Социальная инженерия – примитивный тип мошенничества, который не требует ни больших финансовых вложений, ни глубоких технических знаний, главная сложность в том, что банки не могут контролировать своих клиентов, которые, поддавшись обману, отдают деньги мошенникам. В контексте информационной безопасности социальная инженерия - это психологические и социологические приемы, набор условий и обстоятельств, которые максимально эффективно позволяют получить конфиденциальную информацию. В первую очередь идет речь о «взломе» подсознания человеческого мозга. Специалистов, которые используют эти приемы на практике, называют социальными инженерами. С каждым годом, с развитием онлайн-технологий, число таких «инженеров» растет, и все больше людей теряют средства, становясь жертвами мошенников. С помощью методов социальной инженерии создаются определенные условия для человека, при которых достигается степень доверия для получения или внушения требуемой информации.

**Физиология мошенничества методом социальной инженерии. Почему жертва доверяет мошеннику?**

Социальная инженерия основана в первую очередь на работе разума и подсознания человека. Подсознание отвечает за эмоции и работает значительно быстрее (рефлекторная реакция организма при возникающей угрозе), временная задержка между выводами подсознания и разума позволяет совершать мошеннические действия. Чем дольше в стрессовой не включается разум, тем больше мошенник может оказывать свое влияние. Обычный сценарий действий мошенника заключается в непрекращающемся взаимодействии с жертвой, бесконечное количество вопросов и обещаний, нагнетание стрессовой ситуации не позволяет включиться разуму, и «холодной» головой обдумать происходящее.

Этапы работы мошенника методами социальной инженерии включают:

* составление легенды, якоря для входа в доверие. Мошенники представляются сотрудниками силовых структур, социальных служб, работниками Банка, обязательно называют Банк, обращаются к жертве по имени, называют свое ФИО и должность. Подсознание делает вывод, что вероятнее всего мошенник действительно является тем, кем он себя обозначил, так как он владеет достоверной информацией;
* установление контакта. От мошенника поступает информация о незаконных списаниях средства со счета жертвы, попытках взять кредит под залог вклада, различных социальных программах по вычету потраченных денежных средств и т.д. Этот якорь вводит потенциальную жертву в состояние шока, выводит человека на эмоции и затормаживает работу разума;
* совершение мошеннических действий. После установления контакта и подготовки жертвы мошенник предлагает варианты решения сложившейся ситуации. В случаях с хищением предлагается перенести денежные средства на «безопасный, сберегательный» счёт, при легенде с социальным работником, который предлагает вернуть потраченные на лекарства и лечение средства, мошенник предлагает выполнить оплату юридических услуг и т.д.;
* выход из контакта. Мошенник в завершении разговора оставляет полную уверенность в будущем контакте и продолжении работы, оперирует обещаниями, передает свои контактные данные для обратной связи, диктует номер уголовного дела или договора и т.д.

**Как защитить себя при разговоре с мошенником?**

Прежде всего следует понимать, что каждая легенда мошенника – это набор последовательных действий, которые подготовлены заранее и варьируются в зависимости от ответов потенциальной жертвы. Любое нестандартное поведение или ответы могут ввести мошенника в заблуждение. Важно совершить следующие действия:

* выиграть время. Попросить потенциального мошенника изложить все вопросы сразу, сославшись на занятость, затем попросить перезвонить, запросить контактные данные. Сообщить о своей некомпетентности, неосведомленности и взять время на принятие решения или продолжение разговора;
* получив паузу, перепроверить информацию, обратиться к сотруднику Банка, поговорить с близкими, обсудить сложившуюся ситуацию. Успокоиться и не позволять эмоциям взять верх над разумом;
* выйти из сложившейся ситуации. Твердо стоять на своей позиции, не брать трубку при повторном звонке, сообщить звонящему о передаче информации о факте мошенничества уполномоченным органам.

Не следует исключать, что может поступить звонок из Банка, при этом он будет нести лишь предупредительный характер и позволит сохранить решение лишь за Вами. В свою очередь при попытке выиграть время мошенники будут настаивать на ускорении принятия навязываемого решения, всеми способами не давать время на раздумья, сбивать с толку и выводить на эмоции, противодействовать попыткам разорвать контакт.

Важно помнить, что мошеннические действия могут подразумевать несколько сценариев, может поступить два или более звонка от разных людей. Например, сначала происходит обращение от службы безопасности Банка. В том случае, если жертва рушит данный сценарий и выходит из контакта, следом поступает повторный звонок от силовых структур. Мошенник заявит, что он осведомлен о факте правонарушения, принимает меры и хочет наказать нарушителя, но нужна помощь жертвы. В таком случае следует вновь выиграть время и не поддаваться эмоциям, выйти из контакта.

Технологии позволяют выполнять подмену номера телефона, обманывать определитель номера телефона звонящего, вносить ложную информацию в сервисы GetContact и т.д.. Проверяйте информацию, консультируйтесь с близкими, друзьями и коллегами, обращайтесь к сотрудникам Банка и полиции по официальным номерам телефонов, прежде чем совершить действия, предлагаемые мошенниками.