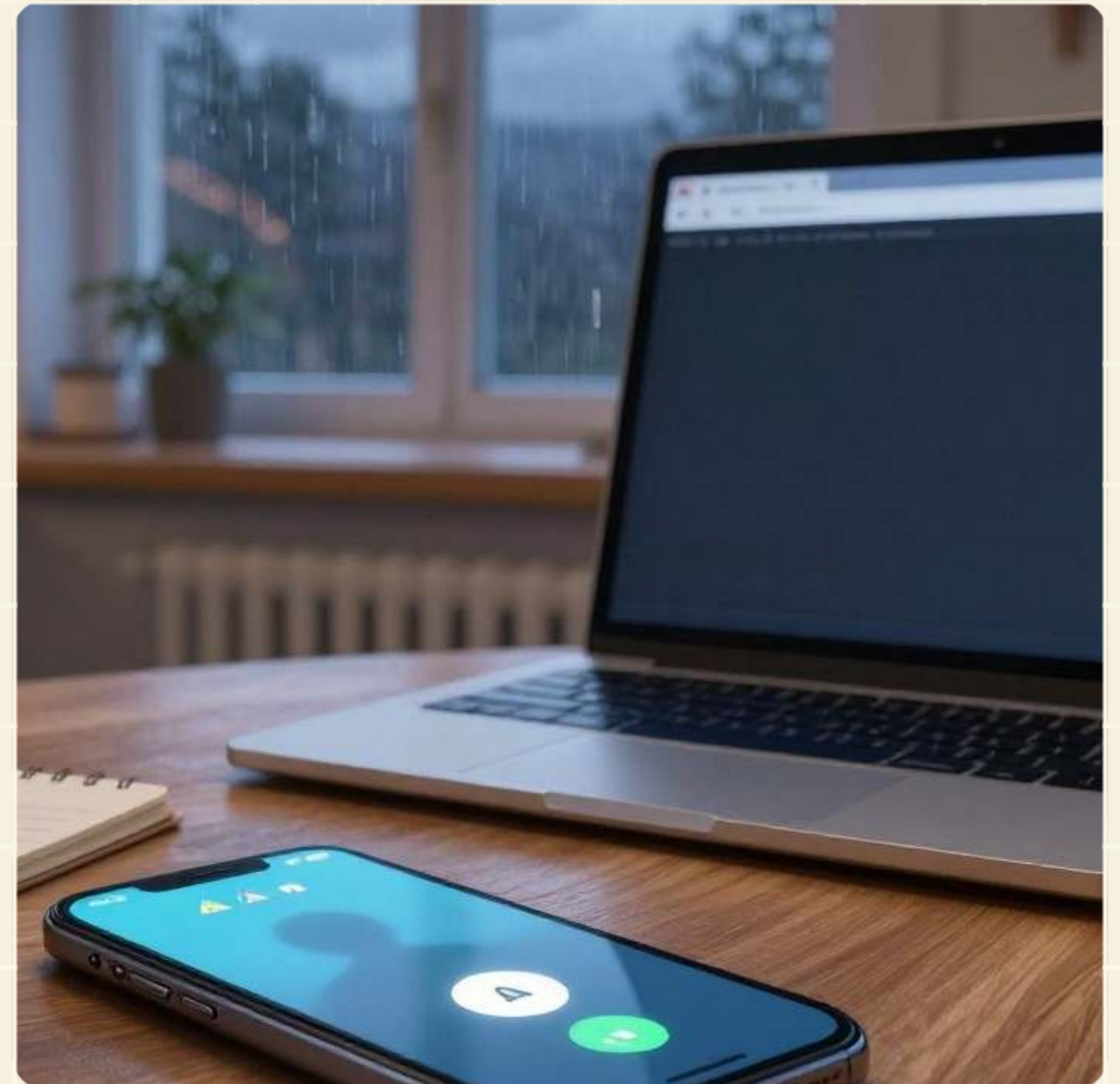




Защита от мошенников: основы безопасного поведения

Как распознать обман и защитить себя в
сети, по телефону и в мессенджерах.



Почему подросткам важно знать правила защиты от обмана

Подростки постоянно пользуются смартфоном, соцсетями, играми и объявлениями, поэтому чаще сталкиваются с фальшивыми сообщениями и поддельными страницами. Мошенники дают спешкой, выгодой и страхом, чтобы заставить действовать без проверки.



01

Звонки от «банка» или «службы безопасности» обычно подталкивают назвать код, пароль или подтвердить операцию, хотя на самом деле цель — получить доступ к аккаунту или карте.

02

Сообщения о выигрыше, подарке или срочной помощи другу создают ощущение выгоды и доверия, но часто ведут на поддельные страницы или к просьбе перевести деньги.

03

Фальшивые интернет-магазины, сервисы объявлений и страницы входа копируют знакомый внешний вид, чтобы вы сами ввели данные и потеряли доступ к своим сервисам.

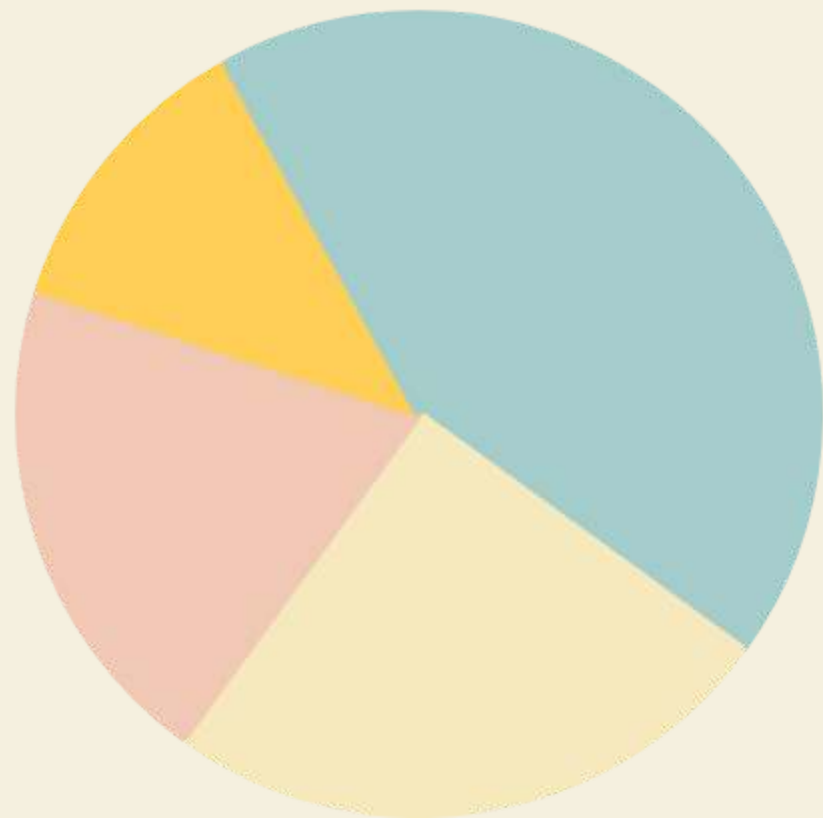
04

В играх обман строится на обещаниях бесплатной валюты, редких предметов и быстрого роста уровня, а затем требует код, пароль или переход по опасной ссылке.

Основные схемы обмана, с которыми сталкиваются школьники

Какие приёмы давления чаще всего используют мошенники

Срочность Страх Выгода
Доверие Жалость



- Такие сообщения специально заставляют не думать и отвечать сразу, пока человек растерян.
- Чаще всего обман опирается на срочность и страх, поэтому пауза и проверка резко снижают риск ошибки.

Обобщение типичных приёмов социальной инженерии в учебных материалах по цифровой безопасности.

Фишинг: поддельные сайты и сообщения



Фишинг маскируется под знакомые сервисы и просит ввести пароль, код или данные карты. Ошибка в адресе, лишние символы и навязчивая срочность часто выдают подделку.

Опаснее всего переходить по ссылкам из сообщений, когда обещают приз, скидку или блокировку аккаунта. Безопаснее открыть сайт вручную и проверить адрес самостоятельно.

Признаки мошеннического сообщения и их значение

- Одинстораживающий признак уже повод остановиться и всё перепроверить.
- Срочность, коды, подозрительные ссылки и просьбы о деньгах помогают быстро распознать опасное сообщение до того, как будет нанесён вред.

Признак	Что значит	Чтостораживает
Срочность	Давят на ответ	Не дают подумать
Код	Пытаются украсть доступ	Просят SMS
Ссылка	Ведёт на подделку	Адрес выглядит странно
Приз	Приманка доверия	Слишком выгодно
Перевод	Риск потери денег	Просят заплатить



Обобщение типичных признаков мошенничества в цифровой среде.

Какие личные данные нельзя сообщать



Пароли и коды

Никому нельзя сообщать пароли, одноразовые коды и SMS-подтверждения: именно они открывают доступ к аккаунтам и позволяют злоумышленнику войти от вашего имени.



Данные карты

Номер карты, срок действия, CVV-код и фото банковской карты нельзя передавать даже знакомым в переписке, если нет полной уверенности в их подлинности.



Документы и адрес

Фотографии документов, адрес проживания и номер школы помогают мошенникам выдавать себя за вас, оформлять доступ к сервисам и подбирать убедительные сообщения.



Геолокация

Местоположение, расписание и привычные маршруты раскрывают, где вы находитесь и когда вас легко отвлечь или обмануть через личное сообщение.



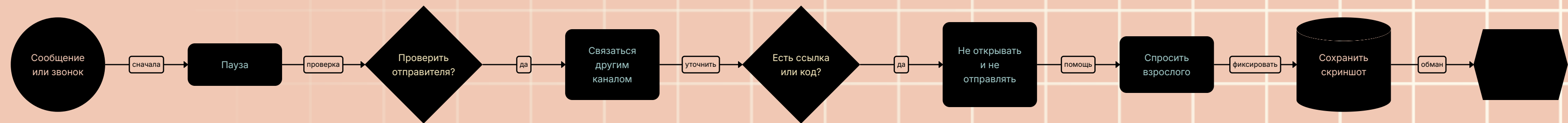
Контакты близких

Номера телефонов родителей и друзей тоже нужно беречь: их используют для давления, выманивания денег и создания ложного доверия в переписке.

Как действовать при подозрительном сообщении



Последовательность шагов для проверки и безопасной реакции.



Безопасные пароли и защита аккаунтов

01

Надёжный пароль должен быть длинным, разным для каждого сервиса и составленным из букв, цифр и знаков. Простые варианты вроде имени, даты рождения и 123456 легко угадываются.

02

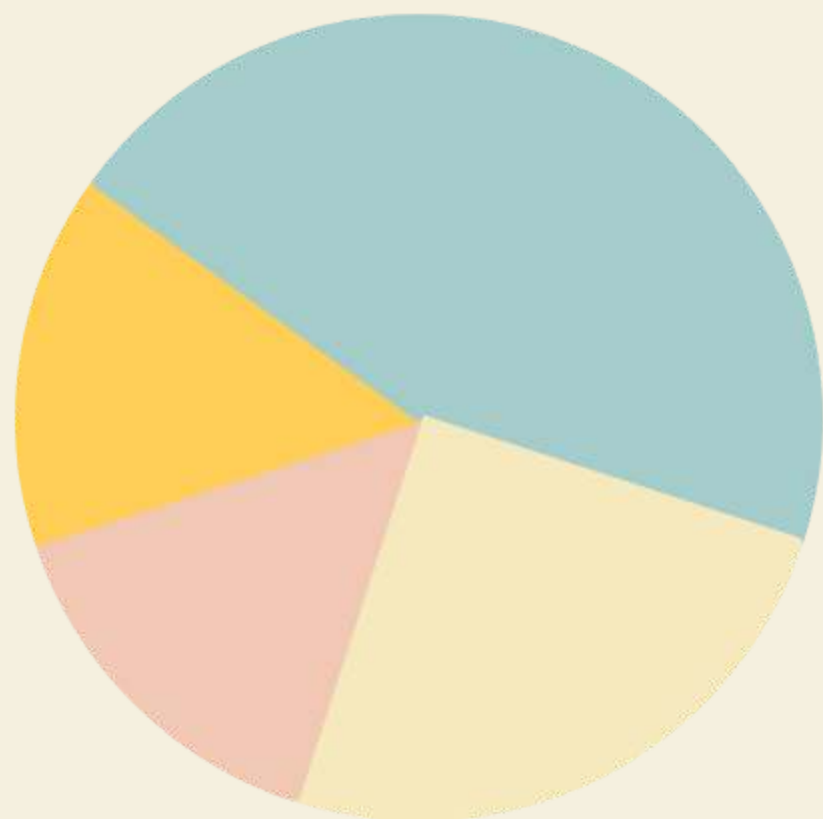
Дополнительную защиту дают двухфакторная проверка, уведомления о входе и выходе из чужих устройств. Полезно регулярно смотреть, где аккаунт открыт, и закрывать лишние сессии.

03

Если пароль уже использовался где-то ещё, его лучше заменить сразу. Один взломанный сервис не должен открывать доступ ко всем остальным аккаунтам.

Где чаще всего встречаются попытки обмана

Мессенджеры Соцсети Телефон
Игровые чаты Сайты объявлений



- В разных каналах мошенники используют свои приманки: от «подарков» до срочных просьб о помощи.

- Мессенджеры и соцсети особенно рискованны из-за поддельных аккаунтов, а в играх и объявлениях чаще встречаются ловушки с выгодой и предоплатой.

Обобщение типичных каналов мошенничества в интернете, играх и телефонных звонках.

Мошенничество в играх и при онлайн-покупках

В играх мошенники обещают бесплатную валюту, скины или быстрый рост уровня, но затем требуют пароль, код или переход по ссылке, чтобы украсть доступ к аккаунту.

На сайтах объявлений опасны слишком низкая цена и просьба о предоплате: после перевода продавец исчезает. Без проверки нельзя платить незнакомым людям и вводить данные карты.

Что делать в опасной ситуации



Ситуация	Действие	Почему
Просят код	Не сообщать	Кража доступа
Ссылка вызывает сомнение	Не открывать	Риск фишинга
Звонят «из банка»	Перезвонить самому	Может быть обман
Аккаунт взломан	Сменить пароль	Нужно остановить доступ

- Таблица показывает, как реагировать на самые частые признаки обмана. Главное — не спешить и сразу выбирать безопасное действие.
-

- Если действие связано с кодом, ссылкой или деньгами, нужно
- остановиться и проверить информацию через официальный канал или взрослого.

Как проверять информацию без ошибок

1. Остановиться

Не отвечайте сразу на сообщение и не переходите по ссылке. Пауза помогает заметить срочность, давление и другие признаки манипуляции.

3. Сравнить факты

Проверьте новость или просьбу минимум по двум надёжным источникам. Особенно внимательно относитесь к просьбам о деньгах, кодах и установке приложений.

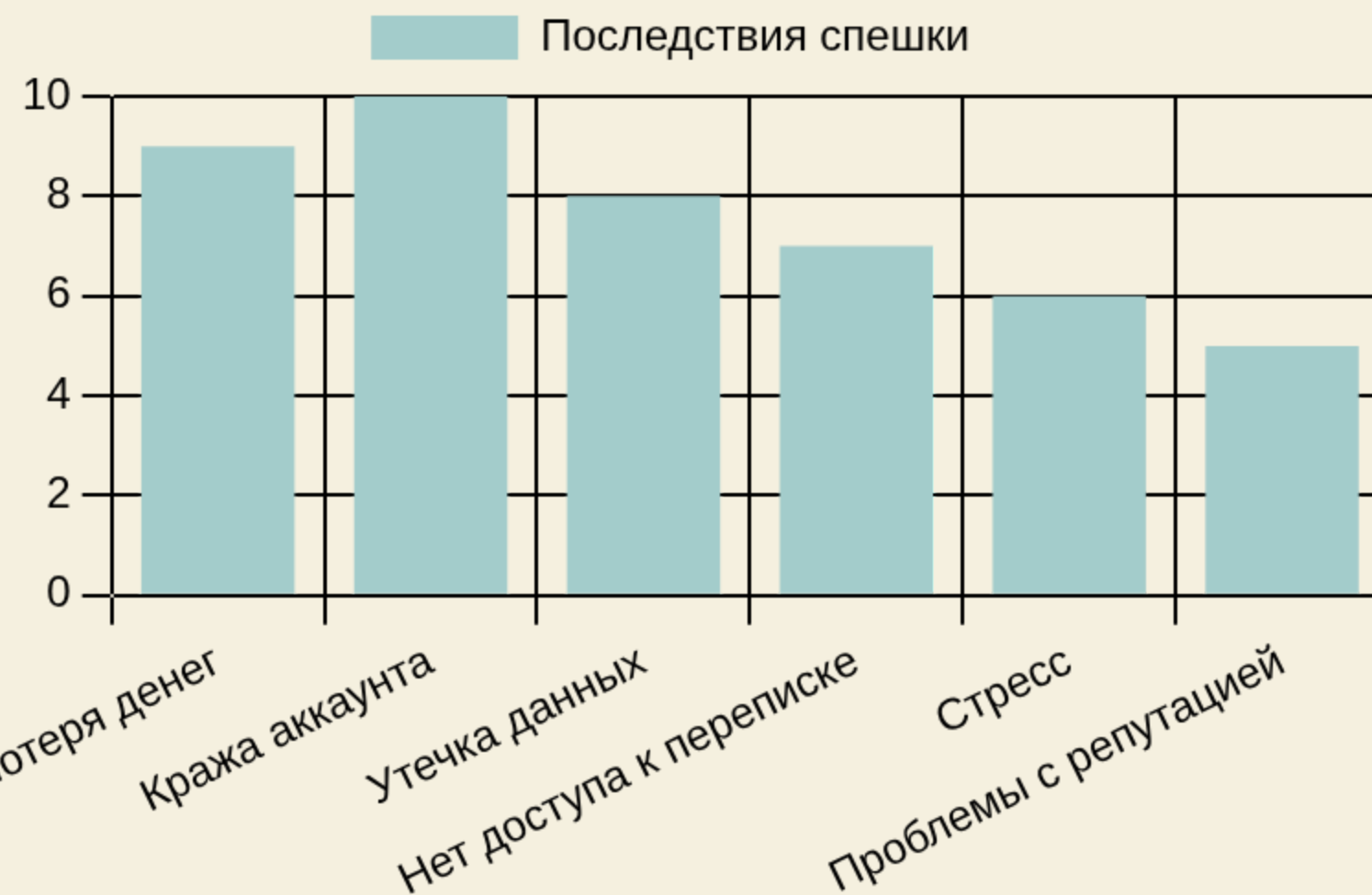
2. Найти официальный источник

Контакты берите только на сайте организации, в приложении или на карте. Номер телефона лучше набрать вручную, а не из сообщения.

4. Принять безопасное решение

Если информация не подтверждается, не отвечайте и не выполняйте просьбу. При сомнении сразу обратитесь к взрослому или в поддержку сервиса.

К чему приводит спешка и невнимательность



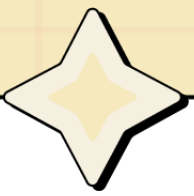
- Даже один неосторожный клик может запустить цепочку проблем, которые потом трудно остановить без помощи взрослых и службы поддержки.
- Самые серьёзные риски связаны с потерей доступа к аккаунтам и утечкой данных: именно они чаще всего дают мошенникам новые способы атаки.

Сводка типичных последствий интернет-мошенничества;
оценка по степени риска для школьников

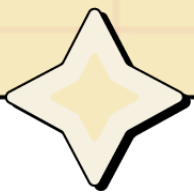
Если обман уже произошёл



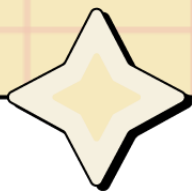
Сразу расскажите взрослому, что случилось, и не скрывайте детали. Чем раньше начнётся помощь, тем легче остановить дальнейший вред и вернуть контроль над аккаунтом.



Смените пароли, завершите все активные сеансы и сохраните переписку, ссылки и скриншоты. Эти материалы помогут разобраться в ситуации и подтвердить факт обмана.



Если были деньги или карта, немедленно свяжитесь с банком и заблокируйте карту при необходимости. При переводе средств важно действовать без промедления.

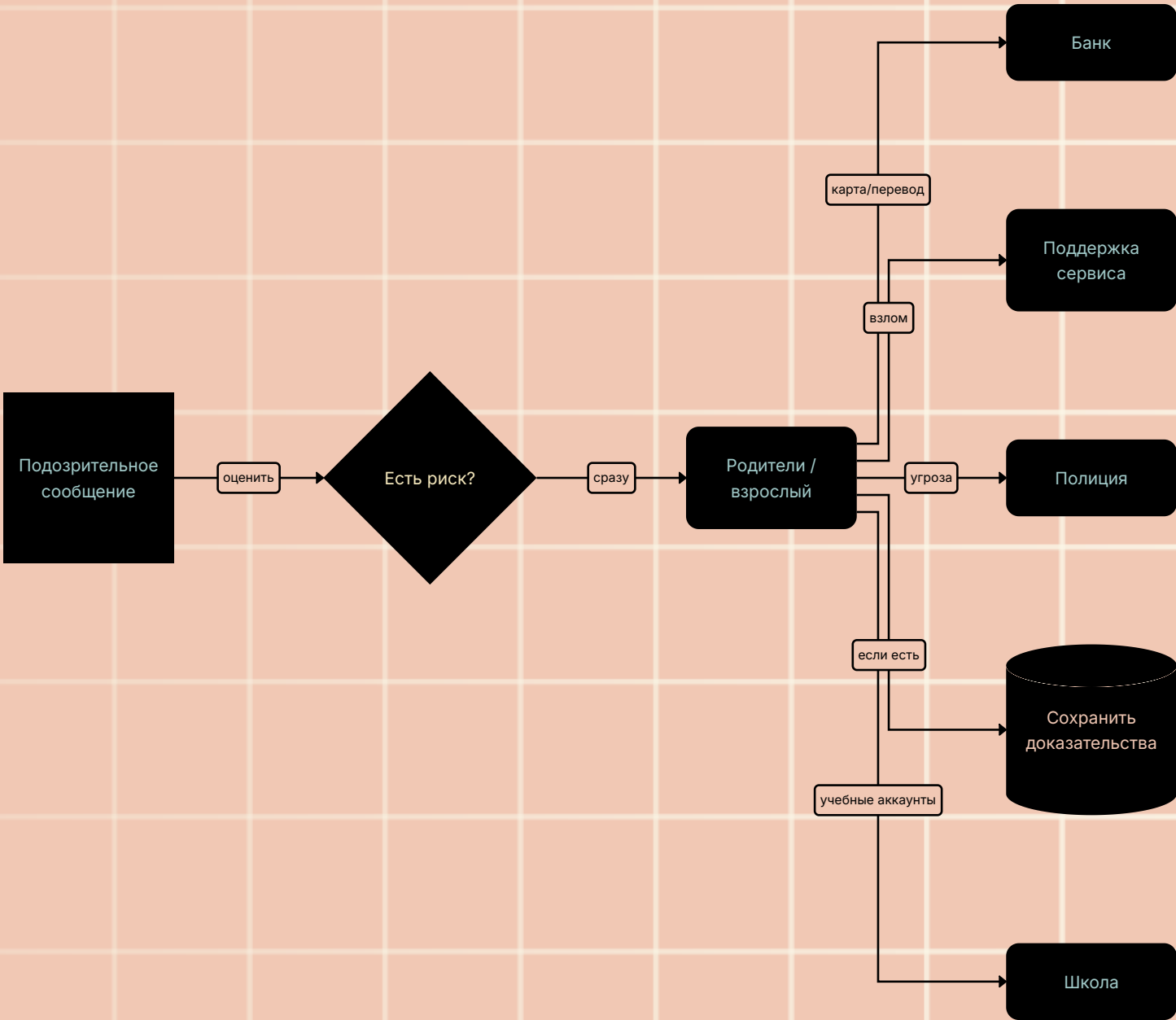


При серьёзном ущербе, угрозах или вымогательстве нужно обратиться в полицию. Сообщите все известные данные, чтобы помочь остановить мошенников.

Кому сообщать о мошенничестве



Схема обращения после подозрительного сообщения или взлома аккаунта



Правила цифровой осторожности на каждый день



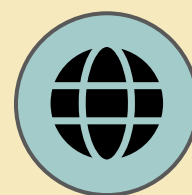
Не переходить по ссылкам

Незнакомая ссылка может вести на поддельный сайт или запускать вредоносную страницу. Перед переходом всегда проверяйте адрес и источник сообщения.



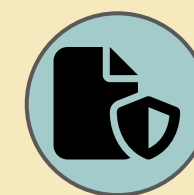
Не передавать коды и пароли

Коды из SMS и пароли нужны только владельцу аккаунта. Если их просят сообщить срочно, это почти всегда попытка получить доступ.



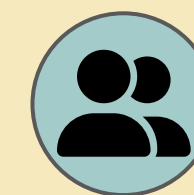
Проверять адрес сайта

Даже одна лишняя буква в адресе может означать подделку. Вводите сайт вручную или открывайте его через сохранённую закладку.



Осторожно с файлами и приложениями

Не открывайте файлы и не ставьте приложения из сомнительных сообщений. Они могут украсть данные или выдать себя за полезный сервис.



Советоваться со взрослыми

Если сообщение вызывает сомнение, лучше показать его родителям или учителю. Совместная проверка помогает избежать ошибки и лишнего риска.

Короткий чек-лист безопасного поведения

- Краткий список привычек помогает быстро оценить сообщение и выбрать безопасное действие.
- Пять простых привычек закрывают большинство типичных рисков: поддельные аккаунты, кражу доступа, фишинг и давление на эмоции.

Действие	Зачем
Проверить отправителя	Не ответить мошеннику
Не торопиться	Замечать несоответствия
Не сообщать код	Защитить доступ
Сложный пароль	Снизить риск взлома
Сказать взрослому	Получить помощь



Семья, школа и друзья как защита от обмана



Когда сообщение читают вместе

Пятикласснику приходит письмо о «выигрыше», и он почти нажимает на ссылку. Мама замечает странный адрес и ошибки в тексте, поэтому переход удаётся остановить вовремя. Совместная проверка занимает минуту, но экономит нервы и деньги.



Подруга, которая заметила поддельный аккаунт

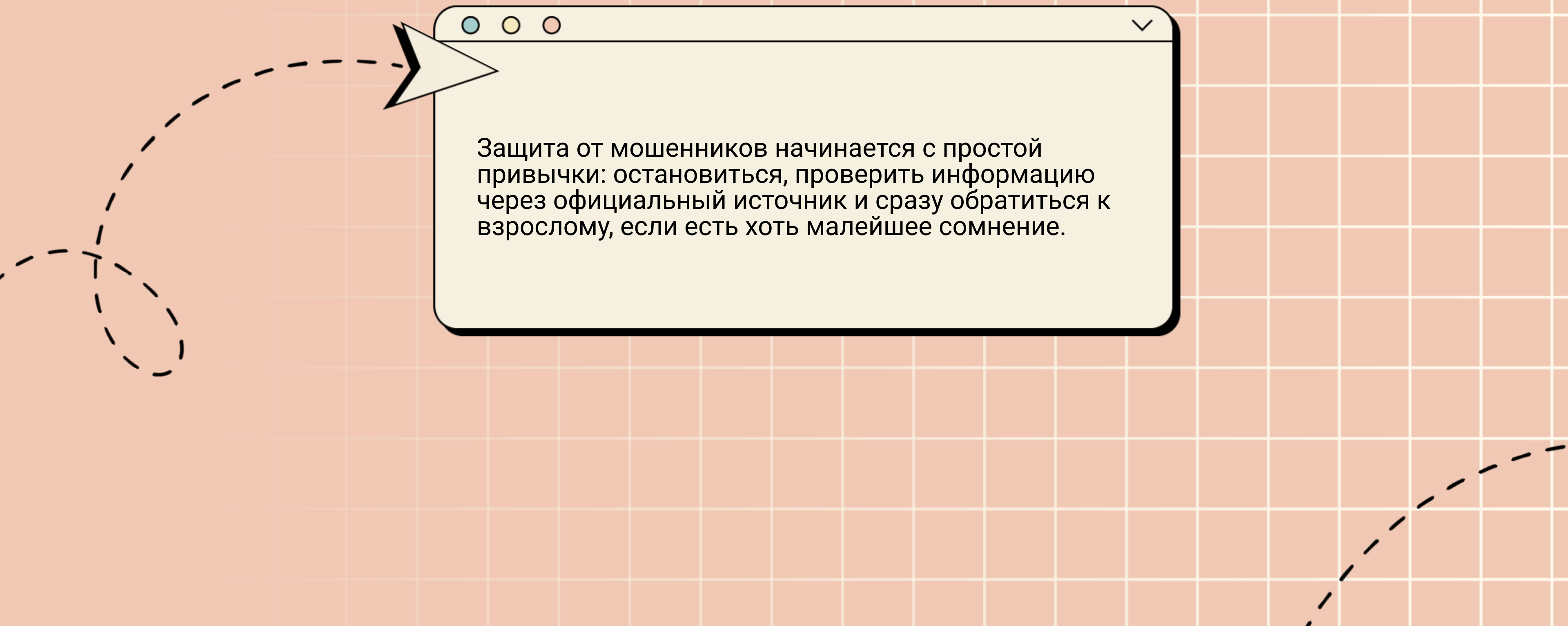
В чате появляется просьба срочно перевести деньги якобы от знакомой. Одна из подруг не спешит отвечать и звонит по обычному телефону. Оказывается, страницу уже взломали, а рассылка ушла всем подряд.



Школьный разговор после игры

После матча друзья обсуждают обещание бесплатных скинов и редких предметов. Учитель напоминает, что хорошие бонусы не раздают за код из SMS. Когда об этом знают все, мошенникам труднее застать подростков врасплох.

Главный вывод: пауза, проверка, помощь



Защита от мошенников начинается с простой привычки: остановиться, проверить информацию через официальный источник и сразу обратиться к взрослому, если есть хоть малейшее сомнение.