

ПРОТИВОДЕЙСТВИЕ ТЕЛЕФОННЫМ И ОНЛАЙН- МОШЕННИКАМ



ПРИ ПОДДЕРЖКЕ
ФОНДА ПРЕЗИДЕНТСКИХ ГРАНТОВ

Мошенничество – присвоение
имущества другого лица
или приобретение прав
на это имущество путем
использования обмана
или злоупотребления доверием

ЦЕЛИ МОШЕННИКОВ:

1

Социальные сети

2

Игровые аккаунты

3

Личные данные

4

Права

5

Имущество

4 СХЕМЫ МОШЕННИЧЕСТВА

1

Мошенничество, при котором главной целью злоумышленника является получение доступа к личным данным пользователя (логин, пароль, банковские реквизиты и т. д.)

4 СХЕМЫ МОШЕННИЧЕСТВА

2

Мошенничество, при котором злоумышленник устанавливает вредоносные программы или вирусы на устройстве жертвы

4 СХЕМЫ МОШЕННИЧЕСТВА

3

Мошенничество, при котором
пользователям в сообщениях приходит
просьба перейти по ссылке

4 СХЕМЫ МОШЕННИЧЕСТВА

4

«Двойная транзакция» –
мошенничество, при котором
во время оплаты товаров и услуг
продавец сообщает об ошибке
и предлагает повторить операцию,
а в дальнейшем денежные средства
списываются дважды по каждой
из проведенных операций

НАИБОЛЕЕ ЧАСТЫЕ СХЕМЫ МОШЕННИЧЕСТВА:

Мошенничество с персональными данными
пользователя

Объявление о создании
«домового чата»



Переход по QR-коду



Гаджет заражается
вредоносной программой



Мошенник похищает
данные

НАИБОЛЕЕ ЧАСТЫЕ СХЕМЫ МОШЕННИЧЕСТВА:

Мошенничество с кражей данных

Создается канал
магазина



Создают поддельные
отзывы и низкие цены



При покупке
получают данные



Используют
полученные данные

МОШЕННИЧЕСТВО

«Друг в беде»

Мошенники взламывают
аккаунты пользователей,
чтобы от их имени рассылать
сообщения с просьбой денег

КАК РАСПОЗНАТЬ МОШЕННИКА?

1

Обращайте внимание на язык общения

2

Фактор времени

3

Позвоните близкому человеку

4

Задайте специальные вопросы

5

Блокируйте мошенника

МОШЕННИЧЕСТВО

«Бот-атаки»

Поддельный бот отправляет
пользователям сообщения,
что их аккаунт не прошел
верификацию



Далее бот предлагает перейти
по ссылке и ввести свои данные
заново – так они попадают в руки
злоумышленников

КАК ЗАЩИТИТЬ СЕБЯ?

1

Обратите внимание на сам бот.
Если на него пожаловалось большое количество пользователей, он будет иметь пометку «Scam»

2

Обратите внимание
на орфографические ошибки.
Боты мошенников могут содержать
ошибки в тексте и предлагать
упрощенные программы ответов

МОШЕННИЧЕСТВО

«Выгодные крипто-предложения»

Мошенники стремятся получить доступ к криптокошелькам пользователей или предлагают воспользоваться «заманчивыми» услугами обогащения и их вложения

ЧТО ДЕЛАТЬ?

1

Игнорируйте всех, кто сулит «гарантированную» прибыль от любых инвестиций

2

Не размещайте средства на криптокошельке, который вам прислали по ссылке – зачастую, они ложные

3

Никогда не посылайте деньги, криптовалюту или данные аккаунта лицам, с которыми вы контактировали исключительно через Telegram

СХЕМА 1

«Служба безопасности банка»

Звонок от банка



Сообщение
о подозрительных действиях



Просьба сообщить
3 цифры с оборота карты



Списание денег
с вашего счета

СХЕМА 2

«Служба безопасности банка»

Аккаунт банка
в мессенджере



Вопрос об обновлении
приложения



Звонок сотрудника
по видео



Демонстрация экрана
и хищение средств

СХЕМА

«Представитель МВД»

1. Звонит сотрудник банка

Спрашивает: оформляли ли вы кредит?

2. Звонит сотрудник МВД

Предлагает обратиться в банк
и подать заявку на кредит

3. Как только получаете деньги,
их просят перевести на «безопасный»
счет

СХЕМА

«Работа за лайки»

Мошенники размещают объявление о заработке в мессенджерах или на официальных страницах по поиску работы. Все, что требуется от пользователя, поставить лайк или оставить отзыв

ВАРИАНТЫ ПОСЛЕДСТВИЙ:

1. Мошенники просят сообщить данные карты для начисления вознаграждения

2. После начисления денег просят сообщить код из SMS для подтверждения перевода

3. Мошенники присылают ссылку на поддельный сайт, где надо ввести данные карты

КАК ЖЕ МОЖНО ЗАЩИТИТЬ СЕБЯ ОТ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА?

Обязательно блокируйте номера, с которых поступают подозрительные звонки

Не сообщайте логины и пароли от аккаутов, платежные данные, одноразовые коды из СМС

Не переводите деньги на счета, номера которых вам называют по телефону

Если вам поступило подозрительное сообщение, позвоните напрямую и уточните

Установите лимит на карту

КАК ЗАЩИТИТЬ СЕБЯ ОТ ИНТЕРНЕТ- МОШЕННИЧЕСТВА?

Внимательно проверяйте ссылки на сайты

Для входа в интернет-банк используйте
приложение банка

Перепроверяйте предлагаемые вакансии

Ищите первоисточник

Если стали жертвой, сообщите об этом

**ГЛАВНОЕ — ПРОЯВЛЯТЬ
ЗДОРОВЫЙ СКЕПТИЦИЗМ.
НЕ ВЕРЬТЕ СЛИШКОМ
УЖ ЗАМАНЧИВЫМ
ПРЕДЛОЖЕНИЯМ
И БЕРЕГИТЕ СЕБЯ**