**Мошенничество**

В сети существует огромное количество мошеннических схем, рассчитанных именно на детей. Преступники полагаются на доверчивость, любопытство, некритичность и невнимательность школьников.

Конечная цель мошенников, как правило, деньги, которые списываются с банковских карт, телефонных счетов, электронных кошельков. В некоторых случаях целью могут быть личные данные пользователей.

## **Как распознать угрозу?**

* Дети часто получают фишинговые письма якобы от известных компаний. Ребёнок читает это письмо, переходит по ссылке или вводит какие-то данные в форму обратной связи. И открывает преступникам доступ к паролям и номерам банковских карт.
* Или ребёнок видит баннер со ссылкой типа: «Узнай, кто заходил к тебе на страницу». Переходит по ней и попадает на сторонний сайт, где мошенники просят указать свой телефон. Затем присылают на этот номер ссылку и списывают с телефонного счёта деньги
* Вообще, любое сообщение, в котором есть просьба пройти по ссылке должно насторожить. Даже если оно пришло от знакомого. Часто мошенники взламывают аккаунт и от лица друзей рассылают спам или просят деньги.
* Иногда подросток находит какую-то лёгкую работу в интернете. Он выполняет её, но когда сумма на счёте становится достаточной для вывода, кошелёк блокируется. Чтобы разблокировать его, мошенники требуют оплату.
* Часто дети сами тратят родительские деньги. Они легко верят, что выиграли какой-то крупный приз. А мошенники просят их оплатить сущую мелочь — доставку или налог.
* Если аккаунт ребёнка привязан к вашей банковской карте, то можно ждать самых странных покупок. Дети легко выкидывают тысячи на прокачку аккаунтов в онлайн-играх. Устанавливают огромное количество платных приложений и игр.

## **Как предупредить угрозу?**

Расскажите ребёнку об основах безопасного сетевого общения:

* Важно критически относиться к любой информации в сети, не кликать на подозрительные баннеры, не переходить по неочевидным ссылкам, не вводить персональные данные на непонятных сайтах.
* Следить за приватностью и безопасностью. Не оставлять личные данные в соцсетях и мессенджерах, закрыть свой профиль от незнакомцев. Придумывать сложные и индивидуальные пароли.
* Скачивать только легальные программы на официальных сайтах. Установить надёжный антивирус и регулярно обновлять программное обеспечение на своих гаджетах.

## **Как понять, что ребёнок стал жертвой?**

Самое очевидное — пропажа денег со счёта. Даже исчезновение десяти рублей, которую редко кто замечает, может быть началом атаки кибермошенников на ваш кошелёк.

* У ребёнка меняется поведение: он выглядит озабоченным и грустным, уходит от разговора, прячет глаза, делает всё, чтобы бы вы не узнали баланс веб-кошелька или мобильного телефона.
* Если с аккаунта ребёнка рассылается спам или просьбы перевести деньги, то, скорее всего, его профиль украли. Оповестите об этом его виртуальных друзей, чтобы они случайно не перевели деньги мошенникам.

## **Что теперь делать?**

Как только вы узнали о мошенничестве — обратитесь в свой банк. Действовать нужно оперативно. Напишите заявление об отмене перевода и запросите выписку по транзакциям.

* Если ребёнок куда-то вводил данные карты, то нужно заблокировать её как можно скорее, иначе ваши средства могут быть украдены.
* Сообщите администрации сайта, если аккаунт ребёнка взломали. Важно вовремя заблокировать мошеннические рассылки. Смените пароли на связанных ресурсах.

Не стоит сильно ругать ребёнка, даже если он сам по