Дружи с финансами

НАЦИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ ФИНАНСОВОЙ ГРАМОТНОСТИ ГРАЖДАН

вашифинансы.рф

Как победить социальных инженеров?

МОШЕННИЧЕСТВО В ФИНАНСОВОЙ СФЕРЕ

Т.Н. Аитов, канд.физ.-мат.наук,
заместитель председателя Комиссии по цифровым финансовым технологиям ТПП РФ,
замгендиректора ГК «Программный продукт»

facebook.com/timur.aitov

СИ это атака на доверие

социальная инженерия использует естественную склонность человека доверять

социальная инженерия это не тупость – это **неуместная** степень доверия к злоумышленнику

пример атаки СИ

как строится диалог с клиентом

Госпожа Петрова? Говорит служба безопасности VTB-банка//
По вашей карте приостановлена подозрительная транзакция в городе Бангкоке на сумму 300 000 рублей//

пример атаки СИ

как строится диалог с клиентом

Моя благодарность не знает границ…

пример атаки СИ

как строится диалог с клиентом

Вы должны подтвердить правильность наших действий и после этого транзакция будет окончательно заблокирована//

Что мне надо сделать?

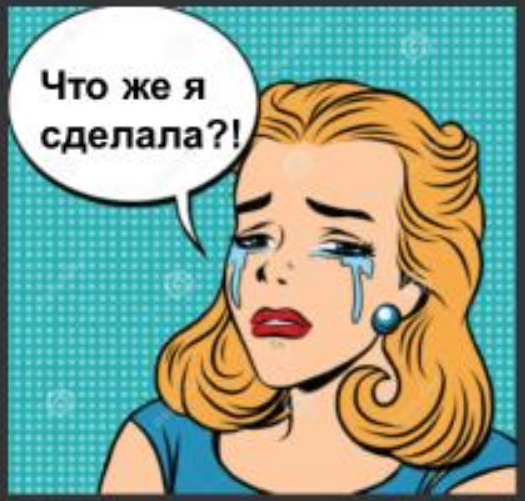
пример атаки СИ

как строится диалог с клиентом

Для блокировки транзакции перешлите секретный код, который мы вам направили, в службу процессинга VTB//
Для этого пройдите по ссылке она уже у вас в смартфоне..

Все непременно, я это уже сделала, спасибо вам!

пример атаки СИ



Рабочие диалоги («скрипты СИ») рассчитаны не на бабушку из далекой деревни, а на компетентного клиента

Центробанк сообщил о 577 тыс. несанкционированных операциях с использованием ЭСП - на 6,4 млрд рублей в 2019 году

В России более 90% хищений со счетов физических лиц совершаются психологами, способными уговорить клиента совершить платеж в своих корыстных интересах

Бороться с СИ бесполезно – таково мнение большинства специалистов ИБ

Но стоит ли опускать руки?

Примеры атак СИ за рубежом

> компания EQUIFAX была взломана, а конфиденциальные данные клиентов украдены в 2018 году
В результате кражи злоумышленники получили доступ к личной информации 145,5 миллионов потребителей финуслуг во всем мире
В ходе фишинговых атак были отправлены тысячи электронных писем, якобы от финансовых учреждений или крупных банков, таких, как Банк оф Америка

Федеральное бюро расследований США (ФБР) сообщило недавно об увеличении числа мошеннических действий со стороны «генеральных директоров», когда злоумышленники от их имени отправляют письма сотрудникам и просят помощи - по оценкам ФБР потери уже превысили $ 2,3 миллиарда долларов

Общая схема атаки

метод социальной инженерии

(1) подготовка

злоумышленник выбирает жертву на основе некоторых требований

(2) контакт

хакер завоевывает доверие жертвы посредством прямого контакта или общения по электронной почте

(3) атака

злоумышленник эмоционально воздействует на жертву, чтобы получить от нее конфиденциальную информацию или совершить ошибки безопасности

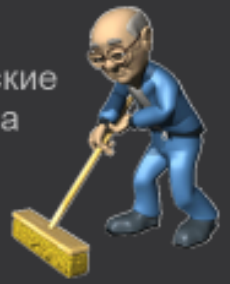
(4) выход

злоумышленник исчезает, не оставляя никаких доказательств

Классификация атак СИ

Социальные - осуществляются через прямые контакты с жертвами. Эти атаки являются наиболее опасными, поскольку включают в себя взаимодействие с человеком
Технические - осуществляются через Интернет - соцсети и веб-сайты онлайн-служб. Хакеры собирают необходимую информацию, такую как пароли, данные кредитной карты и коды безопасности.
Физические – включает офф-лайн действия, выполняемые злоумышленником для сбора информации о цели. Пример - поиск в мусорных корзинах ценных документов под видом уборщицы

Деление условно - так как социальные могут включать технические средства, а технические атаки использовать физические средства



Классификация атак

по признаку прямые или косвенные

П. используют прямые контакты между атакующим и жертвой. Атаки осуществляются через физический или зрительный контакт, голосовые взаимодействия.
Примеры: «подглядывание », социальная инженерия по телефону, фальшивые уборщики и прочее

К. атаки не требуют присутствия атакующего для запуска атаки. Атака может быть запущена удаленно с помощью вредоносного ПО, передаваемого через вложения электронной почты или SMS-сообщения.
Примеры : фишинг, ПО вымогателей

Классификация атак СИ

атак в отношении банковских клиентов

атаки **«СИ1»** - когда клиента уговаривают совершить перевод на счета злоумышленников и эту процедуру клиент совершает добровольно.
атака **«СИ2»** - клиент передает ключи, пароли и иной инструментарий ДБО злоумышленникам, будучи введенным ими в заблуждение.

Важное отличие СИ1 от СИ2 в том, что при СИ1 клиент желает передать средства злоумышленникам, а в схеме СИ2 клиент не хочет передавать свои средства - злоумышленники, получив пароли, совершают хищения со счета клиента самостоятельно.

В схеме СИ1 бороться со злоумышленниками бесполезно, при хищениях по схеме СИ2 клиент нуждается в защите, дополнительную техническую защиту ему оказать и можно, и нужно

НИКТО НЕ ХОТЕЛ ЗАЩИЩАТЬ :
проблемы СИ банков

Основные участники борьбы с хищениями в сфере платежей не заинтересованы противодействовать **СИ**

>**МВД** с такого рода преступниками не работает, ссылаясь на быстротечность, отсутствие доступа к инфраструктуре банковских сетей, на несовершенство законодательства в части Закона о банковской тайне.
>**банки** не заинтересованы менять ситуацию. За хищения методами СИ банк не несет ответственности — ни одного случая возврата средств клиенту в рамках требований ст. 9 Закона № 161-ФЗ не наблюдается.

Если же банк захочет противодействовать атакам **СИ** (усложнит доступ к счету многочисленными проверками, введет изощренную систему антифрода), то может и пострадать:
подавляющее число пользователей не любит сложные процедуры платежей

Методы смягчения последствий атак СИ

> Объект кибербезопасности минимизирует потери путем определения мер безопасности в случае атаки СИ
> Объект формирует правильную корпоративную культуруру как инструмент предотвращения атак СИ

позитивная корпоративная культура помогает жертве не стыдиться того, что ею манипулируют, социальный инженер эксплуатирует неуместную степень доверия, а не то, что жертва глупа или недостаточно образована

Новые парадигмы противодействия СИ

1. Следует исходить из того, что 90% клиентов обязательно подпадут под атаку СИ

2. Банк должен усложнять процедуры перевода средств, когда сумма перевода начинает возрастать

Небольшие переводы (меньше 1.000) действует одна схема подтверждения, на сумму 10.000 другая, и на 100.000+ рублей третья, которая должна максимально затруднить злоумышленнику осуществлять перевод по схеме СИ

3. Банк обязан ограничивать суммы транзакций в зависимости от рисков.
Риски определятся видами операций и **надежностью методов аутентификации платежа (МАП).**
Для МАП, при которых возможны атаки методами **СИ,** лимиты должны быть меньше

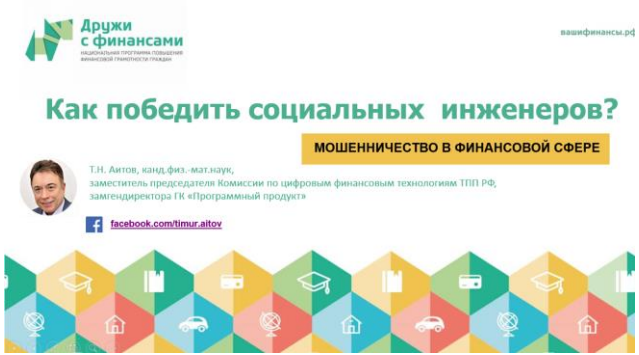
4. Клиент должен иметь возможность самостоятельно минимизировать свои риски, и даже отключать ДБО!

Между банком, клиентом и государством в лице Законодателя сегодня существуют нелепые отношения, в которых

- клиент всегда прав, но в действительности всегда виноват и не защищен,
- банк виноват, но сделать с ним клиент ничего не может, ну, а
- Законодатель рапортует , что сделано все достаточно для того, чтобы защитить клиента и прекратить хищения.

Взаимоотношения должны базироваться на двух простых постулатах
— есть нормативные требования, которые обеспечивают оптимальный уровень защиты клиентов и банков,
— есть ответственность за невыполнение этих требовании.

всё это в руках регулятора и это нужно обязательно реализовать в ближайшее время



Т.Н. Аитов, канд.физ.-мат.наук,
заместитель председателя Комиссии по цифровым финансовым технологиям Совета ТПП РФ по финансово-промышленной и инвестиционной политике, замгендиректора ГК «Программный продукт», директор по развитию АФИ (Ассоциации «Финансовые инновации»), глава центра компетенций Фонда развития цифровой экономики

facebook.com/timur.aitov

timur.aitov