

Республика Марий Эл
Горномарийский район
МБОУ «Усолинская средняя общеобразовательная школа»

Доклад на тему:
Информационная безопасность. Социальная инженерия.

Учитель физики и информатики
Мельников Эдуард Юрьевич

с.Усола 2020 г.

Социальная инженерия — это молодая наука, которая находится на стыке знания психологии человеческих ошибок», так как эта наука вбирает в себя всё, что связано с человеческим фактором и его людей и их поведения в критических ситуациях. Ее также можно назвать «копилкой использованием».

В качестве социолога социальный инженер:

- Анализирует и объясняет различные социальные явления и процессы;
- Использует принципы и методы анализа, обработки и обобщения данных социологических исследований;
- Разрабатывает программно-методическое обеспечение исследовательского процесса;
- Организует деятельность социологической службы.

А как инженер он владеет инженерным стилем мышления и деятельности.

Профессиональная реализация социальных инженеров ориентирована на решение конкретных социальных проблем.

В широком смысле — это специалисты, которые умеют манипулировать другими. Но обычно мы слышим о тех социальных инженерах, которые с помощью психологических приемов выманивают деньги или данные для доступа к чужому счету.

По статистике в большинстве случаев люди теряют свои сбережения не потому, что их счета взламывают хакеры. Владельцы банковских карт чаще всего сами сообщают мошенникам их полные реквизиты, включая номер, срок действия, трехзначный CVV/CVC-код, а также пароли и коды из СМС, которые банки присылают для подтверждения операций.

Задача любого мошенника — «социального инженера» заключается в том, чтобы на доверии заставить человека предпринять какие-то действия, которые в нормальной жизни он не стал бы делать.

Мошенники быстро адаптируются к появлению новых сервисов. Например, СМС типа: «Мама, я попал в аварию. Положи на счет номер... денег, потом расскажу», с помощью которых раньше очень часто пытались выманить деньги, теряют популярность у мошенников. Сейчас в основном они нацелены на получение доступа к счетам и картам.

Часто мошенники благодаря использованию социальной инженерии узнают нужные им данные, представляясь сотрудниками банка либо просто пользуясь низкой финансовой грамотностью и доверчивостью.

Самые распространенные психологические уловки, которые используют мошенники:

Вызвать доверие

Мошенники часто представляются теми, от кого люди не ждут подвоха: сотрудниками банков, налоговой службы, юридических контор и других официальных организаций. Социальный инженер может прикинуться вашим приятелем или родственником, например, взломав или сделав дубликат их аккаунтов в соцсетях.

Подделать телефонные номера, документы и сайты

Подменяют номер, с которого звонят или присылают сообщение. Подделывают документы с помощью фотошопа, копируют сайты банков, микрофинансовых организаций, страховых компаний, популярных онлайн-магазинов,

Запугать потерей денег

Вызвать страх – уже полдела для обманщика. Испуганный человек гораздо лучше поддается внушению. Например, мошенник звонит «из службы безопасности банка» и сообщает, что по карте «прямо сейчас» проводится подозрительная операция.

Заманить выигрышем

Мошенники активно эксплуатируют стремление людей к легкому обогащению.

Восстановить справедливость

Махинаторы ведут базы данных людей, которые уже однажды поддались на их обман и могут снова клюнуть на их уловки. Под предлогом оплаты «услуг юриста» или «комиссии за перевод денег» человека убеждают указать полные реквизиты карты, чтобы он снова получил шанс потерять свои деньги.

Использовать громкие информационные поводы

Мошенники активизируются на фоне различных катастроф, стихийных бедствий и эпидемий. Например, во время пандемии коронавируса обманщики собирают деньги «на разработку вакцины» под видом Всемирной организации здравоохранения.

Социальные инженеры следят за новостями и настроениями и быстро адаптируются к текущей ситуации. В период самоизоляции они рассылают всем подряд СМС о «штрафе» за нарушение карантина.

Не дать время на размышления

Мошенники специально торопят и давят, чтобы лишить человека возможности принять взвешенное решение в спокойной обстановке.

Как обезопасить себя от социальных инженеров?

Аферисты постоянно придумывают новые схемы обмана. Единственный способ избежать денежных потерь при встрече с мошенниками — критически воспринимать любые предложения, перепроверять информацию и никогда не торопиться при принятии финансовых решений.

Следуйте базовым правилам финансовой безопасности:

- Никому ни при каких обстоятельствах не сообщайте полные реквизиты банковской карты, включая трехзначный код с обратной стороны; а также ПИН-коды и пароли из СМС от банка.
- Не переходите по сомнительным ссылкам из сообщений и не переводите незнакомцам деньги по первому требованию.
- Не храните много денег на карте, которой расплачиваетесь в интернете: кладите только ту сумму, которую собираетесь потратить в данный момент. В этом случае,

даже если мошенники попытаются украсть деньги, им не удастся вывести слишком много.

- Получив внезапный звонок из какой-либо финансовой организации со срочным вопросом или предложением, положите трубку и позвоните туда сами, найдя номер на ее официальном сайте. Набирайте этот номер вручную. Если с вами связались из компании, клиентом которой вы не являетесь, сначала проверьте ее по справочнику финансовых организаций.
- Не соглашайтесь сходу ни на какие «заманчивые предложения» — будь то «выгодный кредит» или внезапная компенсация. Дайте себе время на размышление, посоветуйтесь со знакомыми, пробейте в интернете информацию о компании и «уникальной акции», которую она вам рекламирует.
- Не публикуйте в открытом доступе свои персональные данные: номер телефона, домашний адрес, данные паспорта. Мошенники охотно задействуют эту информацию в своих аферах.

Используемые ресурсы Интернета:

<https://fincult.info/article/sotsialnaya-inzheneriya-pochemu-lyudi-sami-otdayut-moshennikam-dengi/>

<https://infopedia.su/1x8ac9.html>

<https://inde.io/article/30540-11-tipichnyh-i-novyh-shem-moshennichestva-s-nashimi-bankovskimi-schetami>