмотренного законодательными актами [1].

Однако какими бы надежными и даже совершенными ни были бы технические и программные средства, какой бы строгой и продуманной ни была юридическая ответственность, лицо, имеющее к ней доступ, снижает надежность системы защиты. «Человеческий фактор» – устойчивое выражение, которым обозначают психические способности человека как потенциального и актуального источника информационных проблем при использовании этим человеком современных технологий. Потому «самое слабое звено» системы защиты конфиденциальной информации – человек, а не техника [2].

Действия, связанные с нарушением режима информационной безопасности, могут быть умышленными и неосторожными. К умышленным относятся действия, предусмотренные Кодексом об административных правонарушениях и Уголовным кодексом Республики Беларусь: несанкционированный доступ к компьютерной информации (ст. 23.4 Кодекса Республики Беларусь об административных правонарушениях, ст. 349 Уголовного кодекса Республики Беларусь), разглашение коммерческой или иной охраняемой законом тайны (ст. 23.6 Кодекса Республики Беларусь об административных правонарушениях), нарушение законодательства о защите персональных данных (ст. 23.7 Кодекса Республики Беларусь об административных правонарушениях), уничтожение, блокирование или модификация информации (ст. 350 Уголовного кодекса Республики Беларусь), неправомерное завладение компьютерной информацией (ст. 350 Уголовного кодекса Республики Беларусь). К неосторожным действиям относятся: утрата носителей информации, уничтожение или искажение информации по неосторожности. При этом человек может не осознавать, что его действия приводят к нарушению режима коммерческой или личной тайны [3].

Деяния неосторожного характера, составляющие нарушение режима защиты информации или компьютерных сетей, могут быть спровоцированы посредством использования злоумышленником методов социальной инженерии. Злоумышленники используют тактику социальной инженерии, так как использовать естественную склонность человека к доверию проще, чем искать способы преодоления технических средств защиты и программного обеспечения.

Отличительной чертой преступлений рассматриваемого вида является обстановка их совершения, образованная электронным устройством, виртуальной средой, а также дистанционностью противоправных действий [4]. То есть действия, вводящие в заблуждение, осуществляются в условиях, исключающих вербальный контакт с потерпевшим. По мнению В.Д. Зеленского и Г.М. Меретукова, «основой механизма мошенничества выступают «действия, слова, те или иные манипуляции преступников, направленные на вхождение в доверие к потерпевшим и вовлечение их в обман» [5].

Социальная инженерия, иногда называемая наукой и искусством взлома человеческого сознания, становится все более распространенной в связи с повышением роли социальных сетей, электронной почты и других видов онлайн-коммуникации. Множество случаев взлома основано на техниках социальной инженерии, что в последующем дает возможность злоумышленникам доставить вредоносное ПО на компьютеры жертв. Среди наиболее популярных – фальшивые обновления Flash Player и других популярных программ, вшитые в документ Word исполняемые файлы и многое другое.

В сфере информационной безопасности термин «социальная инженерия» широко используется для обозначения ряда техник, используемых киберпреступниками. Последние имеют своей целью выманивание конфиденциальной информации у жертв либо побуждение жертв к совершению действий, направленных на проникновение в систему (сеть) в обход системы безопасности [4].

Социальной инженерией признается метод несанкционированного доступа к информации или системам хранения информации без использования технических средств. Метод основан на использовании слабостей человека и потому является очень эффективным. Основная цель социальной инженерии – нелегальным способом получить доступ к информации [6]. В процессе осуществления незаконных действий злоумышленник использует методы (приемы, техники) социальной инженерии. Способы совершения преступлений с использованием методов социальной инженерии представляют собой совокупность приемов, являющихся вспомогательными средствами при неправомерном получении доступа к конфиденциальной информации пользователей для достижения корыстных целей с помощью информационных технологий.

Рассмотрим каждый из них.

Фишинг – техника интернет-мошенничества, направленная на получение конфиденциальной информации пользователей, – авторизационных данных различных систем. Основным видом фишинговых атак является поддельное письмо, отправленное жертве по электронной почте, которое выглядит как официальное письмо от платежной системы или банка. В письме содержится форма для ввода персональных данных (пин-кодов, логина и пароля и т.п.) или ссылка на web-страницу, где располагается такая форма [7].

Претекстинг – это набор действий, отработанных по определенному, заранее составленному сценарию, в результате которого жертва может выдать какую-либо информацию или совершить определенное действие. Чаще всего данный вид атаки предполагает использование голосовых средств, таких как Skype, телефон и т. п. [7].

«Троянский конь» – эта техника основывается на любопытстве, страхе или других эмоциях пользователей [7].

«Кви про кво» («Услуга за услугу») предполагает обращение злоумышленника к пользователю по электронной почте или корпоративному телефону с просьбой решения какой-либо проблемы, в процессе разговора злоумышленник получает персональные данные или секретную информацию [7].

«Дорожное яблоко» представляет собой адаптацию троянского коня и состоит в использовании физических носителей (CD, флеш-накопителей). Злоумышленник обычно подбрасывает такой носитель в общедоступных местах на территории компании (парковки, столовые, рабочие места сотрудников, туалеты) [6].

Обратная социальная инженерия – вид атаки, направленный на создание такой ситуации, при которой жертва вынуждена будет сама обратиться к злоумышленнику за «помощью» [7].

Как мы видим, по своему содержанию методы социальной инженерии многообразны, зачастую их виды дополняются более новыми и современными в связи с активной деятельностью мошенников и развитием научно-технического прогресса [2].

Одним из стремительно развивающихся методов социальной инженерии стал фишинг, поэтому считаем целесообразным разобрать подробно его характеристики.

Фишинг представляет собой сообщения в электронной почте, социальных сетях и мессенджерах, которые схожи с сообщениями от легальных организаций о том, что по какой-либо причине получателю требуется срочно совершить какое-либо действие (например, подтвердить учетную запись), при этом пользователя мотивируют чувствами срочности или выгоды (например, блокировка учетной записи, получение подарка от компании). Устойчивое развитие фишинга породило создание фишинговых сайтов и рассылку сообщений в популярных мессенджерах.

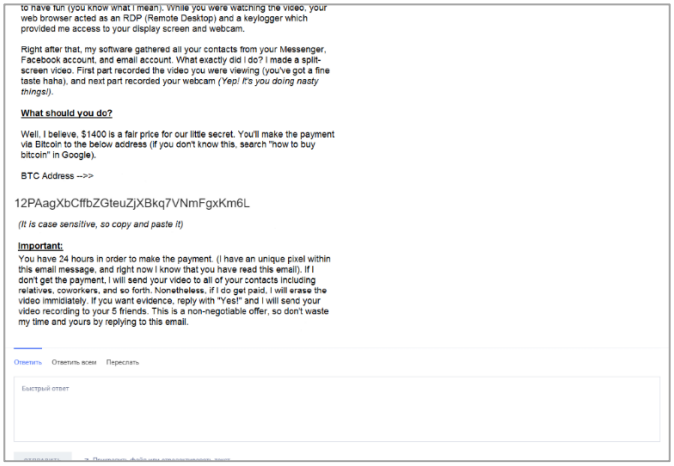
Наиболее частые жертвы фишинга – банки, электронные платежные системы, аукционы. То есть мошенников интересуют те персональные данные, которые дают доступ к деньгам и не только к ним.

Также популярность набирает кража личных данных из электронной почты – эти данные могут пригодиться тем, кто рассылает вирусы или создает зомби-сети. Характерной особенностью фишинговых

электронных писем является очень высокое качество подделки. Адресат получает письмо на электронную почту с логотипами банка/сайта/провайдера, выглядящее в точности так же, как настоящее. Ничего не подозревающий пользователь переходит по ссылке «Перейти на сайт и залогиниться», но попадает на самом деле не на официальный сайт, а на фишерский его аналог, выполненный с высочайшей точностью.

Поэтому одной из хитростей фишеров являются ссылки, очень похожие на URL оригинальных сайтов. Ведь достаточно наблюдательный пользователь может обратить внимание на то, что в командной строке браузера высвечивается ссылка, совершенно отличная от легитимного сайта. Часто они начинаются с IP-адреса, хотя известно, что настоящие солидные компании давно не используют подобные ссылки. Потому фишинговые URL часто похожи на настоящие. Они могут включать в себя название настоящего URL, дополненное другими словами (например, вместо www.examplebank.com стоит www.login-examplebank.com). Также в последнее время популярный фишинговый прием – ссылка с точками вместо слешей, внешне очень похожая на настоящую (вместо www.examplebank.com/personal/login стоит www.examplebank.com.personal.login). Можно привести еще такой фишерский вариант: www.examplebank.com-personal.login.

В дополнение к вышесказанному, в самом письме может высвечиваться ссылка на правомерный сайт, но реальный URL, на который она ссылается, будет другим. Бдительность пользователя притупляется еще тем, что в письме может быть несколько второстепенных ссылок, ведущих на официальный сайт, но основная ссылка, по которой пользователю надо пройти и залогиниться, ведет на сайт мошенников. Иногда личные данные предлагается ввести прямо в письме. Надо помнить, что никакой банк (либо другая организация, запрашивающая конфиденциальную информацию) не будет этого делать подобным образом. На рисунке приведен конкретный пример фишинга в электронной почте.


to have fun (you know what I mean). While you were watching the video, your web browser acted as an RDP (Remote Desktop) and a keylogger which provided me access to your display screen and webcam.

Right after that, my software gathered all your contacts from your Messenger, Facebook account, and email account. What exactly did I do? I made a split-screen video. First part recorded the video you were viewing (you've got a fine taste haha), and next part recorded your webcam *(Yep! It's you doing nasty things!)*.

What should you do?

Well, I believe, $1400 is a fair price for our little secret. You'll make the payment via Bitcoin to the below address (if you don't know this, search "how to buy bitcoin" in Google).

BTC Address -->>

12PAagXbCffbZGteuZjXBkq7VNmFgxKm6L

(It is case sensitive, so copy and paste it)

Important:
You have 24 hours in order to make the payment. (I have an unique pixel within this email message, and right now I know that you have read this email). If I don't get the payment, I will send your video to all of your contacts including relatives, coworkers, and so forth. Nonetheless, if I do get paid, I will erase the video immidiately. If you want evidence, reply with "Yes!" and I will send your video recording to your 5 friends. This is a non-negotiable offer, so don't waste my time and yours by replying to this email.

Ответить Ответить всем Переслать

Быстрый ответ

Рисунок 1. – Фишинг в электронной почте

Из примера мы можем выяснить, какие методы социальной инженерии использует мошенник по отношению к адресату. А именно мошенник мотивирует пользователя чувством срочности (у Вас есть 24 часа для того, чтобы произвести платеж), запугивает, используя шантаж (если я не получу оплату, то я отправлю Ваше видео всем Вашим контактам, включая родственников, коллег и т.д., но если Вы произведете оплату, то я немедленно удалю видео) за неуплату платежа, электронное письмо содержит ссылку, по которой долен перейти атакуемый. То есть, сообщение предназначено для того, чтобы адресат запаниковал и немедленно предпринял какие-либо меры.

Таким образом, фишинг как основной метод социальной инженерии свидетельствуют о том, что человек более уязвим, чем система. Ведь человек легко поддается чужому влиянию и психологической манипуляции посредством задействования мошенниками преступных схем. Именно поэтому преступники все чаще используют методы социальной инженерии для получения доступа к привлекающей их конфиденциальной информации пользователей, а также для достижения иных (не связанных с информацией) преступных целей. В связи с чем представлена обобщенная и систематизированная классификация способов совершения мошеннических действий рассматриваемой категории преступлений, анализ и изучение которых представляет существенное криминологическое и криминалистическое значение при раскрытии и расследовании преступлений, совершаемых с использованием информационных технологий.

ЛИТЕРАТУРА

1. Об информации, информатизации и защите информациий : Закон Респ. Беларусь от 10 нояб. 2008 г. № 455-З // Эталон / Нац. Центр правовой информ. Респ. Беларусь. – Минск, 2021.

2. Безопасность в интернете [Электронный ресурс]. – Режим доступа: http://info-helper.ru/files/prezent/security.pdf. – Дата доступа: 27.09.2021.
3. Что такое «фишинг» [Электронный ресурс]. – Режим доступа: https://encyclopedia.kaspersky.ru/knowledge/what-is-phishing/. – Дата доступа: 13.07.2021.
4. Косенков, А.Н., Черный Г.А. Общая характеристика психологии киберпреступника / А.Н. Косенков, Г.А. Черный // Криминологический журнал ОГУЭП. – 2012. – № 3(21). – С. 87−94.
5. Зеленский, В.Д., Меретуков Г.М. Криминалистика: учеб. пособие / В.Д. Зеленский, Г.М. Меретуков; Из-во Издательство «Юридический центр». – Санкт-Петербург, 2015. – 488 с.
6. Социальная инженерия, или Как «взломать» человека [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/blog/socialnaya-inzheneriya-ili-kak-vzlomat-cheloveka/2559/. – Дата доступа: 13.07.2021.
7. Краткое введение в социальную инженерию [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/83415/. – Дата доступа: 24.09.2021.
8. Социальная инженерия – как не стать жертвой [Электронный ресурс]. – Режим доступа: https://efsol.ru/articles/social-engineering.html. – Дата доступа: 27.09.2021.