ПРИЗНАКИ МОШЕННИЧЕСТВА:

ОСТОРОЖНО! МОШЕННИКИ!

Давление: «Если не сделаешь это сейчас, будет хуже»

Срочность: «Нужно прямо сейчас отправить деньги/сообщить данные»

Угрозы: «Твои родители могут пострадать, а тебя отправят в детский дом»

Мне звонит незнакомый номер...

⚠ ОСТАНОВИСЬ! ⚠

- **не отвечай** на звонки с незнакомых абонентских номеров;
- **не выполняй указания** неизвестных лиц, даже если они представились сотрудниками правоохранительных органов (с просьбой провести обыск в своем жилище, направленный на обнаружение денежных средств/ передать денежные средства курьеру/ передать личные данные и данные своих родственников);
- **сообщи взрослым** об указаниях неизвестных лиц;
- **обратись по номеру 02/102/112.**

Добрый день! Это прокурор. Необходимо следовать моим указаниям, иначе твои родители будут привлечены к уголовной ответственности...

ОСТОРОЖНО: МОШЕННИКИ!

НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

ИНТЕРНЕТ-МОШЕННИКИ

ОБЪЯВЛЕНИЕ О ПРОДАЖЕ

Мошенники-продавцы просят перечислить деньги за товар, который впоследствии жертва не получает.

ОБЪЯВЛЕНИЕ О ПОКУПКЕ

Мошенники-покупатели спрашивают реквизиты банковской карты и (или) смс-код якобы для перечисления денег за товар, после чего похищают деньги с банковского счета.

СООБЩЕНИЯ ОТ ДРУЗЕЙ

Мошенник пользуется чужой страничкой в социальной сети в Интернете, и под видом друга (родственника) просит перечислить ему деньги или сообщить данные Вашей карты якобы для перечисления Вам денег под различными предлогами.

ТЕЛЕФОННЫЕ МОШЕННИКИ

ЗВОНОК О НЕСЧАСТНОМ СЛУЧАЕ

Мошенники звонят жертве от лица близкого человека или от представителя власти и вымогают деньги.

Мама, я попал в аварию!

БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ

Сообщение о блокировании банковской карты с номером, по которому нужно позвонить. Цель – узнать личный код банковской карты.

ПОЛУЧЕНИЕ ВЫИГРЫША (компенсации за потерянный вклад)

Мошенники сообщают о выигрыше приза, возможности получения компенсации за потерянный вклад в «финансовую пирамиду» и т.п. Жертве можно забрать его, заплатив налог или плату якобы «за сохранность денег».

ВИРУС В ТЕЛЕФОНЕ

Мошенники запускают вирус в телефон, предлагая пройти по «зараженной ссылке» (в том числе и от имени друзей). С помощью вируса получают доступ к банковской карте, привязанной к телефону. Установите антивирус и не проходите по сомнительным ссылкам.

Если вас убеждают скачать приложение с целью перевода денежных средств на безопасный счет, прервите телефонный разговор, вам звонят мошенники!!!!!

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ

ОСТОРОЖНО! МОШЕННИКИ!

Звонок от мошенника

ПРИЗНАКИ

1. Вам предлагают перевести свои денежные средства на БЕЗОПАСНЫЙ СЧЁТ;
2. Вас просят ПРОДИКТОВАТЬ реквизиты банковской карты или ВВЕСТИ их на сайте;
3. Вам предлагают ОТМЕНИТЬ (взять) заявку на КРЕДИТ или ЗАБЛОКИРОВАТЬ банковскую карту;
4. Вам предлагают получить БОНУСЫ и ПОДАРКИ от банка, а также различные КОМПЕНСАЦИИ;
5. Вам предлагают оформить БЕЗОПАСНУЮ СДЕЛКУ или ДОСТАВКУ, при ПОКУПКЕ/ПРОДАЖЕ ТОВАРОВ в сети Интернет, при этом скидывают Вам ссылку;

ЗАПОМНИТЕ!

НЕ ОТВЕЧАЙТЕ НА ЗВОНКИ, поступившие с неизвестных номеров, особенно зарегистрированных в другом регионе;

НЕ ВЕРЬТЕ любой информации от незнакомца, **ДАЖЕ ЕСЛИ** звонок поступил с официального телефона горячей линии банка;

ПРЕРВИТЕ РАЗГОВОР и самостоятельно позвоните на телефон горячей линии банка, набрав номер **ВРУЧНУЮ**;

ПОМНИТЕ: код от вашей карты и пароли подтверждения операций **НЕ ИМЕЕТ ПРАВА** спрашивать даже сотрудник банка!

КАК ЗАЩИТИТЬСЯ ОТ ИНТЕРНЕТ-МОШЕННИКОВ

1. Не переходите по подозрительным ссылкам
Даже если они пришли от знакомых. Мошенники часто взламывают аккаунты и рассылают фишинговые сайты.

2. Не вводите персональные данные на неизвестных сайтах
Если просят паспорт, СНИЛС, данные карты — дважды проверьте источник. Банки и госслужбы не запрашивают это через мессенджеры и соцсети.

3. Не устанавливайте программы по просьбе "сотрудников банка"
Никогда. Ни "удалённый доступ", ни "обеспечение безопасности" не требуют установки стороннего ПО.

4. Проверяйте адрес сайта (URL)
Настоящий сайт всегда начинается с https:// и содержит корректное доменное имя. Остальное — обманка.

5. Не ведитесь на "экстренность"
Фразы вроде "Ваш счёт заблокирован", "Вы попали в реестр должников", "Оформлен кредит" — классическая уловка. Не спешите, перезвоните официальным контактам.

6. Не переводите деньги неизвестным
Даже если звонят "родственники", "покупатели", "курьеры" или "сотрудники госорганов". Всегда проверяйте личность звонящего.

7. Используйте антивирус и двухфакторную аутентификацию
Это минимальная цифровая гигиена, которая может спасти ваши данные и деньги.

Главное правило: если сомневаетесь — не действуйте в спешке. Перепроверьте информацию и посоветуйтесь с близкими.

АЛГОРИТМ ДЕЙСТВИЙ ПО ПРЕДУПРЕЖДЕНИЮ МОШЕННИЧЕСТВА

Самые распространенные виды телефонного мошенничества:

1. Мошенники рассылают сообщения с мольбой: «Ребёнку нужен донор». В SMS указывается номер, куда нужно позвонить в случае согласия. При звонке со счета владельца снимаются дополнительные средства.

2. «Оператор» звонит лично и сообщает о проблемах с Вашим счетом. На предложенный номер предлагает отправить SMS. Проблемы со счетом появляются как раз после отправленного сообщения.

3. На телефон приходит SMS «Привет, как дела?». Разговорчивый абонент может продлить переписку вплоть до отрицательного баланса в пользу тайного собеседника.

4. Абоненту звонит молодой человек и объясняет, что случайно положил деньги не на свой, а на его счет. Настойчиво, но вежливо мошенник будет упрашивать перевести ему такую же сумму в ответ.

5. На улице подходит незнакомец и просит позвонить с Вашего мобильного. Злоумышленник звонит с него на платные номера.

6. Абоненту звонят с неизвестного номера. Он из любопытства перезванивает, но платит за это соединение гораздо больше, чем за обычный звонок по тарифу.

7. Абоненту сообщают по телефону, что он выиграл приз от компании – оператора, но чтобы его забрать, надо купить карту оплаты. После этого абонента якобы переводят на автоматическую систему пополнения счета. По тоновым сигналам мошенники вычисляют код карты и переводят деньги на свой счет. **Будьте внимательны при получении SMS-сообщения «Вы выиграли!».** Со 100% вероятностью оно содержит ссылку на некий интернет-ресурс, благодаря которому Ваш гаджет будет заражен вредоносной программой. В результате это даст доступ мошенникам к Вашей банковской карте!

8. «Вам предоставлена компенсация». Звонок от неизвестного абонента о полагающейся Вам компенсации за приобретенный ранее товар может оказаться ловушкой. Перепроверьте данное сообщение, перезвоните в магазин, где Вы совершили покупку!

Безопасное поведение школьника в сети интернет

Всегда рассказывай родителям, если у тебя есть какие-либо подозрения или страхи, связанные с интернетом

Не покупайся на различные заманчивые предложения на страницах интернета

Никогда и не при каких обстоятельствах не отправляй незнакомцам контактную информацию о себе и реквизиты банковских платежных карточек родителей

Помни, что совершая покупки в интернете ты потратишь свои реальные денежные средства

Никогда не встречайся с незнакомцами из интернета в реальной жизни и не выполняй для них какие-либо услуги за денежное вознаграждение

Не переходи по предложенным незнакомцами ссылкам. Не открывай спам-сообщения с различными файловыми вложениями

Не публикуй в интернете информацию, которая в дальнейшем может скомпрометировать тебя или твоих близких

Информация, которую не следует размещать на своих страницах в социальных сетях

- *О СВОЕМ МЕСТОПОЛОЖЕНИИ*
- *О ПЛАНАХ НА ДЛИТЕЛЬНЫЕ ПОЕЗДКИ*
- *ФОТО ДОРОГИХ ВЕЩЕЙ И ПОДАРКОВ*
- *ФОТО КВАРТИРЫ ИЛИ ДОМА*
- *СВОЙ ДОМАШНИЙ АДРЕС*
- *КОПИИ ЛИЧНЫХ ДОКУМЕНТОВ*

ПРАВИЛА БЕЗОПАСНОГО ИНТЕРНЕТА ДЛЯ ДЕТЕЙ

В период дистанционного обучения школьники много времени проводят в Интернете. Объясните детям несколько простых правил сетевой безопасности

Проверь вместе с родителями настройки своего аккаунта в соцсетях: пусть только твои друзья могут видеть информацию на этой страничке и писать тебе сообщения

Не размещай в сети номер телефона и школы, домашний адрес и большое количество фотографий с геотегами

Не переходи по подозрительным коротким ссылкам в сообщениях, полученных от незнакомцев. А если возникло подозрение, что кого-то из друзей взломали (от него приходят странные сообщения), свяжись с ним по телефону

Защити свои аккаунты. Для каждой соцсети придумай свой уникальный сложный пароль - от 8 символов, с большими и маленькими буквами, цифрами и спецсимволами