

# Словарь кибермошенников



Фрейпинг

Смишинг

Доксинг

Снифферинг

Вишинг

# ФИШИНГ



**Вас пытаются поймать на удочку:** рассылают письма и СМС, маскируясь, например, под банк, известный сервис или госорган. Внутри — крючок: ссылка на подделку официального сайта.

**Цель** — чтобы вы, ничего не заподозрив, «клюнули» и ввели свои логины, пароли или данные карты. Всё это сразу попадёт к злоумышленникам.

## **Как защититься?**

Не переходите по ссылкам из подозрительных писем. Всегда заходите на сайты банков и сервисов напрямую, через браузер или официальное приложение.

# СМИШИНГ



СМС о выигрышах, суперраспродажах или получении выплат с просьбой перейти по ссылке для «оформления» или «подтверждения». Переходя по ссылкам, вы попадаете на фейковый сайт.

**Цель** — кража ваших данных или денег.

## Как защититься?

Не переходите по ссылкам и не звоните на номера из СМС. Помните: государство не рассылает сообщения со ссылками для получения выплат.



# Доксинг



Публикация личных данных человека (адрес, телефон, фото, место учебы) без его согласия.

**Цель** — травля и шантаж ради вымогательства денег, а также запугивание и угрозы распространить личную информацию с целью унижения жертвы.

## Как защититься?

Настройте приватность в соцсетях.  
Не выкладывайте в открытый доступ конфиденциальную информацию о себе и близких.  
Объясните детям, почему важно защищать личные данные.



# ВИШИНГ



Мошенники под разными предложениями под видом звонков по телефону «из банка», «из техподдержки» или «из полиции» вынуждают жертву перейти по фишинговой ссылке. Злоумышленники используют психологические приёмы.



**Цель** — выманить данные карт, пароли или коды подтверждения.

## Как защититься?

Никогда и никому не сообщайте по телефону коды, пароли из СМС и другие конфиденциальные данные. Прервите разговор и перезвоните в организацию по номеру с официального сайта.

# Претекстинг



Мошенник заранее собирает о вас информацию, например из соцсетей, чтобы во время звонка или переписки вы поверили, что имеете дело с «работником госорганов» или «службой безопасности».

**Цель** — доказать своё право на получение конфиденциальных данных.

## **Как защититься?**

Будьте всегда начеку, даже если собеседник знает малоизвестные факты о вас. Всегда перепроверяйте личность звонящего.

# Снифферинг



Кража данных через непроверенные точки трафика: VPN, общедоступный Wi-Fi — например, в кафе, аэропорту. Мошенники используют специальные программы-«снифферы» для перехвата информации, которую вы передаёте по незащищённой сети.

**Цель** — получить логины, пароли.

## **Как защититься?**

Не проводите платежи и не вводите пароли, подключаясь к публичной сети.



# Дроппинг



Вас делают посредником в преступной схеме. Через ваш счёт или кошелёк переводят украденные деньги.

**Цель** — использовать вас для обналичивания преступных денег.

## Как защититься?

Никогда не соглашайтесь на предложения «просто получить деньги на свой счёт» от незнакомцев. Обратитесь в банк, если вам поступил перевод с незнакомого номера и вас просят вернуть деньги.



# Фрейпинг



Мошенники обманом получают доступ к вашему аккаунту в соцсетях или мессенджерах. Получая доступ, они публикуют оскорбительную, провокационную информацию.

**Цель** — завладеть вашим аккаунтом и унижить, испортить имидж.

## **Как защититься?**

Используйте сложные пароли и двухфакторную аутентификацию для всех соцсетей. Никому не передавайте свои логины и пароли.

# Квишинг



В QR-кодах может быть зашита ссылка на фишинговый сайт или вирус. Их могут размещать на фальшивых квитанциях, объявлениях у подъездов или даже наклейках на самокатах.

**Цель** — кража данных.

## Как защититься?

Не сканируйте подозрительные QR-коды из непроверенных источников. Если отсканировали — не вводите на открывшейся странице личные и платёжные данные.

