Ловушки виртуального мира.

**«Легкий заработок»**

Незнакомец связывается с ребенком в любом из мессенджеров и предлагает **заработать путем просмотра видеороликов** известных блогеров. Далее злоумышленник оправляет ссылку и просит ввести банковские данные одного из родителей, а также код из смс-уведомления, пояснив, что в дальнейшем по этим реквизитам будет переводить деньги.

**«Дополнения для онлайн-ирг»**

Мошенники заманивают несовершеннолетних пользователей онлайн-игр **низкими ценами и «уникальными акциями» на различные девайсы** для своего виртуального мира, чтобы быть наравне с лидирующими игроками. Для покупки усовершенствующих дополнений отправляют ссылку, перейдя по которой просят ввести данные банковской карты.

**«SMS от друга»**

Киберпреступники **взламывают аккаунт друга в соцсетях**, а затем **от его имени присылают сообщение**. **Начинают разговор с банального «Как дела?»** и практически сразу переходят к просьбе о помощи и просят в долг. Или со словами **«Лови фотки со дня рождения!»** вместо ссылки на фотографии присылают вредоносный вирус, который крадет с гаджета персональные данные, логины и пароли.

**«Выигрыш в конкурсе»**

Аферисты рассылают сообщения в социальных сетях или отмечают в комментариях под постом с розыгрышем, где сообщают о **неожиданном выигрыше**. Но затем за доставку «приза» или какие-то другие дополнительные услуги школьника просят **оплатить небольшую комиссию**.

**Важно!**

- не переходите по неизвестным ссылкам и не сообщайте незнакомцам данные банковских карт и коды подтверждения смс-сообщений;

- прежде, чем выполнить все, о чем просит «приятель» в соцсетях, позвоните ему и уточните, действительно ли нужна помощь;

- когда для получения приза организаторы конкурса просят что-либо оплатить, это повод насторожиться. Убедитесь, что это не мошенники: почитайте отзывы в Интернете, новости (вдруг они уже были замечены в обмане);

- если у ребенка имеется собственная банковская карта, то не стоит переводить на нее огромные деньги. Кроме того, ограничить суммы списаний или количество операций по карте в день, чтобы мошенникам не удалось украсть с нее все сбережения разом;

- подключите смс и push-оповещения ко всем банковским картам, так вы сразу заметите подозрительные покупки.

*Информация предоставлена*

*ГУ МВД России по Новосибирской области*