

# Онлайн мошенничество

защита старшего поколения

- Что это такое
- Каналы распространения
- Виды онлайн угроз
- Как защититься





# Онлайн мошенничество

Что это такое?



Онлайн мошенничество — это действия киберпреступников, направленные на овладение информационными данными или финансовыми средствами пользователя сети Интернет



Старшее поколение является одной из наиболее незащищенных от мошеннических действий групп населения. Нередко мошенники пользуются вашей доверчивостью и недостаточной информированностью. Сегодня мы поговорим с вами об основных мошеннических схемах, рассмотрим как вести себя в разных ситуациях.



# Онлайн мошенничество

## виды онлайн угроз



### Скам

Мошенничество, которое нацелено на быстрое получение денег обманным путём.



### Фишинг

С его помощью кибермошенники пытаются выманить у человека конфиденциальные данные или вынудить его на какие-либо нежелательные действия. С этой целью злоумышленники используют мгновенные и почтовые сообщения и специально созданные поддельные веб-сайты.



### Вишинг

от англ. Vishing — «voice» и «фишинг». Мошенничество с помощью звонков. Мошенники, используя социальный инжиниринг, стараются получить от жертвы необходимые им данные.



### Смишинг

от англ. SMiShing — от «SMS» и «фишинг» — вид фишинга с использованием SMS. Например, мошенники отправляют жертве SMS-сообщение, содержащее ссылку на фишинговый сайт и мотивирующее получателя пройти на этот сайт.



### Кража личности

Незаконное использование чужих персональных данных для получения выгоды.



# Онлайн мошенничество

## Лотереи, розыгрыши призов (скам)



## Лотереи, розыгрыши призов

Предложения поучаствовать в «беспроигрышной» лотерее, получить приз или пройти опрос за вознаграждение. Часто предлагается оплатить «закрепительный платёж» или комиссию для вывода приза.

Цель – получение денег обманным путём.

Мошенники делают «очень выгодное предложение», цель этих действий – вынудить вас совершить действия, выгодные мошеннику.



# Онлайн мошенничество

## Мошенничество на сайтах объявлений (фишинг)



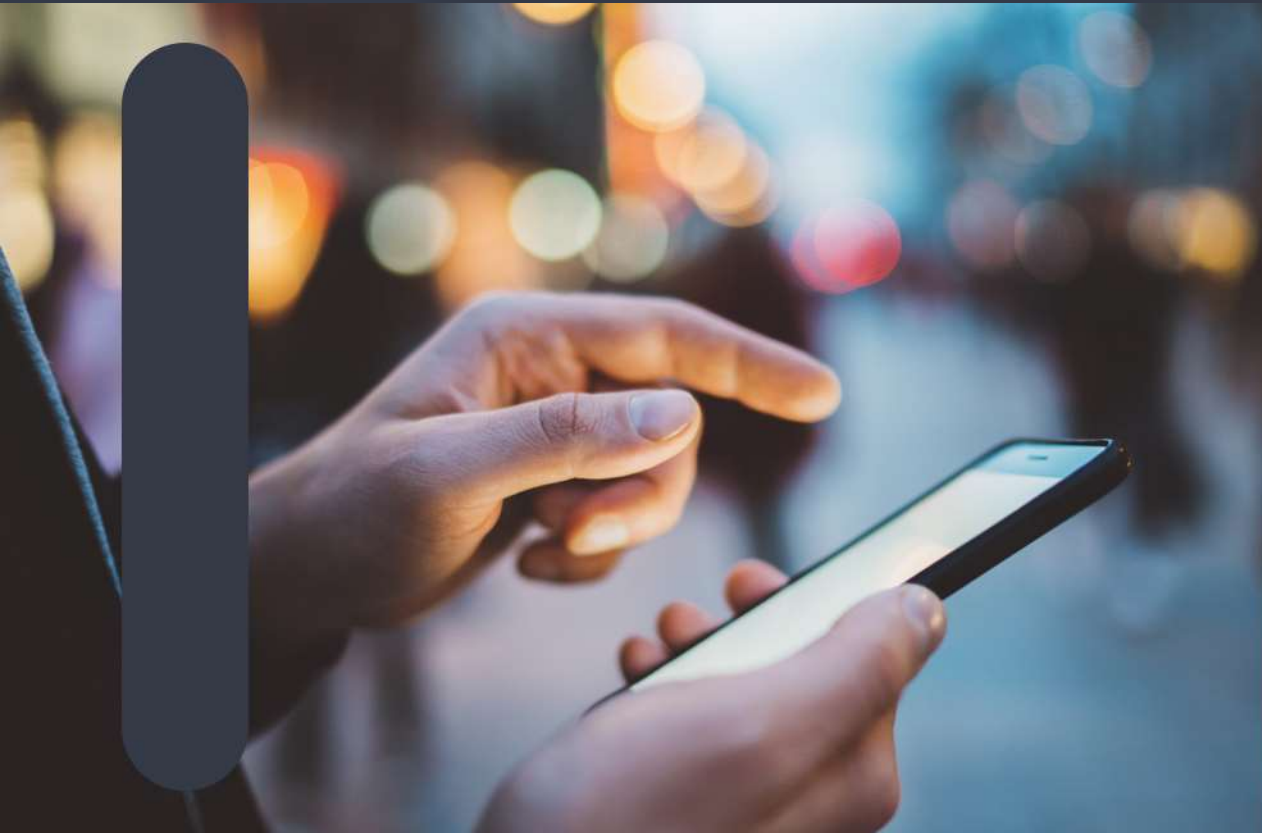
## Мошенничество на сайтах объявлений (фишинг)

**Мошенники используют поддельные сайты с объявлениями для того, чтобы получить через них персональные данные и деньги жертв. А реальные сайты с объявлениями они используют для обмана пользователей средствами социальной инженерии.**

**Цель – получение денег и персональных данных.**



Внимательно анализировать адрес сайта (URL), на который была переадресация. В большинстве случаев фишинга, несмотря на то, что сайт выглядит идентично настоящему, URL-адрес может отличаться от оригинального (например, заканчиваться на .com вместо .gov).



## Смишинг

**Мошенники отправляют жертве SMS-сообщение, содержащее ссылку на фишинговый сайт и мотивирующее получателя пройти на этот сайт.**

Необходимо следовать принципам безопасного поведения в интернете и не переходить по ссылкам, присланным в подозрительных или непонятных сообщениях электронной почты или через мессенджеры. Не загружать вложенные файлы из сообщений, которых вы не ожидали.

## Вишинг

**Мошенники звонят жертве для того, чтобы убедить её предоставить им разные персональные данные, например, данные банковской карты или логин и пароль от какого-либо сервиса.**



Никому ни при каких обстоятельствах не называйте данные своей карты, в особенности, три цифры на обратной стороне и код, который приходит вам в СМС. Не продолжайте разговор с мошенниками, скажите, что обратитесь в полицию.



# Оффлайн мошенничество

## Виды оффлайн угроз



### «Выгодное предложение»

Предлагают приобрести товар, услугу «с большой скидкой», «по акции» или «с субсидией для пожилых людей». Вас ограничивают во времени, торопят, заставляют совершать какие-либо действия в спешке. Мошенникам крайне важно не дать вам шанса хорошо подумать над их предложением.



### Приглашение на мероприятие

Приглашают в салоны красоты или медицинские центры на бесплатные процедуры или обследование. В учреждении «медиками» ставится «страшный диагноз», и прямо на месте вам предлагают пройти необходимое лечение по «новейшей методике» или с применением «уникальных средств». Эти дорогостоящие процедуры предлагается оформить в кредит.



### Вишинг

Выдавая себя за работников социальных учреждений, рассказывают пенсионерам, что им положены некие выплаты или льготы, чтобы их получить, надо подписать ряд документов. Затем подсовывают доверенность, которая позволяет мошенникам распоряжаться квартирой.





# Мошенничество

Что важно помнить?



Если вы стали жертвой мошенников – незамедлительно обращайтесь в полицию. Будьте бдительны!



Мошенники делают «очень выгодное предложение», цель данных действий – вынудить вас совершить действия, выгодные мошеннику.



Мошенники всячески вас торопят, сужают временные рамки, цель этих действий – не дать вам как следует все обдумать, проконсультироваться с родственниками.



Мошенники либо представляются сотрудниками государственных органов, либо говорят о том, что им доверяют звезды шоу-бизнеса или ваши соседи, только что купившие их товар. Цель этих действий – усыпить вашу бдительность и войти к вам в доверие.