# Памятка о способах социальной инженерии и необходимых мерах безопасности

Социальная инженерия или «атака на человека» — это совокупность психологических и социологических приёмов, методов и технологий, которые позволяют получить доступ к конфиденциальной информации.

Киберпреступники все чаще используют методы социальной инженерии для проникновения в инфраструктуру организации при целевой атаке. Согласно статистике, количество атак с использованием социальной инженерии в 2021 году выросло на 216%. Злоумышленники, предпринимая попытки найти доступ к системе или ценным данным, используют самое уязвимое звено — человека. Простой пример — телефонный звонок, где преступник выдаёт себя за кого-то другого, пытаясь узнать у абонента конфиденциальную информацию, играя на чувствах человека, обманывая или шантажируя его. К сожалению, многие продолжают попадаться на такие ловушки и доверчиво рассказывают социальным хакерам всё, что им нужно.

Человеческий фактор по-прежнему остается слабым звеном в любой системе защиты, поэтому сегодня как никогда возрастает потребность в обучении сотрудников основам информационной безопасности.

Также стоит отметить, что на текущий момент социальная инженерия установила прочную связь с киберпреступностью,

## Рассмотрим самые популярные методы социальной инженерии

Так называемая «Атака на человека» может производиться по многим сценариям, но существует несколько наиболее распространённых техник работы злоумышленников.

### Фишинг

*Основной упор на невнимательность.*

Метод сбора пользовательских данных для авторизации — обычно это массовые рассылки спама по электронной почте. В классическом сценарии на почту жертвы приходит поддельное письмо от какой-то известной организации с просьбой перейти по ссылке и авторизоваться (ввод комбинации логин/пароль). Чтобы вызвать больше доверия, мошенники придумывают серьёзные причины для перехода по ссылке: например, просят потенциальную жертву обновить пароль или ввести различного рода персональную информацию (ФИО, номер телефона, должность и т.д.).

### Троян

*Основной упор на невнимательность, доверие.*

Вирус не зря получил своё название по принципу работы троянского коня из древнегреческого мифа. Только приманкой здесь становится email-

сообщение, которое при классическом сценарии мошенников обещает быструю прибыль, выигрыш или другие «золотые горы» — но в результате человек получает вирус, с помощью которого злоумышленники крадут его данные. Данный вид атаки тоже необходимо относить к методам социальной инженерии, потому что создатели вируса как правило хорошо знают, как замаскировать вредоносную программу, чтобы вы наверняка кликнули по нужной ссылке, скачали и запустили файл.

Часто сотрудники непреднамеренно помогают злоумышленнику в развитии атаки, пересылая зараженное письмо коллегам с просьбой открыть вложение или перейти по ссылке. Например, в теле письма используются формулировки из повседневной служебной деятельности. «Уважаемые начальники подразделений, направляем график отпусков на текущий год. Просим довести до сотрудников и т.д. С уважением, отдел кадров». При положительном для злоумышленников развитии событий письмо пересылается по организации. В свою очередь сотрудник, получивший письмо уже от своего коллеги абсолютно не подозревает о наличии ссылок на вредоносное ПО.

Как только злоумышленник убедился, что сотрудник принял его за коллегу или какое-то доверенное лицо, распространил письмо по организации, в ходе дальнейшей переписки он может попытаться получить нужную ему информацию, не вызывая подозрений. Так можно узнать версию используемого ПО, наличие антивируса на рабочем компьютере, электронную почту других сотрудников, номера мобильных телефонов, структуру компании. Все это представляет ценность и может использоваться при планировании и проведении последующих социотехнических атак.

Злоумышленники часто опираются на страх, жадность, надежды, ожидания и другие эмоции, которые могут заставить пользователя поддаться сиюминутной слабости. Когда внезапно на почту приходит письмо «список сотрудников на увольнение» — пользователь забывает об элементарных правилах техники кибербезопасности, он даже не задумывается, почему ему вообще пришло подобное письмо.

Часто бывает так, что именно тема письма побуждает сотрудника открыть его, перейти по ссылке, скачать и запустить файл, не разбираясь — кто адресат и почему домен отправителя написан как-то странно.

Если недостаточно внимательно отнестись к прочтению такого письма, то подвох заметить непросто.

Предсказуемо страх увольнения или сокращения — достаточно мощный фактор, чтобы забыть о правилах информационной безопасности: письма с такой темой в большинстве случаев побуждали пользователей совершить потенциально опасное действие. Высокий процент успеха показывают письма, где есть слова «премия», «поощрение», «повышение зарплаты»:

Злоумышленник может также попытаться привязать тему рассылки к какому-то знаменательному событию (если располагает, например, сведениями о недавно прошедшем в компании корпоративе), профессиональным и государственным праздникам.

**Дорожное яблоко**

*Основной упор на доверчивость, любопытство*

Представляет собой адаптацию троянского коня и состоит в использовании физических носителей (CD, флэш-накопителей). Злоумышленник обычно подбрасывает такой носитель в общедоступных местах на территории компании (парковки, столовые, рабочие места сотрудников, туалеты). Для того, чтобы у сотрудника возник интерес к данному носителю, злоумышленник может нанести на носитель логотип компании и какую-нибудь подпись. Например, «данные о продажах», «зарплата сотрудников», «отчет в налоговую» и другое.

**Услуга за услугу**

*Основной упор на доверчивость*

Используя этот метод, злоумышленник представляется сотрудником службы технической поддержки и спрашивает о наличии сбоев в работе программного обеспечения, предлагает исправить возникшие неполадки в системе либо предупредить о вероятности их наступления, хотя на самом деле проблем в работе ПО не возникало. Жертва верит в наличие неисправностей и, выполняя указания хакера, лично передаёт ему доступ к важной информации.

Распространенный сценарий, когда пользователь сам говорит об отсутствии времени и сообщает необходимые пароли для того, чтобы сотрудник технической поддержки самостоятельно провел необходимые манипуляции.

**Обратная социальная инженерия**

*Основной упор на доверчивость, невнимательность*

Методика направлена на то, чтобы жертва сама обратилась к социальному инженеру и выдала ему необходимые сведения. Это может достигаться несколькими путями:

**Внедрение особого ПО**

*Основной упор на невнимательность*

На электронную почту поступает письмо, информирующее о возможных сбоях в работе часто используемого программного обеспечения (например, пакет офисных программ). В этом же письме указаны контактные данные

специалиста технической поддержки, используемые злоумышленником. При возникновении сбоя в работе вышеперечисленного ПО, пользователь вспоминает о ранее поступившем предупреждении и связывается со злоумышленником в лице технического специалиста.

Таким образом, ситуация заранее подстроена, пользователь связывается с социальным хакером. Налаживая работу ПО, производятся необходимые для взлома манипуляции. А когда взлом обнаруживается, социальный инженер остаётся вне подозрения (поскольку создается впечатления, что он помогал вам).

## ЗАКЛЮЧЕНИЕ

С учетом изложенного, самые распространенные сценарии вышеуказанных атак реализуются путем email-рассылок.

Причиной тому относительная дешевизна и простота таких методов, а также высокая эффективность.

На текущий момент целевой вектор подобных атак значительно сместился от получения доступа к информации к её уничтожению (блокированию) путем применения вирусов-шифровальщиков.

Для рядовых пользователей самый актуальный и действенный совет — всегда оставаться бдительными, проверять информацию об отправителе, прежде чем перейти по ссылке или скачать предлагаемый файл — убедиться, что это не вредоносный ресурс. Полученные файлы перед открытием необходимо проверить с помощью антивирусного ПО. Стоит также удостовериться, что домен отправителя легитимный и реальный. В случае возникновения сомнений, рекомендуется проверить, действительно ли адресат отправлял данное письмо и является ли он настоящим владельцем домена и (или) электронного ящика, связавшись с ним каким-то альтернативным способом, например, через мессенджер или по телефону.

Своевременное выявление и пресечение атаки позволит избежать серьезных последствий.

Что касается организационных мер, то основой является систематическое повышение осведомленности сотрудников в области информационной безопасности.

Исследование компаний в области ИБ показывают, что 38% организаций вообще не проводят тренинги для сотрудников по вопросам ИБ, а 37% делают это формально, без какой-либо проверки эффективности. Хотя проводить периодическое обучение с контролем информированности каждого сотрудника крайне важно. При этом процесс повышения осведомленности должен в первую очередь быть направлен на практическую сторону обеспечения

безопасности, а каждый сотрудник должен понимать свои обязанности и ответственность за обеспечение ИБ.

Отличная практика, когда сотрудники оповещают подразделения ИБ о том, что им пришло сомнительное письмо, особенно если заметно, что над рассылкой тщательно поработали. В таком случае, даже если заражение или утечка имели место, еще можно успеть оперативно отреагировать на атаку и принять контрмеры.

**Основные меры по защите от вышеперечисленных видов социальных атак.**

- **Сохраняйте бдительность**. Всегда обращайте внимание на отправителя писем и адрес сайта, где собираетесь ввести какие-то личные данные. Если это почта на домене крупной организации, удостоверьтесь, что домен именно такой и в нём нет опечаток. Если есть сомнения — свяжитесь с техподдержкой или представителем организации по официальным каналам.
- **Используйте только доверенные носители информации**.
- **Не переходите на подозрительные сайты и не скачивайте сомнительные файлы**, один из самых лучших помощников социальной инженерии — любопытство.
- **Не используйте один и тот же пароль** для доступа к личным и корпоративным (рабочим) ресурсам.
- **Использование антивирусного программного обеспечения**. Недопущение его отключения.
- **Систематический инструктаж**. Все сотрудники должны быть проинструктированы о том, как вести себя при обнаружении попыток или осуществления незаконного проникновения.