

Лето в телефоне. Как защитить детей от кибермошенников во время каникул

Летние каникулы давно перестали быть только про велосипеды, дворы и поездки к бабушке. Сегодня лето у многих детей проходит в двух пространствах одновременно: офлайн и онлайн. Пока родители работают, подростки часами сидят в играх, смотрят видео, переписываются в мессенджерах, знакомятся в соцсетях и проводят время в голосовых чатах. TikTok, Discord и Telegram - именно туда на летние каникулы выходят и мошенники.

«Бесплатные бонусы» и ловушки в играх

Именно летом цифровая активность детей резко растет. Вместе с ней растет и интерес мошенников. Для них школьные каникулы - почти отдельный сезон. Дети чаще остаются без присмотра, быстрее принимают решения и легче вовлекаются в эмоциональные истории: розыгрыши, игровые подарки, «секретные» предложения или тревожные сообщения.

Самая большая территория риска — онлайн-игры. Именно там дети чаще всего сталкиваются с мошенниками впервые.

Схема выглядит почти безобидно. Подростку пишет человек с красивым профилем и предлагает подарок: игровую валюту, редкий предмет, прокачанный аккаунт или доступ к закрытым возможностям. Иногда мошенники маскируются под популярных стримеров или даже под знакомых игроков.

Дальше все развивается одинаково: ссылка, авторизация, просьба ввести код или пароль. Ребенок уверен, что просто получает бонус, но на самом деле передает доступ к своему аккаунту.

В одной из таких ситуаций школьник во время летних каникул решил получить «бесплатный Battle Pass» в популярной игре. После входа через поддельный сайт он потерял не только игровой аккаунт, но и доступ к электронной почте, к которой был привязан профиль. Для подростков это часто становится настоящей трагедией. В цифровом мире аккаунт — это не просто игра. Это месяцы или годы времени, общения и вложенных денег.

Поэтому зачастую ребенок готов сделать почти что угодно, чтобы вернуть аккаунт. Нередки случаи, когда дети сообщали данные банковских карт и счетов родителей только чтобы вновь получить доступ к любимой игре. Самое обидное, что обычно вернуть аккаунт уже невозможно.

Под угрозой будут находиться и друзья горе-игрока. Мошенники не стесняются отправлять сообщения притворяясь друзьями и знакомыми. И порой ребенка может подвести его доброта и желание помочь. Поэтому угроза здесь двойная и внимательнее нужно быть тоже в несколько раз.

Соцсети: где любопытство работает против ребенка

Если взрослые чаще попадают на страхе, то дети - на любопытстве.

«Это ты на фото?», «Смотри, что про тебя сняли». «Ты попал в видео».

Такие сообщения приходят в мессенджерах ежедневно. Особенно летом, когда дети активнее знакомятся онлайн и добавляют новых людей.

Поддельные ссылки ведут на фальшивые страницы авторизации. Внешне они почти не отличаются от настоящих сервисов. Ребенок вводит логин и пароль - и аккаунт оказывается у злоумышленников.

После этого начинается вторая волна мошенничества. От имени подростка друзьям рассылают просьбы занять деньги, проголосовать в конкурсе или перейти по ссылке. И именно потому, что сообщение приходит «от своего», доверия к нему гораздо больше.

Интернет-дружба как инструмент манипуляции

Самые опасные схемы сегодня далеко не всегда связаны с технологиями. Все чаще мошенники работают через психологию.

Во время каникул подростки проводят много времени онлайн и легче идут на контакт. Этим пользуются злоумышленники. Они могут неделями общаться с ребенком: обсуждать музыку, игры, фильмы, школу. Иногда создается ощущение настоящей дружбы.

Потом появляется просьба. Сначала небольшая и «безобидная»: помочь зарегистрироваться, отправить код из SMS, дать аккаунт «на время» или перевести небольшую сумму.

В одной ситуации подросток несколько недель общался в игровом чате с человеком, который представился ровесником. Позже «друг» попросил помочь пройти верификацию и прислать код из сообщения банка, потому что «у него не работает номер». Ребенок не понял, что фактически подтверждает банковскую операцию.

Главная проблема в том, что дети часто не воспринимают интернет-общение как потенциально опасное. Для них это такая же дружба, только через экран.

Розыгрыши, скидки и «подарки от блогеров»

Летом резко увеличивается количество фейковых конкурсов и псевдорозыгрышей. Особенно в TikTok, Telegram и Instagram.

«Вы выиграли смартфон». «Заберите сертификат». «Подарок подписчикам».

Обычно ребенка просят перейти по ссылке, заполнить анкету или оплатить «доставку». Суммы небольшие – несколько сот или пару тысяч тенге. Именно поэтому схема и работает: потеря кажется незначительной, а ребенок может даже не рассказать об этом взрослым.

Иногда мошенники специально делают «выигрыш» максимально правдоподобным. Используют логотипы известных брендов, фотографии популярных блогеров и даже поддельные комментарии победителей.

Для подростков это выглядит как обычная интернет-активность, а не преступление. Последствия же могут быть аналогичны предыдущим случаям.

Иногда ребенок оказывается не жертвой, а невольным помощником мошенников. Например, подростку предлагают «легкий заработок» на лето: принять перевод на карту, помочь с регистрацией аккаунтов или передать банковскую карту «для работы». За это обещают процент или быстрые деньги.

На самом деле через такие карты могут проходить украденные средства. А ребенок, сам того не понимая, становится участником незаконной схемы.

Подобные предложения особенно опасны именно летом, когда подростки хотят собственные деньги, но еще не умеют оценивать последствия.

Почему запреты почти не работают

Первый импульс многих родителей – просто ограничить интернет. Но полный запрет редко дает результат. Современные дети живут онлайн так же естественно, как прошлые поколения жили во дворе. Интернет для них — это общение, отдых, игры и социальная среда.

Поэтому гораздо важнее не тотальный контроль, а привычка обсуждать цифровую безопасность спокойно и регулярно.

Ребенок должен понимать: мошенник — это не обязательно взрослый человек с подозрительным голосом. Иногда это дружелюбный профиль с мемами, популярный игровой аккаунт или «знакомый», который пишет с чужой страницы.

Поэтому полностью исключить риски невозможно. Но снизить их вполне реально.

Полезно заранее договориться с ребенком о нескольких простых правилах:

- никогда не вводить данные карты без взрослых;
- не сообщать коды из SMS даже друзьям;
- не переходить по ссылкам из сообщений;
- включить двухфакторную защиту для почты, игр и соцсетей;
- не хранить банковские данные в открытом доступе на устройствах;
- обсуждать новые схемы мошенничества без запугивания;
- объяснить, что даже «маленький секрет» от родителей в интернете может стать большой проблемой.

И, пожалуй, самое важное правило: ребенок не должен бояться признаться, что ошибся.

Потому что в большинстве случаев мошенники побеждают не технологии, а молчание и растерянность. А цифровая безопасность сегодня это уже такая же базовая привычка, как смотреть по сторонам перед дорогой. Расскажите об опасности своим детям.

Материал подготовлен при помощи www.fingramota.kz