НЕДЕТСКИЕ ИГРЫ

КАК НЕ СТАТЬ УЧАСТНИКОМ ФИНАНСОВЫХ ПРЕСТУПЛЕНИЙ

ТЕМАТИЧЕСКИЙ УРОК

СИТУАЦИЯ

21 ноября дома у 12-летней Вики зазвонил домашний телефон — на том конце провода кто-то сильно плакал. Школьнице показалось, что голос принадлежит её бабушке. После Вике сразу же позвонили на мобильник, неизвестный сказал, что бабулю сбила машина — она получила серьёзные травмы, на лечение которых нужно 600 тысяч рублей. Вика пообещала помочь: по инструкции от звонившего она подготовила полотенце, бумагу, постельное бельё, взяла у отца 50 тысяч и упаковала их так, чтобы было не видно, что внутри.

Вскоре к ней домой пришёл неизвестный мужчина — он был в спортивных штанах и с тёмной бородой. Вика отдала ему деньги, надеясь, что бабуля скоро поправится.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

...психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации.

МЕТОДЫ

обман или злоупотребление доверием

психологическое давление

манипулирование

СХЕМА СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

НЕОЖИДАННОСТЬ

ЭМОЦИИ

ПСИХОЛОГИЧЕСКОЕ ДАВЛЕНИЕ

АКТУАЛЬНАЯ ТЕМА

ЭМОЦИИ, КОТОРЫЕ ВЫЗЫВАЕТ ИНФОРМАЦИЯ ОТ МОШЕННИКОВ, БЫВАЮТ ДВУХ ВИДОВ:

ОТРИЦАТЕЛЬНЫЕ

СТРАХ ПАНИКА

ЧУВСТВО СТЫДА

ПОЛОЖИТЕЛЬНЫЕ

РАДОСТЬ, НАДЕЖДА

ЖЕЛАНИЕ ПОЛУЧИТЬ ДЕНЬГИ

ТЕЛЕФОННОЕ И МОБИЛЬНОЕ МОШЕННИЧЕСТВО

КЕМ МОЖЕТ ПРЕДСТАВИТЬСЯ МОШЕННИК:

Службой безопасности банка, банковскими сотрудниками

Сотрудником правоохранительных органов

Друзьями

Родными

АЛГОРИТМЫ МОШЕННИКОВ

Пять признаков того, что вам звонит мошенник

Звонок поздно вечером, ночью или рано утром в выходные

От вас требуют немедленных действий

Торопят и запугивают, давят на эмоции

Требуют сообщить конфиденциальную информацию: данные карты, ПИН-код или одноразовый пароль из СМС

При отказе называть данные угрожают, что деньги с вашей карты прямо сейчас уйдут к мошенникам

БАДы

Если Вам звонят и представляются сотрудниками медицинских учреждений, дистанционно ставят диагнох, при этом сразу назначают курс лечения препаратом и предлагают тут же его приобрести. Не спешите отдавать свои сбережения. Скорее всего это МОШЕННИКИ.

ЗАБЛОКИРОВАНА БАНКОВСКАЯ КАРТА

Вам поступил звонок из банка или пришло сообщение о блокироваке банковской карты или несанкцигнированных операциях со счтеом. Не отечайте и не перезванивайте. ЭТО МОШЕННИКИ. обратитесь в отдел.

ВЫПЛАТА КОМПЕНСАЦИЙ

Вам позвонили или пришло СМС сообщение с предложением получить выплату компенсаций за страхование, медобслуживание, коммунальные и прочие услуги, но для этого Вам необходимо перевести некую сумму в качестве комиссии. Будьте осторожны, скорее всего это ОБМАН!

ВЫИГРЫШ В ЛОТЕРЕЕ

Вам сообщили, что Вы выиграли приз, но для его получения необходимо перевести сумму денег на незнакомый Вам счет. НЕ торопитесь следовать инструкции! Проверьте информацию! Вполне возможно, что с Вами общаются МОШЕННИКИ.

ПЕРЕВОД ДЕНЕЖНЫХ СРЕДСТВ

Если для перевода Вам денежных средств на банковскую карту просят сообщить 3 цифры с оборота карты (код CVV), Вы столкнулись с мошенничеством. Никому не сообщайте 3-х значный код проверки подлинности карты, а также пароль для списания средстав.

СЛУЧАЙ С РОДСТВЕННИКОМ

Если Вам звонят и сообщают, что Ваши родственник попал в аварию, за решетку, в больницу или совершил ДТП, и теперь за него нужно внести залог, штраф, взятку - ЭТО ОБМАН!

СИТУАЦИЯ

21 ноября у 15-летнего школьника Пети зазвонил мобильный телефон. На том конце провода мошенник представился стримером. Он сообщил, что случайно выбрал Петю для участия в онлайн-стриме, он готов оплатить ему билет в другой город для участия в стриме, но для этого ему потребуются фотографии паспорта Пети и фотография его банковской карты или карты его родителей

КИБЕРПРЕСТУПНОСТЬ И КИБЕРМОШЕННИЧЕСТВО

киберпреступность - любое противозаконное деяние, нарушающее права и свободы человека с помощью компьютерных систем и сетей.

ФИШИНГ

...вид мошенничества, при котором злоумышленники рассылают письма и пытаются обманом заставить получателей различные действия

итоговая цель - получение доступа к финансам или личным данным обманутых пользователей.

темы и авторы писем:

- службы доставки
- маркетплейсы
- криптовалюта
- горячие новости
- лотереи
- дополнительный заработок и инвестиции
- туроператоры и отдых
- билеты на мероприятия
- подписки и онлайн-сервисы
- фото с вечеринки

ФИШИНГОВОЕ ПИСЬМО

— письмо, которое содержит вредоносное вложение, ссылку на мошеннический сайт или вредоносное программное обеспечение.

ПОДДЕЛЬНЫЕ САЙТЫ ИЛИ ПРИЛОЖЕНИЯ

ПРИЗНАКИ ПОТЕНЦИАЛЬНО ОПАСНОГО ИНТЕРНЕТ-МАГАЗИНА

НИЗКАЯ ЦЕНА

стоимость товаров в магазине мошенников зачастую существенно ниже, чем в других. Не следует поддаваться на слова “акция”, ”количество ограничено”, “спешите купить” и т.д.

ОТСУТСТВИЕ КУРЬЕРСКОЙ ДОСТАВКИ И САМОВЫВОЗА

в этом случае нередко приходится вносить предоплату за услуги транспортной компании. Злоумышленники могут предоставить поддельные квитанции об отправке товара

ОТСУТСТВИЕ КОНТАКТНОЙ ИНФОРМАЦИИ И СВЕДЕНИЙ О ПРОДАВЦЕ

Если на сайте прописаны только форма обратной связи и мобильный телефон продавца, такой магазин может представлять опасность. Перед обращением сюда следует почитать отзывы в интернете.

ПОДТВЕРЖДЕНИЕ ЛИЧНОСТИ ПРОДАВЦА ПОСРЕДСТВОМ НАПРАВЛЕНИЯ ПОКУПАТЕЛЮ СКАНА ЕГО ПАСПОРТА

Документ, особенно отсканированный, легко подделать

НЕТОЧНОСТИ И НЕСООТВЕТСТВИЯ В ОПИСАНИИ ТОВАРОВ

Желательно почитать описания такого же товара на других сайтах.

ОТСУТСТВИЕ ИСТОРИИ У ПРОДАВЦА ИЛИ МАГАЗИНА

Потенциально опасными являются страницы, зарегистрированные пару дней назад

Steam и Warface

сценарий:

1/4 вам приходит письмо, что вы «выиграли» приз в одной из игр;

2/4 вы нажимаете на ссылку для обмена со специальным ботом;

3/4 заходите в свой аккаунт на поддельном сайте;

4/4 отдаёте данные от аккаунта мошенникам.

ПРИМЕР

МОШЕННИЧЕСТВО В СОЦИАЛЬНЫХ СЕТЯХ И МЕССЕНДЖЕРАХ

- Переписка с мошенниками
- Взлом аккаунтов
- Цифровое клонирование
- Голосования
- Быстрый заработок
- Онлайн-пирамиды
- Инфоцыгане

СИТУАЦИЯ

К подростку в Telegram, обратился неизвестный, представившись блогером. «Блогер» сообщил, что мальчик выиграл в конкурсе, и для получения награды ему необходимо взять телефон мамы и сделать скриншот экрана. Дальше подросток действовал по указаниям блогера-мошенника, однако не помнит, что именно делал. На следующий день после общения с «блогером» переписка автоматически удалилась, а со счета мамы мальчика исчезли 235 тысяч рублей.

СИТУАЦИЯ

Неизвестные лица создали телеграм-канал для любителей онлайн-шутера и предлагали делать ставки с обещанием заработать на турнирах по этой игре.

14-летний подросток сделал очень крупные ставки и перевел 100 тысяч рублей со счета своей мамы на Qiwi-кошелек и номера телефонов. В итоге он не получил никаких денег.

СИТУАЦИЯ

Молодой человек познакомился в соцсетях с девушкой и общался с ней две недели. Периодически она просила оплатить ей всякие недорогие «плюшки», чтобы они встретились – положить деньги на телефон, оплатить маникюр и т. д. И вот она пишет: «Я забронировала нам билеты в кино, сейчас тебе придет смс-ка с кодом для оплаты, можешь, пожалуйста, ее продиктовать, чтобы эти билеты оплатить».

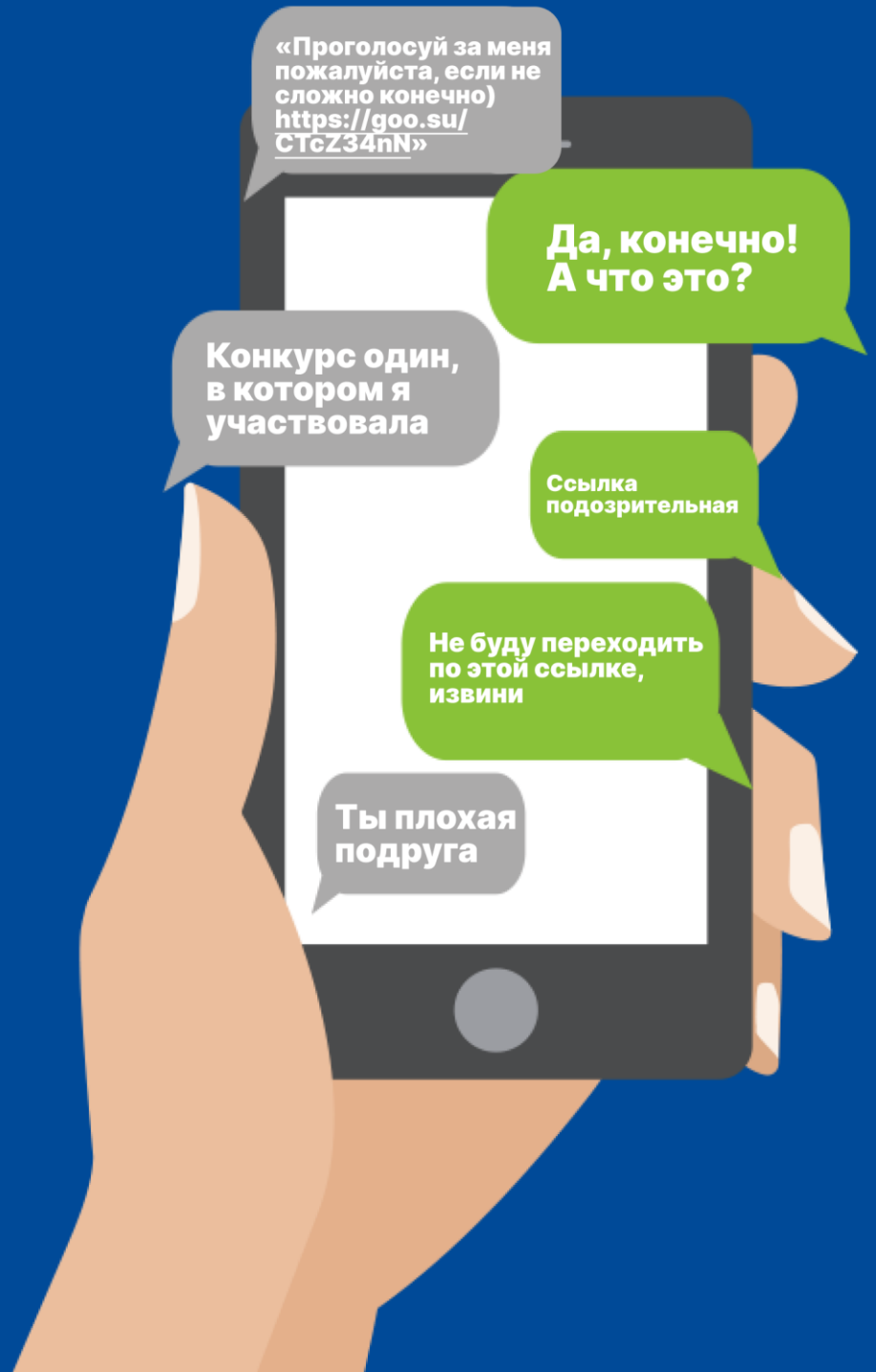
Парень продиктовал ей коды из смс. После этого с карточки списались все деньги, а девушка перестала отвечать на сообщения и звонки и удалила свой аккаунт

СИТУАЦИЯ

В начале октября 14-летней девочке в социальной сети пришло сообщение от ее знакомого. Он утверждал, что счета и деньги родителей школьницы в опасности. Все из-за того, что в интернете есть их персональные данные, которыми могут воспользоваться мошенники.

«Приятель» сразу же предложил решение проблемы. Он рассказал девочке, как спасти семейные сбережения. Школьница последовала совету. Взяла банковские карты родителей, которые лежали на пуфике в прихожей, сфотографировала их со всех сторон и отправила снимки знакомому.

В итоге со счетов взрослых пропали 280 тысяч рублей. Потерпевшие обратились в полицию. Установлено, что страницу знакомого девочки взломали, и от его лица с ней общались аферисты.


«Проголосуй за меня пожалуйста, если не сложно конечно) https://goo.su/CTcZ34nN»
Да, конечно! А что это?
Конкурс один, в котором я участвовала
Ссылка подозрительная
Не буду переходить по этой ссылке, извини
Ты плохая подруга

ФИШИНГ

МОШЕННИЧЕСКИЕ СХЕМЫ С БЫСТРЫМИ ЗАРАБОТКАМИ

- вложения в выгодные проекты
- просмотры видеороликов популярных блогеров
- оценка картинок и отелей
- голосование в рейтингах
- букмекерские ставки
- экономические онлайн-игры

БЕСПЛАТНЫЙ СЫР БЫВАЕТ ТОЛЬКО В МЫШЕЛОВКЕ

МОШЕННИЧЕСКАЯ СХЕМА «ТЫ ПЛАТИШЬ – ТЫ ВЫИГРЫВАЕШЬ»

ФИНАНСОВАЯ ПИРАМИДА

ПРИЗНАКИ:

- отсутствие геймплея
- сложная схема начисления дохода
- выплата средств за привлечение новых участников
- гарантия высокого дохода без всякого риска и агрессивная реклама в соцсетях

СХЕМА МОШЕННИЧЕСТВ С КРИПТОВАЛЮТАМИ И ICO

- скам-проекты (скам)
- проекты-пустышки
- rug n pull (раг пулл, дернуть коврик)
- классический фишинг

ДЕТИ – СОУЧАСТНИКИ ФИНАНСОВЫХ МОШЕННИКОВ

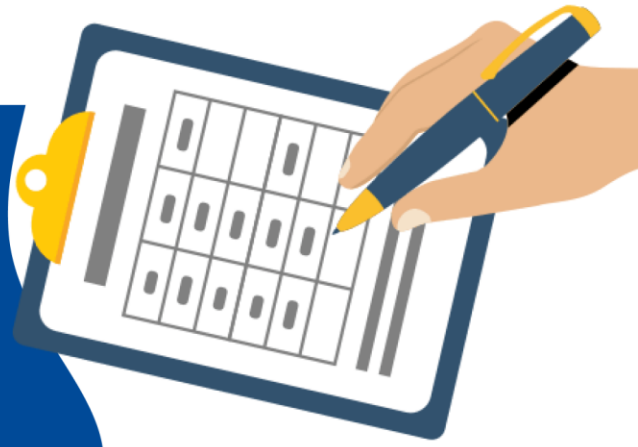
Соучастие в мошенничестве - оказание услуги курьера

«81-летняя пенсионерка, обратилась в полицию после того, как 17-летний подросток забрал у нее 100 тысяч рублей.
Бабушка думала, что помогает внучке, которая якобы попала в ДТП и по телефону попросила деньги. Чтобы на молодую женщину не завели дело, пенсионерка не пожалела все свои сбережения, но позвонить родным додумалась только после ухода курьера.
Когда полиция задержала юношу, он рассказал, что в поисках подработки оставил заявку в группе с вакансиями в соцсетях. Вскоре ему предложили работу в инвестиционной компании: забирать деньги у клиентов и пересылать их через банкомат на определенные счета и получать процент от перечисленных денег. Юноша согласился, отправил "работодателю" свои паспортные данные и стал курьером.
Также он предложил подзаработать своему знакомому сверстнику. Они вместе отправились на "дело" в соседний город. И пока один следил за обстановкой на улице, второй забрал более 700 тысяч рублей у 12-летней девочки, поверившей, что ее мама попала в аварию и нуждается в дорогостоящем лечении.»

Соучастие в мошенничестве

ДРОППЕРЫ

- люди, которые помогают обналичивать и выводить деньги после совершения преступниками финансового преступления



“Подросток Петя хочет найти подработку в свободное время. На одном из сайтов по поиску работы Петя увидел объявление:
‘Требуется сотрудник для удаленной работы с денежными переводами. Серьезный заработок за несколько часов в день. Трудоустройство без проверок и заполнения документов. Опыт работы не требуется. Гарантия высокого дохода. Требования: наличие карты любого банка РФ”

ВАЖНО!

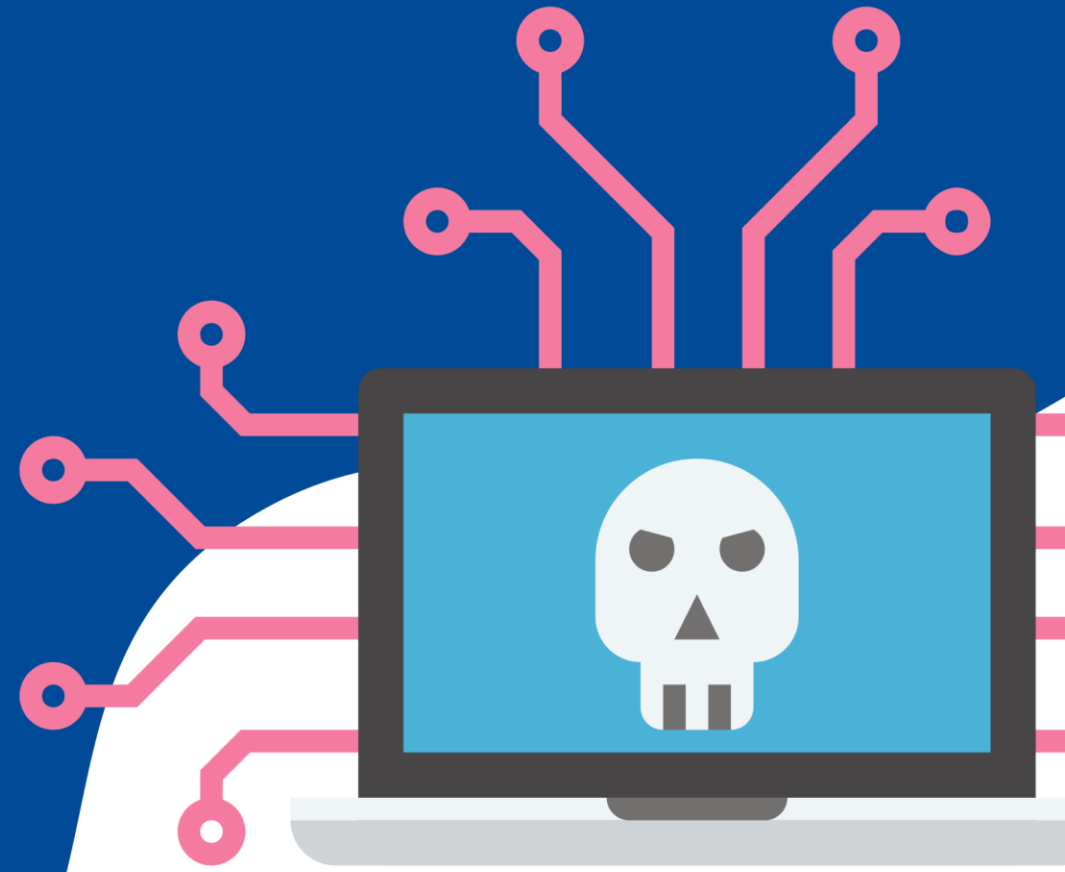
ЛЮДИ, ОТКЛИКНУВШИЕСЯ НА ПОДОБНЫЕ ОБЪЯВЛЕНИЯ, ЧАСТО СТАНОВЯТСЯ УЧАСТНИКАМИ МОШЕННИЧЕСКИХ СХЕМ.

СХЕМЫ ВЕРБОВКИ ДРОППЕРОВ

1. Объявления в Интернете, социальных сетях и мессенджерах о быстром заработке, о подработке, связанная с денежными переводами, обналичиваем, работой в IT-сфере.

2. Звонки под видом правоохранительных органов о работе или о помощи в поимке преступников. Случайный перевод денег на карту с просьбой вернуть.

3. Случайный перевод денег на карту с просьбой вернуть.



ВИДЫ ДРОППЕРОВ

разводные

неосведомленные о преступной схеме

действуют неосознанно, неумышленно и/или под воздействием мошенников

неразводные

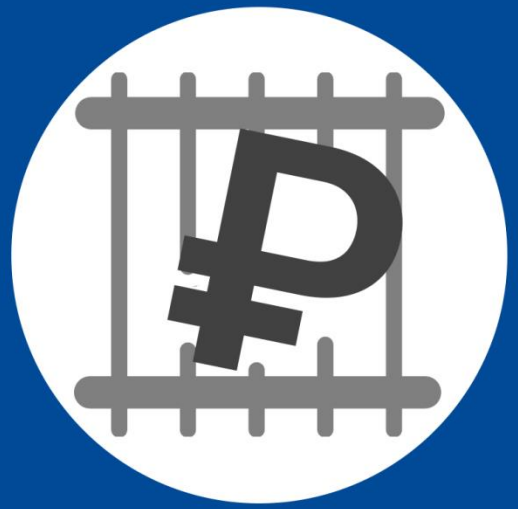
осведомленные о преступной схеме

действуют добровольно и умышленно

ПОСЛЕДСТВИЯ ДЕЙСТВИЙ ДРОППЕРОВ

- От мошенников могут поступать угрозы дропперу и его близким, шантаж
- Дроппер становится участником схем отмывания денежных средств, продажи оружия или наркотиков
- Дроппера будут искать правоохранительные и налоговые органы, иные структуры
- Дроппер станет фигурантом уголовного дела
- Дроппер отвечает своим имуществом и деньгами, а также имуществом и деньгами родителей и опекунов
- Придется выплачивать крупные суммы годами
- Дроппер создает себе негативный финансовый рейтинг, подрывает свою репутацию
- Дроппера могут убить, чтобы избавиться от свидетеля

ОТВЕТСТВЕННОСТЬ ДЛЯ ДРОППЕРА



Штраф

Принудительные работы

Ограничение свободы

Лишение свободы

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ФИНАНСОВЫХ ПРЕСТУПЛЕНИЙ

- фальшивые документы
- создание поддельных картинок и иллюстраций
- фейковые новости и рассылки
- фишинг, мошеннические веб-сайты
- социальные боты и манипуляция в социальных сетях
- беседа (телефонная и в переписке)
- "клон" человека (deepfake)
- поддельные голосовые сообщения
- фальшивая регистрация в chatgpt

Пользователи телеграма столкнулись с новым видом мошенничества - сначала преступники получают доступ к аккаунту, затем начинают писать потенциальным жертвам из числа списка контактов его владельца с просьбой перевести деньги. Историю о необходимости помощи преступники подкрепляют голосовым сообщением якобы от лица владельца аккаунта. Для аудиосообщения используются нарезки из его реальных старых голосовых сообщений.

Аудиосообщение дублируется в личную переписку и во все чаты, где состоит хозяин украденного аккаунта. Затем направляется фото банковской карты с именем и фамилией. Причем у пострадавшего собеседника имя и фамилия отличались в соцсетях от информации в паспорте, и мошенники использовали данные именно паспорта. Сумма, которую хотели заполучить преступники, составляла 200 тыс. руб.

СПОСОБЫ ЗАЩИТЫ ОТ ФИНАНСОВОГО МОШЕННИЧЕСТВА

ОБЩИЕ ПРАВИЛА ЗАЩИТЫ

- критическое восприятие любой ситуации
- незнакомец диктует порядок действий – это точно обман
- обещания быстрой прибыли — всегда тревожный знак
- переход по незнакомым и непроверенным ссылкам – может привести к обману и потере денег
- нельзя говорить незнакомым лицам личные данные
- всегда нужно спрашивать совета у родных и друзей
- позвонить в полицию

ПРАВИЛА ЗАЩИТЫ ОТ МОШЕННИКОВ ПРИ ТЕЛЕФОННЫХ ЗВОНКАХ

- не отвечать и не перезванивать по неизвестным и сомнительным номерам
- обязательно самостоятельно позвонить близкому человеку /в банк / в организацию / в полицию, попросить у них помощи
- прервать разговор, если он касается финансовых вопросов
- никому никогда в разговоре не сообщать никакие данные банковской карты, коды подтверждения из sms-сообщений

ПРАВИЛА ДЕЙСТВИЙ С БАНКОВСКИМИ КАРТАМИ И ПРИ РАСЧЕТНЫХ ОПЕРАЦИЯХ

- никому никогда не сообщать и не фотографировать никакие данные банковской карты, коды подтверждения из sms-сообщений
- заблокировать карту, если она потерялась или пришло уведомление о совершенной без вас операции
- не верить подозрительным смс с неизвестных номеров о карте
- оплачивать покупки только через официальные сайты магазинов и площадок. через переводы оплачивать покупки нельзя
- не давать незнакомцам в руки мобильный телефон с установленными банковскими приложениями
- обязательно самостоятельно позвонить близкому человеку /в банк / в организацию / в полицию, попросить у них помощи

ПРАВИЛА ДЕЙСТВИЙ В ИНТЕРНЕТЕ И В ПЕРЕПИСКЕ ДЛЯ ЗАЩИТЫ ОТ ФИШИНГА И КИБЕРМОШЕННИЧЕСТВА

- не верить информации о выигрышах и о легком заработке
- не устанавливать неизвестные приложения, особенно по просьбе незнакомцев
- не переходить по неизвестным и по странным ссылкам
- сверять официальные источники с полученной информацией, письмами и т.д.
- никому в переписке не сообщать никакие личные данные
- не вводить личные данные на подозрительных сайтах и в приложениях
- всегда проверять у настоящего близкого и друга (лучше позвонить) полученную информацию

ЗАЩИТА АККАУНТОВ И ТЕХНИЧЕСКИХ СРЕДСТВ

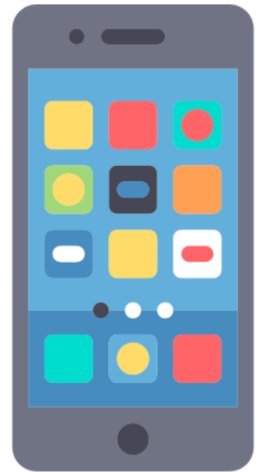
Подключить двухфакторную идентификацию

Установить сложный пароль

Закрыть доступ посторонним к своему профиль

Обновлять антивирусное ПО

ПРАВИЛА ДЕЙСТВИЙ ПРИ ИНТЕРНЕТ-ПОКУПКАХ



ПРОВЕРЯТЬ ИНТЕРНЕТ-МАГАЗИН

НЕ ОБЩАТЬСЯ С ПРОДАВЦОМ В МЕССЕНДЖЕРАХ ВНЕ ТОРГОВОЙ ПЛОЩАДКИ

ОПЛАЧИВАТЬ ПОКУПКИ ТОЛЬКО ЧЕРЕЗ ОФИЦИАЛЬНЫЕ МАГАЗИНЫ, ПЛАТФОРМЫ И Т. Д.

СОВЕТОВАТЬСЯ С РОДНЫМИ И БЛИЗКИМИ

ПРАВИЛА ДЕЙСТВИЙ В ИНТЕРНЕТЕ ОТ УГРОЗ, СВЯЗАННЫХ С ИИ

- Не вводить финансовую информацию в чат ботах
- Проверять полученную информацию у реального человека, лучше ему позвонить
- Проверять данные на официальных ресурсах
- Задавать случайные вопросы

МЕЖДУНАРОДНАЯ ОЛИМПИАДА ПО ФИНАНСОВОЙ БЕЗОПАСНОСТИ

МЫ ЖДЕМ ИМЕННО ТЕБЯ!

Цели Олимпиады:

- повышение общей информационной, финансовой и правовой грамотности молодежи, формирование новой формы мышления и нового формата деятельности, выявление талантливых школьников и студентов в области финансовой безопасности;
- создание условий для индивидуальной образовательной траектории, содействие профессиональной ориентации школьников и студентов для формирования кадрового ресурса системы финансовой безопасности;
- стимулирование учебно-познавательной и научно-исследовательской деятельности школьников и студентов, развитие научных знаний в области финансовой безопасности.

Участники: обучающиеся 8-10 классов / 1-3 курсы бакалавриата / 1-4 курсы специалитета / 1 курс магистратуры