

Методы социальной инженерии

Сергей Венцель — начальник отдела аналитической и образовательной деятельности НЦПТИ.

Ежедневно мы читаем новости о жертвах мошенничества и завербованных в совершение преступлений. Подвержены таким угрозам все: и обучающиеся в школах и университетах, и работающие взрослые, и вышедшие на пенсию. Столкнуться с мошенниками и вербовщиками можно как онлайн, так и в реальной жизни.

В основе действий преступников находится такое незамысловатое явление, как «социальная инженерия». Эту формулировку мы часто слышим в новостях в контексте очередной мошеннической аферы. Разберемся с термином.

Социальная инженерия — это совокупность психологических методов воздействия на поведение человека с целью обмана. По сути, речь идет о нарушении когнитивных процессов человека по анализу, обработке и использованию информации. Если говорить простым языком, это профессиональный обман и давление на человека для совершения им мошеннических действий.

Ловушки, которыми пользуются мошенники

Игра на эмоциях. В психологии есть термин «базовые эмоции», т. е. врожденные, универсальные эмоциональные реакции. Они возникают автоматически, не требуют обдумывания и помогают человеку выживать и адаптироваться. Некоторые ученые выделяют шесть таких эмоций, некоторые — восемь. В их число входит:

Радость	сигнализирует о безопасности	о и
----------------	------------------------------	--------

	удовлетворении потребностей
Печаль	помогает принять человеку потерю и переосмыслить происходящее
Страх	предупреждает об опасности и готовит наше тело к отходу от угрозы
Гнев	дает нам энергию для борьбы с несправедливостью или нарушением границ
Отвращение	становится своего рода щитом перед тем, что организм воспринимает как токсичное или потенциально опасное
Удивление	помогает ориентироваться в неожиданных ситуациях для их оценки
Наслаждение	помогает психике избавиться от внутреннего напряжения и восстановить важные функции организма

Именно под воздействием эмоций люди могут совершать самые нелогичные и рискованные шаги. Например, испытанный гнев может привести к конфликту на национальной или религиозной почве. Из-за страха, в том числе за свою жизнь или за безопасность семьи, человек может пойти на совершение преступления. Или ради получения

определенного наслаждения человек может выйти за рамки моральных норм.

Создание атмосферы срочности. Например, предложение здесь и сейчас получить сумму денег, не предпринимая каких-либо действий (кроме, например, перехода по присланной ссылке). Или требование быстро что-либо сделать: поджечь релейный шкаф, потому что «за твоими родственниками скоро приедут, их обвинят в госизмене, но только ты можешь их спасти».

Попытка войти в доверие. Мошенник, поиграв с эмоциями и создав ощущение срочности, показывает, что «только он тебя понимает, только он может помочь и только вместе с ним ты решишь возникшую проблему».

Как это работает на практике?

Мы сталкиваемся с разными схемами: от вирусных атак для выманивания денег или иных данных до точечных прозвонов под видом «сотрудника банка», «сотрудника спецслужб» и так далее.

Мошенники достаточно активны и в определенные временные периоды. Например, перед сдачей налоговой декларации 3-НДФЛ в инспекцию (где срок подачи — не позднее 30 апреля ежегодно) мошенники могут адресно рассылать на электронные почты письма с требованием быстрее предоставить данные, отнести документы по определенному адресу. В таких случаях нужно либо зайти в свой личный кабинет налогоплательщика для уточнения информации, либо позвонить в инспекцию по району проживания. Особо благоприятная для мошенника пора — предпраздничные периоды (например, перед Новым годом), когда человек занят покупками подарков, сдачей отчетности по работе или подготовкой к зачетной неделе и сессии в университете. В такие периоды его легко подловить.

Перед атакой мошенники могут предварительно собрать данные о потенциальных жертвах. Например, проанализировать какую-то компанию, создать аккаунт в мессенджере маскируясь либо под «директора компании», либо под «начальника службы безопасности» и затем звонить и писать по полученным в открытом доступе контактам. При поступлении такого звонка важно оперативно сообщить своему непосредственному начальнику о случившемся и ждать инструкций.

Чтобы лучше понять феномен социальной инженерии, разберем известные примеры из литературы и кино.

Начнем с легендарного персонажа — Остапа Бендера. Это главный антигерой романов И. Ильфа и Е. Петрова «Двенадцать стульев» и «Золотой теленок». Это мошенник и авантюрист, «великий комбинатор», «идейный борец за денежные знаки», знавший «четыреста сравнительно честных способов отъема (увода) денег». Среди его методов было и создание фиктивных контор, и блестящие речи про междупланетный шахматный конгресс и обустройство населенного пункта Васюки. Герой кинокартины превосходно показал зрителю, как можно убедить собеседника в том, чего не существует, используя правильные методики. Вообще, советская классика полезна для понимания многих современных процессов, и онлайн-мошенничество не является исключением.

Достаточно поучителен в разъяснении методов социальной инженерии американский фильм «Поймай меня, если сможешь» с Л. Ди Каприо и Т. Хэнксом. Обман от главного антигероя фильма строился на понимании поведения людей, в том числе в контексте профессий. Поэтому, не имея образования врача или пилота, но внушая доверие за счет манеры держаться и внешнего вида, персонаж достигал своих целей. Однако в итоге его арестовали.

Как мошенники достигают успеха?

Секрет кроется в знании психологии, собственной уверенности и умении убеждать. Профессиональный мошенник сможет убедить свою жертву в чем угодно, даже в бессмыслице, причем сам мошенник вряд ли будет в такое верить.

Что поможет обезоружить мошенника?

Уметь контролировать свои эмоции. Не поддавайтесь попыткам манипуляций со стороны тех, кто пытается играть нашими эмоциями: от страха до жажды выгоды или наслаждения.

Не распространять о себе много информации в публичном поле. Чем меньше информации о вас получают мошенники перед звонком, тем вероятнее их неуспех в попытке обмануть вас.

Знать алгоритмы действий при опасности: от звонка от якобы «сотрудника ФСБ» до сообщения на электронную почту от якобы «сотрудника налоговой службы».