**Использование ИТ-технологий и методов социальной инженерии для совершения преступлений**

Наше поколение живет в таком времени, в котором почти все люди владеют той или иной информацией. Поэтому роль информационных технологий огромна в жизни каждого из нас. И порой невозможно представить нашу жизнь без этих технологий.

На сегодняшний день, с помощью современных устройств (компьютеры, смартфоны, планшеты, смарт-часы и т.п.) наша жизнь стала намного проще и удобнее

К сожалению, информационные технологии используются не только во благо, но и во вред, например для совершения преступлений. Преступления против собственности, совершаемые с использованием информационных технологий или в сфере компьютерной информации как гражданами, так и организациями, продолжают оставаться одними из самых трудно раскрываемых по причине специфики механизма совершения преступления. Преступления могут совершаться любым лицом, имеющим необходимые навыки работы, включая школьников и лиц, отбывающих наказание в местах лишения свободы.

Потерпевшим от данных преступлений может стать любой человек, имеющий доступ к конфиденциальной информации или обладающий пластиковой картой, привязанной к банковскому счету.

Злоумышленники обладают большим спектром методов совершения преступлений, одним из которых является социальная инженерия, с развитием информационных технологий получивший более широкое распространение.

Метод социальной инженерии - это метод несанкционированного доступа к конфиденциальной информации (пароли, банковские данные и т. д.) или системам хранения информации, основанный на особенностях психологии людей. Злоумышленник получает информацию, например, путем сбора информации о служащих объекта атаки с помощью телефонного звонка или путем проникновения в организацию под видом ее служащего. Злоумышленник может позвонить работнику компании (под видом технической службы) и выведать пароль (или иную необходимую информацию), сославшись на необходимость решения небольшой проблемы в информационной системе. С применением информационных технологий и методов социальной инженерии преступления стали более изощренными и трудно раскрываемыми.

Рассмотрим ряд наиболее часто применяемых методов социальной инженерии.

**Претекстинг.** Это действие, отработанное по заранее составленному сценарию (претексту). В результате цель (жертва) должна выдать определённую информацию или совершить определённое действие. Этот вид атак применяется обычно по телефону. Чаще эта техника включает в себя больше, чем просто ложь, и требует каких-либо предварительных исследований (например, персонализации: выяснение имени сотрудника, занимаемой им должности и названия проектов, над которыми он работает), с тем, чтобы обеспечить доверие цели.

**Пример 1.** Поступает звонок от якобы сотрудника службы технической поддержки оператора мобильной связи с предложением подключить новую эксклюзивную услугу или для перерегистрации во избежание отключения связи из-за технического сбоя, или для улучшения качества связи. Для этого абоненту предлагается набрать под диктовку код, который является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников.

**Пример 2.** Мошенник звонит или отправляет SMS/MMS–сообщение на мобильный телефон, представляется сотрудником банка или иной коммерческой организации, сообщает потерпевшему о начислении бонусов на банковский счет и просит сообщить пришедшие посредством SMS-сообщений персональные данные по банковскому счету, после чего, получив соответствующие необходимые данные с банковского счета потерпевшего, похищает денежные средства.

**Пример 3.** Мошенник звонит или отправляет SMS–сообщение на телефоны, сообщая информацию о том, что банковская карта или счет мобильного телефона заблокированы в результате преступного посягательства, а затем, представляясь сотрудником банка или телефонной компании, предлагает набрать комбинацию цифр на сотовом телефоне или банкомате якобы для разблокировки, в результате чего денежные средства перечисляются на счет мошенника или его доверенного лица.

**Пример 4.** На сотовый телефон абонента приходит сообщение о том, что его банковская карта заблокирована и ему предлагается бесплатно позвонить на определенный номер для получения подробной информации. Когда владелец карты звонит по указанному телефону, ему сообщают о том, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и пин-код для ее перерегистрации. Получив реквизиты банковской карты, злоумышленники переводят денежные средства на свой телефон, а затем снимают их со счета.

**Фишинг.** Техника, направленная на жульническое получение конфиденциальной информации. Обычно злоумышленник посылает жертве email, подделанный под официальное письмо — от банка, платёжной системы, Интернет-магазина — требующее «проверки» определённой информации или совершения определённых действий. Это письмо обычно содержит ссылку на фальшивую web-страницу, имитирующую официальную, с корпоративным логотипом и содержимым, и содержащую форму, требующую ввести конфиденциальную информацию — от домашнего адреса до пин-кода банковской карты.

**Пример.** Мошенничество при покупке товаров через сеть «Интернет». а электронную почту жертвы приходит письмо якобы от Интернет-магазина (например, AliExpress.com) с информацией о действующих на текущий период акциях и купонах с ссылкой на фальшивую web-страницу, имитирующую официальную, с корпоративным логотипом и содержимым. Жертва оформляет и оплачивает заказ, но не получает его, т.к. деньги перечислены на счет злоумышленника, а не продавца.

**Троянский конь**. Эта техника эксплуатирует любопытство либо алчность цели. Злоумышленник отправляет email, содержащий во вложении важное обновление антивируса, компромат на сотрудника или же информацию об аресте его денежных средств, находящихся на банковском счете. Такая техника остаётся эффективной, пока пользователи будут слепо кликать по любым вложениям.

**Пример.** На мобильный телефон жертвы направляется сообщение о наличии у него административного штрафа и с предложением загрузить по Интернет-ссылке приложение для получения более подробной информации. Пройдя по этой ссылке, пользователь вместо обещанного официального приложения скачивает себе вредоносную (троянскую) программу, которая способна, при наличии подключенной услуги «Мобильный банк», без участия абонента запрашивать баланс и выводить денежные средства с лицевого счета абонента на электронные кошельки злоумышленников.

**Дорожное яблоко**. Этот метод атаки представляет собой адаптацию троянского коня и состоит в использовании физических носителей. Злоумышленник может подбросить инфицированный CD-диск или карту памяти в месте, где их можно легко найти (коридор, лифт, парковка). Носитель подделывается под официальный и сопровождается подписью, призванной вызвать любопытство.

**Пример:** Злоумышленник может подбросить CD-диск, снабжённый корпоративным логотипом и ссылкой на официальный сайт компании цели, и снабдить его надписью «Заработная плата руководящего состава за 2019 год». Диск может быть оставлен на полу лифта или в вестибюле. Сотрудник по незнанию может подобрать диск и вставить его в компьютер, чтобы удовлетворить своё любопытство.

**Обратная социальная инженерия**. Целью обратной социальной инженерии является заставить цель саму обратиться к злоумышленнику за «помощью». С этой целью злоумышленник может применить следующие техники: диверсия (создание обратимой неполадки на компьютере жертвы), реклама (злоумышленник подсовывает жертве объявление вида «Если возникли неполадки с компьютером, позвоните по такому-то номеру»).

Учитывая, что мошенники совершают серию однотипных преступлений, эффективность раскрытия и расследования преступлений данной категории напрямую зависит от своевременного сообщения потерпевшими всех обстоятельств совершенного преступления.

**Чтобы не стать жертвами мошенников, следует придерживаться следующих советов:**

1. Не сообщайте никому реквизиты вашей карты. Ни одна организация, включая банк, не имеет право требовать данные вашей пластиковой карты. Чтобы проверить поступившую информацию о блокировании карты, следует позвонить в клиентскую службу поддержки банка. Скорее всего, вам ответят, что никаких сбоев на сервере не происходило, а ваша карта продолжает обслуживаться банком.

2. Не спешите переходить по ссылкам на Интернет-сайты. Проверьте ссылку (побуквенно) на соответствие официальному сайту. Скопируйте ссылку и вставьте в поисковике (Яндекс, Google и т. д.), прочитайте комментарии.

3. Скачивайте приложения с официальных источников. Не доверяйте сторонним приложениям. Если все-таки возникает необходимость использования сторонних приложений, то внимательно изучите его, прежде чем загружать его на свое устройство.

4. Перед использованием носителя информации (CD-диск, USB Flash и т. д.) проверьте его на наличие вредоносных программ.

5. SMS-сообщения могут быть весьма разнообразны, поэтому стоит критически относиться к таким сообщениям и не спешить выполнить то, о чем вас просят. Лучше позвоните оператору связи, узнайте, какая сумма спишется с вашего счета при отправке SMS-сообщения или звонка на указанный номер, затем сообщите о пришедшей на ваш телефон информации. Оператор определит того, кто отправляет эти SMS, и заблокирует его аккаунт.