detkityumen.ru

Как защитить детей от онлайн-мошенников

Кот Базилио и лиса Алиса перепробовали множество хитростей, пытаясь заманить Буратино в Страну Дураков и украсть его золотые. Но, как сказала бы черепаха Тортилла, это было "триста лет тому назад". Рассказываем, **какие уловки мошенники используют сегодня**, чтобы обмануть детей и добраться до их карманных денег или до банковских счетов их родителей.

Теперь мошенники охотятся не просто за "золотыми", а **за данными банковских карт**, с которых можно украсть сразу все деньги, если повезет. Они пытаются раздобыть новые "золотые ключики" — секретные пароли и коды, — которые откроют им заветную "дверь" от банковских карт детей и их родителей.

Многие школьники используют банковские карты, привязанные к счету родителей или оформленные на себя (если у них уже есть паспорт). Иногда через детей мошенники пытаются добраться не только до денег, но и до документов взрослых. Чтобы втереться в доверие ребенка, в ход идут обкатанные схемы.

Создают фейковые страницы для онлайн-покупок

Хакеры любят онлайн-игры не меньше, чем дети, но у них на это свои причины. В виртуальном мире бдительность ослабевает, и игроки могут не заметить обмана и клюнуть на уловки мошенников. Например, на предложение **"выгодно купить" объекты для игры на фейковом сайте.**

"Мы с ребятами из школы подсели на одну онлайн-игру, там можно общаться между собой и знакомиться с другими игроками. Игра сама по себе бесплатная, но чтобы быть наравне с топами, нужно платить за лучший шмот и пушки. В игре есть свой магазин, где все это можно купить. Однажды мне написал в игровой чат какой-то парень, мы поболтали, и он по секрету скинул мне ссылку…"
Будьте бдительны, не наступайте на чужие грабли!

Игроков заманивают низкими ценами и "уникальными акциями". И не стоит заблуждаться, в подобные ловушки могут попасть не только дети, но и взрослые.

"Мы с мужем решили подарить сыну смартфон на день рождения. Он выбрал дорогую модель, но 18 лет не каждый день исполняется — надо его порадовать. Посмотрели в интернете, где купить такой телефон, и наткнулись на московский интернет-магазин с доставкой в любую точку России. Цены там намного ниже, чем везде…"
Будьте бдительны, не наступайте на чужие грабли!

Прежде чем вводить где бы то ни было персональные данные, пароли, коды или реквизиты банковской карты, **удостоверьтесь, что это не мошенническая страница**.

Как отличить фишинговый сайт от настоящего?

- Длинное и сложное доменное имя или имя, похожее на название известного интернет-магазина, банка, социальной сети, бренда.
- Перед адресом сайта нет префикса https: буква s означает secure — безопасное соединение.
- Сайт зарегистрировать совсем недавно. Проверить дату создания домена можно здесь: whois-service.
- Встречаются опечатки, несоответствия, небрежности и ошибки: орфографические, пунктуационные, фактические.
- Цены ниже рыночных более чем на 20%. Даже если их объясняют таможенным конфискатом или ликвидацией товара, это настораживает.
- Ссылка пришла из неизвестного вам источника. Будьте осторожнее и со ссылками друзей в соцсетях: их могли ввести в заблуждение или взломать.
- Вы попали на сайт, вызвавший подозрения, когда использовать открытую сеть Wi-Fi без пароля.

Похожие схемы мошенничества работают и вне интернета, поэтому никому не сообщайте данные карты. Звонок «от банка» с просьбой назвать пин-код и реквизиты, чтобы якобы разблокировать карту, — сигнал повесить трубку и позвонить на подлинную горячую линию банка.

Предлагают быстрое обогащение

Если подростку не хватает карманных денег на модный телефон и терпения, чтобы на него накопить, мошенники с радостью ему "помогут". Они размещают в интернете множество **объявлений о быстром и легком заработке.** Но зачастую в таких случаях внезапно разбогатеть удается только самим махинаторам.

Мошенники могут убедить подростка вложить деньги в "сверхприбыльный проект" (спойлер — в финансовую пирамиду). До выплат вкладчикам дело обычно не доходит. Собрав деньги как можно большего числа людей, организаторы исчезают.

Порой обманщики предлагают "быстро заработать", просто зарегистрировавшись на сомнительном сайте. Надо только выполнять задания или делать букмекерские ставки. Для вывода "заработка" они **просят оплатить комиссию.** В итоге деньги вместе с данными карты оказываются в руках махинаторов.

"Мой одноклассник однажды нарвался на мошенников. Он упрашивал родителей купить ему новый айфон, но его мама сказала, что слишком дорого, максимум прошлогодний купят. И то, если хорошо четверть закончит. Короче он стал искать, где купить новый, но дешевле, и нашел интересное объявление. Типа можно быстро заработать на новый айфон…"

Будьте бдительны, не наступайте на чужие грабли!

Обещания молниеносной прибыли — это всегда тревожный знак. Если подросток хочет купить дорогую вещь, обсудите с ним, как достичь этой цели. Иногда ребенок может сам накопить необходимую сумму полностью или хотя бы ее часть. Быстрее достичь намеченного поможет финансовый план, его можно составить самостоятельно или вместе с родителями. Если копить придется долго, то лучше положить деньги на банковский вклад под процент.

Завлекают "выигрышами" в конкурсах

Нередко мошенники рассылают письма и сообщения, в которых обещают нежданный выигрыш, или от имени популярных блогеров запускают рекламу "беспроигрышных лотерей". Но затем за доставку "приза" или какие-то другие дополнительные услуги просят оплатить небольшую комиссию. Для этого надо **пройти по ссылке и**

ввести данные банковской карты. Но на самом деле ссылка ведет на фишинговый сайт, и вместо призов доверчивый пользователь получает убытки.

"Участвовала в конкурсе в соц.сети Instagram около месяца назад, где призом была любая вещь, которую я выберу, размещенная на странице. Я выбрала кроссовки, написала организаторам, после чего мне предложили оплатить доставку…"

Будьте бдительны, не наступайте на чужие грабли!

Если организаторы конкурса **просят что-либо оплатить, это повод насторожиться.** Прежде чем пытать удачу в онлайн-розыгрышах, надо убедиться, что организаторы — не мошенники: почитать отзывы в интернете, новости (вдруг они уже замечены в скандалах). Стоит проверить на официальной странице блогера, действительно ли он рекламирует этот конкурс, или он тоже стал жертвой мошенников.

Просят о помощи от имени друзей в соцсетях

Киберпреступники взламывают аккаунты в соцсетях, а затем от чужого имени **рассылают сообщения по списку друзей.** Начинают разговор с банального "как дела?" и практически сразу переходят к жалобам на жизнь и просят в долг. Или со словами "лови фотки с дня рождения!" **вместо ссылки на фотографии присылают вредоносный вирус**. Он крадет с гаджета персональные данные, логины и пароли от личных кабинетов, в том числе от банковских.Могут быть и более сложные махинации.

"Мне во ВКонтакте написала давняя знакомая. Сказала, что потеряла мой номер и попросила его напомнить. Я напомнила. И тут она попросила выручить ее: она что-то покупала, и продавец должен был скинуть ей код подтверждения…"

Будьте бдительны, не наступайте на чужие грабли!

Прежде чем выполнять все, о чем просит "приятель", лучше **перезвонить ему и уточнить, действительно ли нужна помощь.** Скорее всего, он не в курсе переписки. Но чем раньше он узнает о случившемся, тем быстрее предупредит остальных, что его аккаунт взломали.

Защититься от вредоносных ссылок помогут **антивирусы, которые можно установить на всех гаджетах.** Для безопасности маленьких детей также можно настроить программы родительского контроля.

Набиваются в друзья на тематических форумах

Мошенники часто скрываются под маской интересных собеседников на форумах и в группах в соцсетях. Они **заводят с подростком виртуальную дружбу** на почве общих интересов и втираются в доверие ради будущей выгоды. Когда контакт налаживается, они выдумывают различные предлоги, чтобы получить необходимую им информацию. Например, мошенники просят ребенка прислать фотографии банковских карт или паспортов родителей. Этих данных может оказаться достаточно, чтобы украсть деньги со счета или оформить кредит на чужое имя.

"Недавно мне позвонили из банка. Сотрудница сообщила, что по карте идут подозрительные списания и они заблокировали карту. Я сказала, что ничего не оплачивала, изучу смски и перезвоню им. Залезла в сообщения и ужаснулась: оказалось, что последние полчаса мне приходили какие-то сообщения с кодами, а потом снимались деньги…"

Будьте бдительны, не наступайте на чужие грабли!

Чтобы обезопасить ребенка, нужно как можно раньше обсудить с ним **правила разумного финансового поведения**. Если он жить не может без гаджетов, то разобраться в теме финансов ему также помогут специальные мобильные приложения, а для любителей почитать есть подходящие подборки книг про деньги и экономику.

Подключите **СМС или push-оповещения ко всем банковским картам**, так вы сразу заметите подозрительные покупки.

Не стоит переводить на карту ребенка крупные суммы. Кроме того, можно ограничить суммы списаний или количество операций по карте в день, чтобы мошенникам не удалось украсть с нее все деньги разом.

Цитаты персонажей взяты из фильма "Приключения Буратино" (киностудия "Беларусьфильм", 1975 год).

https://fincult.info/

Адрес на сайте «Детки!» detkityumen.ru/biblio/category135/category150/4867/