Информационная справка по видам мошенничества.

Современные виды мошенничества

1. Мошенничество, основанное на применении социальной инженерии.
2. Телефонное мошенничество.
3. Компьютерное мошенничество.
4. Модификации банкоматов.
5. Поддельные карты.
6. Поддельные документы.

Мошенничество, основанное на применении социальной инженерии

Социальная инженерия — это использование знаний о человеческом поведении для направления его на достижение желаемых целей [1]. Угрозы мошеннических действий со стороны социальных инженеров остаются актуальными в течение многих веков. Как и раньше, мошенник использует ничего не подозревающих людей для совершения преступления. В этом ему помогают знание психологии, выбор удачного момента, правильной жертвы, умение убеждать в свое правоте.

Социальная инженерия подразделяется на прямую и обратную. Пример метода прямой социальной инженерии – обращение к сотруднику от имени вышестоящего руководства с требованиями выполнить определенные действия, которые создадут уязвимость в системе защиты и обеспечат злоумышленнику возможность несанкционированного доступа. В качестве примера обратной социальной инженерии можно привести ситуацию, когда злоумышленник заражает компьютер жертвы вирусами и в непринужденном разговоре «случайно» упоминает о том, что является специалистом по устранению подобных проблем, чем вынуждает человека самого обратиться за помощью к социальному инженеру.

Меры защиты от социальной инженерии:

1. Постоянные инструктажи сотрудников с приведением им примеров удачных атак социальных инженеров, в результате которых сотрудники понесли наказание за свою доверчивость.
2. Комплексная система безопасности, включающая в себя, как технические, так и организационные меры защиты.
3. Квалифицированные сотрудники СБ и сотрудники охраны, обладающие достаточным опытом в борьбе с социальными инженерами.
4. Проверки по типу «тайного покупателя», имитирующие атаку социального инженера.

Телефонное мошенничество (sms, звонки)

Тему телефонного мошенничества довольно полно раскрыл в своей книге Кевин Митник [2]. Телефонное мошенничество – один из видов социальной инженерии, который, в отличие от традиционных методов, предполагает активное использование средств телефонной связи.

Одним из ярких примеров современного телефонного мошенничества является рассылка СМС с текстом «Ваша карта заблокирована. Для разблокировки обратитесь по телефонному номеру: …». Дальше возможны два варианта развития событий: либо звонок на этот номер окажется

платным, либо злоумышленник будет убеждать, что необходимо совершить определенные операции для разблокировки карты, которые в итоге приведут к переводу денежных средств на счет злоумышленника.

Меры защиты от телефонного мошенничества:

1. Все меры, которые были указаны для защиты от социальной инженерии. Главное правило – стараться по возможности не перезванивать на незнакомые номера и не отвечать на СМС.
2. Проверка номера телефона в Интернете на наличие информации о мошеннических действиях.

Модификации банкоматов

При проведении операций с использованием банкоматов необходимо соблюдать несложные правила безопасности – не допускать подсматривания пин-кода посторонними лицами, пересчитывать выданные деньги, не забывать карту внутри банкомата. Эти правила знают все, однако, одних их недостаточно для того, чтобы защитить себя от мошенничества.

Можно выделить три популярных направления махинаций с банкоматами: использование технологических записей для доступа к программному обеспечению банкомата с целью незаконного получения денежных средств, скиминг – использование накладок для считывания данных карты, а также накладок на клавиатуру для считывания пин-кода, установка фальшивых банкоматов, оформленных в полном соответствии с настоящими.

Меры защиты от мошенничеств с банкоматами:

1. Необходимо знать, как выглядят накладки, для этого следует изучить информацию в Интернете, в том числе фотографии установленных в банкомат скимеров.
2. Также стоит запомнить, как должен выглядеть настоящий банкомат, особенное внимание следует обратить на картоприемник и клавиатуру – цвет, форма очень важны, накладки имеют внешнюю часть и при простом визуальном осмотре заметны.
3. Для защиты от фальшивых банкоматов обязательно нужно проверять адреса установки банкоматов на официальных сайтах банков.
4. Для защиты от использования в корыстных целях технологических учетных записей необходимо тщательно контролировать персонал, обслуживающий банкоматы, все операции должны совершаться минимум двумя сотрудниками.

Поддельные карты

Использование накладок на банкоматы оправдано только в случае дальнейшего изготовления поддельных пластиковых карт. Они содержат информацию, которая была записана на карте жертвы, проведение операций с фальшивой картой приводит к исчезновению денег со счета. Расследование затрудняется тем, что суммы обычно снимаются небольшие, каждый раз в разных местах, злоумышленники при этом применяют маскировку. Зачастую хозяевами карт являются иностранные граждане, поэтому уголовные дела возбуждаются не так часто.

Меры защиты от поддельных пластиковых карт:

1. Для физических лиц - хранение карты в недоступных местах, хранение пин-кода не рекомендуется.

2. Для организаций – видеонаблюдение в банкоматах, в помещениях, где установлены банкоматы, обращение в органы внутренних дел при выявлении нарушения.

Поддельные документы

Если раньше поддельные документы изготавливались злоумышленниками «на коленке», то в настоящее время существуют программные и технические средства, фирмы, предоставляющие подобные услуги. В качестве примера можно привести специальные программы по изготовлению копий паспортов. На выходе злоумышленник получает полноценный скан паспорта, выполненный на государственном бланке.

Меры защиты от предъявления поддельных документов:

1. Нужно обязательно требовать оригиналы документов или их заверенные копии, стараться не принимать временные удостоверения личности, которые не имеют должной степени защиты.

2. Следует внимательно изучать предоставленные удостоверения личности на предмет замены фотографии, соответствует ли она лицу, предъявившему документ. Край печать должен быть четким и ровным, также необходимо проверять на специальном оборудовании наличие специальных знаков, проявляющихся при УФ излучении.

3. Обязательно проводить инструктажи сотрудников о признаках подделки документов, в том числе иностранных граждан. Очень немногие люди знают, как выглядит удостоверение личности гражданина Китая или Южной Кореи.

Компьютерное мошенничество

Согласно статье 159.6 УК [3] под компьютерным мошенничеством понимается хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Исходя из этого определения, можно выделить несколько групп мошенничества:

1. Ввод компьютерной информации. *Пример: ввод логина и пароля зарегистрированного пользователя и получение, таким образом, легального доступа к ресурсам локальной сети предприятия, чтобы в дальнейшем осуществить хищение чужого имущества.*

2. Удаление компьютерной информации. *Пример: удаление информации на сайте о мерах безопасности, которые должен соблюдать пользователь, а также о случаях мошенничества.*

3. Блокирование компьютерной информации. *Пример: блокирование настроек безопасности межсетевого экрана для дальнейшего получения доступа к информационным ресурсам.*

4. Модификация компьютерной информации. *Пример: подмена платежных реквизитов для незаконного получения денежных средств.*

5. Иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. *Пример: установление «закладок» в программное обеспечение, несанкционированное подключение к сетям связи.*

Чаще всего различные методы используются совместно. Пример: отправка сообщения легальному пользователю с целью заражения компьютера. Троянская программа, содержащаяся в письме, осуществляет сбор информации (логины, пароли), удаление правил безопасности межсетевого экрана и модификацию таблицы разрешенных ip-адресов. Затем нарушитель получает полный доступ к информационным ресурсам путем ввода полученного логина и пароля со своего компьютера.

Меры защиты от компьютерного мошенничества:

1. Назначение ответственных лиц, главный – директор, личная заинтересованность, остальные начальники – каждый в своей области.
2. Инструктажи персонала и клиентов.
3. Служебные расследования.
4. Установка и настройка средств защиты информации.

Популярные виды мошенничества в сфере компьютерной информации:

1. Фишинговые письма.
2. Вирусные атаки и заражения троянскими программами.
3. Социальная инженерия с использованием средств вычислительной техники.
4. Несанкционированный доступ к системе дистанционного банковского обслуживания.
5. Подмена сайта компании.
6. Подделка электронной подписи. Мошенничества на интернет-аукционах.
7. Действия внутренних злоумышленников.

Отдельно хочется отметить фишинг, как один из наиболее активно развивающихся видов мошенничества. Фишинговые письма представляют собой электронные сообщения от злоумышленника, оформленные, как официальное письмо от банка, университета, провайдера, они направляются с целью получения логина и пароля пользователя к информационной системе с целью присвоения денежных средств, либо других ценных ресурсов. Такие письма содержат ссылки на сайт-копию организации, от имени которой якобы отправлено это письмо. Пользователь вводит свои данные на поддельном сайте, чем в результате и пользуются злоумышленники. Благодаря невнимательности и халатному отношению пользователей, фишинговые письма используются мошенниками довольно успешно.

Меры защиты от фишинга:

1. Банки никогда не будут просить прислать им логин и пароль. Любое письмо с просьбой подтвердить свои данные должно вызывать подозрения и внимательно изучаться.
2. Перед тем как переходить по ссылкам, указанным в любом электронном сообщении, необходимо проверить ее в браузере, является ли предлагаемый ресурс настоящим адресом сайта.
3. Подпись ссылки может не соответствовать самой ссылке. Проверять стоит саму ссылку.
4. Внимательно изучайте текст письма, часто мошенники допускают очевидные грамматические и синтаксические ошибки.

5. При возникновении подозрений, необходимо обратиться в службу технической поддержки и проверить, осуществлялась ли подобная рассылка.

6. Важно помнить, что даже если письмо пришло с настоящего электронного ящика банка, его нужно тщательно изучить: возможно злоумышленник получил доступ к электронной почте.

Излишнее проявление доверия к незнакомым людям, письмам с неизвестных адресов, смс и звонкам приводит к негативным последствиям, чтобы их избежать, необходимо проявлять бдительность и осознавать возможные риски своих действий.