Социальная инженерия

Обман с помощью психологического воздействия – самый распространенный вид интернет-мошенничества.

Работают мошенники по сценариям – «Скритам» Они периодически меняются, но все они отслеживаются сотрудниками ПХО и обнародуются.

Ни банки, ни полиция ни ФСБ , ни другие государственные организации НЕ РЕШАЮТ ВОПРОСЫ ПО ТЕЛЕФОНУ.

СООБЩЕНИЕ ОТ «РУКОВОДИТЕЛЯ»

От имени руководителя/близкого родственника

- поступает сообщение, что с Вами скоро должны связаться **представители гос. органов** (ЦБ, МВД, ФСБ и др.)
- необходимо следовать их **указаниям**

С неизвестного номера **звонит «близкий родственник»** и говорит, что:

- он/она попал/а в **неприятную ситуацию** и срочно нужны деньги

Убеждают, что **проводится проверка организации** или вас подозревают **в финансировании ВСУ,** требуют **снять деньги** или **оформить кредит**

Для обеспечения сохранности нужно **получить максимальное количество кредитов,** реализовать свое недвижимое имущество и внести все деньги на **«защищенный счет»**

ЗВОНОК/СООБЩЕНИЕ ОТ «БЛИЗКОГО РОДСТВЕННИКА»

ЧТО ДЕЛАТЬ?

Свяжитесь со своим руководителем или со своим родственником, от которого якобы поступило сообщение **по известному Вам номеру**

Не совершайте никаких действий и банковских операций по инструкциям звонящего

При возникновении опасений за сохранность ваших денег, самостоятельно **свяжитесь с Банком по номеру 900,** в приложении Сбербанк Онлайн или **обратитесь в любой офис**

ЗВОНКИ / СООБЩЕНИЯ ИЗ «СЛУЖБЫ БЕЗОПАСНОСТИ БАНКА»

ЗВОНКИ / СООБЩЕНИЯ ОТ «ПРЕДСТАВИТЕЛЕЙ ГОС. ОРГАНОВ»

С неизвестного номера **от имени службы безопасности банка** (ЦБ или Сбер) или **от имени представителя гос. органов** (ЦБ, МВД, ФСБ и др.) поступает сообщение / звонок

Вас убеждают, что **мошенниками осуществляются попытки хищения** денежных средств с Ваших счетов

Для обеспечения сохранности нужно **получить максимальное количество кредитов,** реализовать свое недвижимое имущество и внести все деньги на **«защищенный счет»**

ЧТО ДЕЛАТЬ?

Не отвечайте на звонки с неизвестных номеров

Не совершайте никаких действий и банковских операций по инструкциям звонящего

При возникновении опасений за сохранность ваших денег, самостоятельно **свяжитесь с Банком по номеру 900,** в приложении Сбербанк Онлайн или **обратитесь в любой офис**

Помните, что сотрудники банков и гос. органов **не звонят/не пишут в мессенджерах** и **не отправляют** свои личные **документы** (служебные удостоверения личности) и **документы организаций и гос. органов**

ЗВОНКИ/СООБЩЕНИЯ ОТ «ПРЕДСТАВИТЕЛЕЙ ГОС. ОРГАНОВ» С УГРОЗОЙ УГОЛОВНОГО ПРЕСЛЕДОВАНИЯ

Убеждают, что в отношении Вас/близкого родственника **возбуждено уголовное дело**

Убеждают, что у Вас возникли проблемы: Ваши **данные фигурируют в преступной деятельности** (необходимо получить доступ к банковским реквизитам или аккаунтам, чтобы «проверить» информацию)

ЧТО ДЕЛАТЬ?

- **Сохраняйте спокойствие,** не паникуйте и не поддавайтесь на эмоциональное давление мошенников
- Не предоставляйте **персональную информацию**
- Прервите разговор и **сбросьте звонок/Запишите данные** звонка
- **Сообщите** о случившемся **в полицию**/оповестите **Банк**
- Информируйте своих **близких**
- **Помните,** что сотрудники гос. органов **не звонят/ не пишут в мессенджерах** и **не отправляют** свои личные **документы** (служебные удостоверения личности) и **документы организаций и гос. органов**

ПОСТУПЛЕНИЕ ЗВОНКА/СООБЩЕНИЯ ОТ «СОТОВОГО ОПЕРАТОРА»

С неизвестного номера / адреса от имени Вашего «сотового оператора» поступает звонок / сообщение на мобильный телефон

С неизвестного номера / адреса от имени **«Госуслуг»** или **«Почты России»** **поступает сообщение на мобильный телефон / письмо на электронную почту**

Убеждают, что **у Вас произошли изменения профиля в личном кабинете** и необходимо **подтвердить свои данные**

Для подтверждения данных Вам необходимо **перейти по указанной ссылке** / отправить **одноразовый код,** который Вам прислали другим сообщением

ПОСТУПЛЕНИЕ СООБЩЕНИЯ/ПИСЬМА ОТ «ГОСУСЛУГ» ИЛИ «ПОЧТЫ РОССИИ»

ЧТО ДЕЛАТЬ?

Не совершайте никаких действий: не переходите по ссылкам; не сообщайте / не указывайте свои данные; не скачивайте какие-либо закрепленные в сообщении файлы

Перепроверьте информацию, позвонив своему сотовому оператору на **официальный** номер телефона

Перепроверьте информацию в личном кабинете на официальном сайте / в мобильном приложении

Удалите сообщение

РАЗМЕЩЕНИЕ НА ДВЕРИ КВАРТИРЫ / ПОДЪЕЗДА ИНФОРМАЦИИ О ДОСТАВКЕ

На двери квартиры / подъезда размещается информация (объявление) о доставке для клиента с просьбой **перезвонить** на номер телефона мошенников

В ходе общения по указанному в объявлении номеру телефона, Вас **пытаются убедить перевести денежные средства** за оплату доставки

В то же время могут **поступить звонки от мошенников под видом правоохранительных органов или сотрудников банка,** которые убеждают, что Вас обманывают мошенники и денежные средства для сохранности нужно перевести на **«безопасные счета»**

ЧТО ДЕЛАТЬ?

Не совершайте никаких действий и банковских операций по инструкциям звонящего

Не отвечайте на звонки с неизвестных номеров

При возникновении опасений за сохранность ваших денег, самостоятельно **свяжитесь с Банком по номеру 900,** в приложении Сбербанк Онлайн или **обратитесь в любой офис**

Помните, что сотрудники банков и гос. органов **не звонят/не пишут в мессенджерах** и **не отправляют** свои личные **документы** (служебные удостоверения личности) и **документы организаций и гос. органов**

ВЗЛОМ АККАУНТОВ В МЕССЕНДЖЕРАХ/СОЦИАЛЬНЫХ СЕТЯХ – РАССЫЛКА СООБЩЕНИЙ С ПРОСЬБОЙ ПЕРЕВОДА ДЕНЕГ В ДОЛГ

Ваш аккаунт или Вашего друга/родственника **взламывают**

Мошенники, **используя специальное ПО,** совершают **массовую рассылку** сообщений с просьбой о помощи (дать денег в долг)

ЧТО ДЕЛАТЬ?

Не совершайте никаких переводов, пока лично не убедитесь, что Вам написал Ваш знакомый

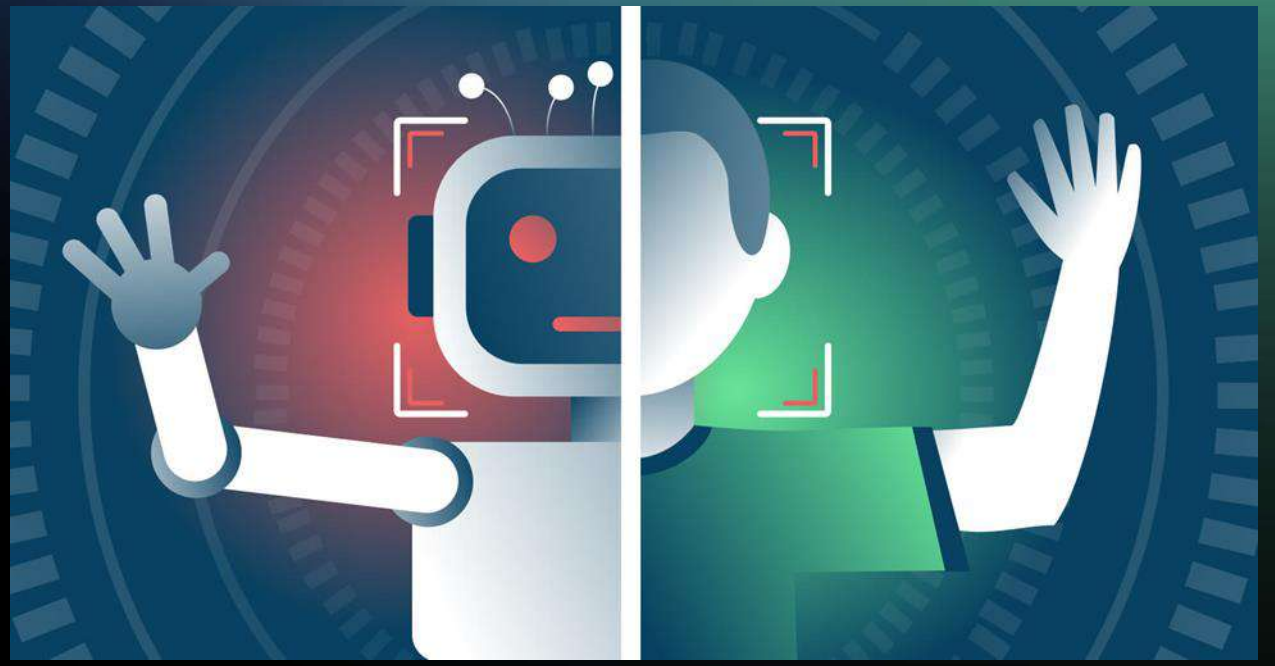
Поменяйте пароли от социальных сетей и мессенджеров, если они очень простые (Имя/Фамилия, дата рождения, простые слова и т.д.)

Если Ваш аккаунт уже взломали, то **немедленно восстановите его**

Незамедлительно уведомите своих родственников и знакомых, которым мошенники успели отправить сообщения, о взломе Вашего аккаунта

DeepFake: как распознать и как защититься

Термин дипфейк (англ. deepfake) состоит из двух понятий: «глубинное обучение» (англ. deep learning) и «подделка» (англ. fake). По сути дипфейк — это метод синтеза контента, основанный на машинном обучении и искусственном интеллекте. Нейросеть накладывает фрагменты контента на исходное изображение. Таким образом подменяется лицо, мимика, жесты и голос в видео или звуковой дорожке.



ЧТО ДЕЛАТЬ?

НЕ совершайте никаких действий и банковских переводов

Свяжитесь со своим родственником/знакомым, от которого якобы поступило сообщение по ИЗВЕСТНОМУ ВАМ НОМЕРУ

УСТАНОВКА ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Вам поступает **смс-сообщение со ссылкой** на установку вредоносной программы под видом обновления приложения сотового оператора

Вас убеждают, что мошенниками осуществляются **попытки хищения денежных средств** клиента или **оформить кредит:**

- для предотвращения попытки хищения денежных средств необходимо **самостоятельно установить специальную программу** на телефон
- после получения доступа к телефону и данным клиента **через вредоносное ПО,** мошенники **получают доступ к банковскому приложению** для вывода средств или оформления кредитов

ЧТО ДЕЛАТЬ?

Не устанавливайте программы по просьбе 3-х лиц на телефон и **не переходите по ссылкам** в сообщении

Не совершайте никаких действий и банковских операций по инструкциям звонящего

При возникновении опасений за сохранность ваших денег, самостоятельно **свяжитесь с Банком по номеру 900,** в приложении Сбербанк Онлайн или **обратитесь в любой офис**

ПОИСК РАБОТЫ В ИНТЕРНЕТЕ – ПОПАЛ НА МОШЕННИКОВ

В процессе **поиска работы** в интернете, **Вы попадаете на сайт мошенников,** якобы с соответствующим предложением

В ходе общения **по видеосвязи «с сотрудником удаленной работы»,** Вас переводят на **«специалиста в мессенджере»**

Убеждают **оформить кредит/кредитную карту,** якобы **для подтверждения кредитоспособности,** после чего пытаются вывести денежные средства

ЧТО ДЕЛАТЬ?

Не сообщайте заранее свои **персональные данные**, включая банковские реквизиты

Не совершайте никаких действий и банковских операций по инструкциям в сообщении

При возникновении опасений за сохранность ваших денег, самостоятельно **свяжитесь с Банком по номеру 900,** в приложении Сбербанк Онлайн или **обратитесь в любой офис**

Помните, что честные **работодатели не просят** у работников денежных средств

САЙТ ЗНАКОМСТВ

В процессе **общения на сайте знакомств,** Вам поступают звонки/сообщения **с просьбой перевести деньги на билеты или оплатить пошлину за дорогостоящий «подарок»,** который отправили по почте

Вас убеждают перевести денежные средства **под предлогом получения посылки или личной встречи**

ЧТО ДЕЛАТЬ?

Незамедлительно прекратите все коммуникации с лицами, которые к Вам обратились, не отвечайте на звонки с неизвестных номеров

Не совершайте никаких действий и банковских операций по инструкциям в сообщении

При возникновении опасений за сохранность ваших денег, самостоятельно **свяжитесь с Банком по номеру 900,** в приложении Сбербанк Онлайн или **обратитесь в любой офис**

УЧАСТИЕ В АКЦИЯХ И ВЫПОЛНЕНИЕ ЗАДАНИЙ

Вам объясняют суть работы, **добиваются пополнения счета и обещают быстрый и легкий доход**

Вам **позволяют заработать,** чтобы завоевать доверие

Мошенники **выманивают деньги** – столько, сколько могут

ЧТО ДЕЛАТЬ?

Не сообщайте свои персональные данные, в частности банковские реквизиты (ваши деньги могут украсть)

Не совершайте никаких действий и банковских операций по инструкциям в сообщении

При возникновении опасений за сохранность ваших денег, самостоятельно **свяжитесь с Банком по номеру 900,** в приложении Сбербанк Онлайн или **обратитесь в любой офис**

ВЛОЖЕНИЕ ДЕНЕЖНЫХ СРЕДСТВ В ФИНАНСОВУЮ ПИРАМИДУ/КРИПТОБИРЖУ

Вас убеждают вносить денежные средства **под предлогом «высокой доходности»**

Вам позволяют заработать, чтобы **завоевать доверие**

Мошенники **выманивают деньги** – столько, сколько могут

ЧТО ДЕЛАТЬ?

Если Вы уже вложили деньги в пирамиду:
Не совершайте новых переводов;
Прекратите общение с представителями организации;
Напишите заявление в полицию;
Обратитесь в Федеральный фонд защиты прав вкладчиков и акционеров.

Не сообщайте свои **персональные данные,** включая банковские реквизиты;
Не совершайте никаких действий и банковских операций по поступившим инструкциям.

Обратите внимание на основные признаки опасных фин. организаций:

Обещают / гарантируют высокую доходность;
Отсутствует лицензия Центрального банка;
Агрессивная реклама;
Отсутствие собственных средств и дорогостоящих активов;
Организация не зарегистрирована в РФ;
Для вывода средств требуют внести деньги для «повышения статуса».

ДРОПЫ/КУРЬЕРЫ

Дроп — это подставное лицо, участвующее в схеме мошенничества
Он использует свои либо предоставленные ему «дроповодом» (мошенником, управляющим дроп-сервисами в локальном регионе) карты и счета для обналичивания или транзита похищенных денежных средств. Таким образом, дроп выступает посредником в цепочке манипуляций с украденными деньгами.

Курьеры – это, как правило, молодые люди, которым в интернете пообещали легкий заработок - приехать по названному адресу и забрать деньги. Себе курьер оставляет обычно 5-10 процентов, остальную сумму переводит мошенникам, которые обманули граждан. Ради такой хорошо оплачиваемой и непыльной работы курьеры соглашались даже отправляться в другие города. При задержании курьеров выяснялось, что в абсолютном большинстве своем они прекрасно понимали, во что ввязались. Но были уверены, что с них не спросят - они же никого не обманывали, а только забрали оговоренную сумму и переслали деньги. А обманщиков они не знают, в глаза не видели - заказ получен анонимно.

УГОЛОВНАЯ ОТВЕТСВЕННОСТЬ: ДРОПЫ/КУРЬЕРЫ

Уголовная ответственность за «Курьерство» предусмотрено ст. 159 УК РФ – Мошенничество. Курьер является соучастником всей преступной цепочки.

В 2023 году:
Оглашен первый приговор суда курьеру телефонных мошенников.
Молодой человек проведет в местах лишения свободы ближайшие 4,5 года за то, что он похитил у 13 пенсионеров больше 3,2 миллиона рублей. Этот приговор вынес суд в Красноярске. Но решение далеко не региональное. Оно - знаковое.

ДРОПЫ:

За продажу/передачу банковских средств платежей: банковская карта, банковский счет, банковский онлайн кабинет - граждане несут уголовную ответственность, предусмотренную ст.187 УК РФ
Санкция статьи предусматривает ответственность в в виде принудительных работ на срок до 5 лет либо лишения свободы до 6 лет со штрафом в размере от 100 до 300 тысяч рублей!!
Если данное преступление совершено группой лиц, то наказание УЖЕСТОЧАЕТСЯ в виде лишения свободы до 7 лет со штрафом до 1 млн.рублей!!
Зачастую указанные средства платежей передаются гражданами 3-м лицам за обещанное им вознаграждение (5,10,15 тыс. рублей)
БОЛЕЕ ТОГО!! если переданные средства платежей будут использованы для транзитного перечисления денежных средств в целях осуществления актов ЭКСТРЕМИЗМА или ТЕРРОРИЗМА, то наказание УЖЕСТОЧАЕТСЯ вплоть до ПОЖИЗНЕННОГО ЛИШЕНИЯ СВОБОДЫ !!

ВНИМАНИЕ – ДЕТИ! / ТЕРРОРИЗМ

«Привет! Хочешь заработать 700к? Нужно просто забрать рюкзак и отвезти в определённое место. Твоя задача — заминировать».

Такие сообщения после теракта в «Крокус Сити Холле» стали массово получать подростки и студенты по всей России. Иногда это — глупые шутки их ровесников. **Но часто — настоящие сообщения от преступников, которые пытаются вовлечь ребят в террористические группы.**

Что делать?

Если у вас есть ребёнок-подросток, поговорите с ним об этом. Объясните, что это — не шутка, а серьёзное преступление. Расскажите о последствиях. Предупредите, чтобы:

• не вступал в переписку с неизвестными, а сразу блокировал этот контакт;
• не пересылал подобные сообщения друзьям и знакомым;
• не проходил по неизвестным ссылкам;
• не слушался незнакомого человека, даже если он угрожает;
• о таких СМС сразу сообщал взрослым (родителям, учителям или полицейским).

МЕРЫ ПРОТИВОВОДЕЙСТВИЯ МОШЕННИКАМ ПО СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

•Прежде чем выполнять любые указания, полученные по телефону, возьмите паузу, сделайте три глубоких вдоха-выдоха, позвоните близким людям и обсудите с ними сложившуюся ситуацию.

•Если вам звонят от имени вашего родственника или знакомого и просят перевести деньги свяжитесь с ним лично. Даже если он не подходит к телефону — это ещё не повод немедленно переводить деньги. Подождите, пока он перезвонит, или разыщите его через общих знакомых.

•Данные о ваших банковских счетах, номер карты, пин-код или CVV/CVC/CVP- код, **код из СМС** и любые другие сведения для совершения банковского перевода нельзя сообщать никому.

•Вы никогда не можете быть уверены в том, что позвонивший вам человек — именно тот, кем представляется. Если вам поступил подозрительный звонок, положите трубку и перезвоните сами в организацию, от имени которой к вам обратились. (ЛУЧШЕ СХОДИТЬ)

•Ни банки, ни полиция, ни другие организации не решают вопросы по телефону, особенно в срочном порядке. Даже если вам угрожают уголовной ответственностью за отказ сотрудничать — знайте, что телефонные угрозы не имеют юридической силы. Если вам поступил подозрительный звонок, положите трубку!!!

КИБРАРИЙ –
библиотека знаний по кибербезопасности.
 # КомандаСБЕРА