Как мошенники обманывают подростков в Интернете?

Наиболее распространенными видами мошенничества в сети Интернет в отношении подростков являются:

1. Использование фишинговых сайтов для оплаты покупок в онлайн-играх. На таких сайтах, имитирующих страницы онлайн-игр, за небольшие деньги предлагается приобрести игровую валюту, персонажей или предметы для получения дополнительного преимущества в игре. После ввода данных банковской карты для оформления желанной покупки подросток может потерять все имеющиеся на ней денежные средства, так как мошенники получают доступ к его банковскому счету.

2. Размещение объявлений о быстром и легком заработке. Злоумышленники приглашают подростков выполнить простые онлайн-задания за вознаграждение, после чего просят подтвердить, что они являются реальными людьми. Как правило, для этого требуется оплатить небольшой взнос. После совершения такой операции мошенники присваивают денежные средства себе и перестают выходить на связь, а подросток не получает обещанное вознаграждение.

3. Организация «инвестиционных онлайн-игр». При помощи яркой рекламы в социальных сетях кибермошенники привлекают молодежь к участию в «выгодном инвестиционном проекте», просят внести «регистрационный взнос» и пригласить друзей, чтобы заработать больше. Однако через определенное время сайт «инвестиционного проекта» перестает работать. В итоге подростки теряют не только возможность получить гарантированный мошенниками сверхдоход, но и ранее внесенные собственные денежные средства.

4. Передача вредоносных программ и вирусов. Злоумышленники под видом фотографии или видео направляют ссылку, содержащую вредоносную программу. Источниками вирусов также могут являться нелицензионные версии загруженных из сети игр и программ. Такие вредоносные программы могут следить за действиями человека в Интернете, в том числе запоминать логины и пароли от социальных сетей, личных кабинетов на сайтах банков и портале государственных услуг. В результате подросток, не осознавая возможных последствий, может потерять доступ к своим аккаунтам, которые будут использоваться мошенниками для хищения его денежных средств и обмана других людей.

5. Сообщения о «выигрышах» в конкурсах. Подростки получают их с аккаунтов мошенников, которые выдают себя за популярных блогеров, с предложением получить подарок за активные действия в социальных сетях. Однако за его доставку, как правило, необходимо заплатить. В результате ребенок не получает обещанный приз и теряет денежные средства.

6. Мнимая дружба 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.

Чтобы подросток не стал жертвой мошенников, ему необходимо рассказать о следующих правилах кибербезопасности:

1. Не публиковать в социальных сетях свои персональные данные (ФИО, пароли от личных кабинетов, аккаунтов, ПИН-коды и CVV-коды банковских карт), фотографии паспорта, банковских карт, иных документов.

2. Не переходить по сомнительным ссылкам, содержащимся в сообщениях и электронных письмах.

3. Проверять безопасность сайта для оплаты товаров, услуг или перевода денежных средств, степень его защиты (безопасный адрес начинается с букв https://, значок замка в адресной строке).

4. Остерегаться сообщений о выгодных покупках, беспроигрышных лотереях и других возможностях быстрого заработка.

5. Не переводить денежные средства, если имеются сомнения в личности получателя.

6. Относиться критически к просьбам знакомых и друзей в сети Интернет, помнить, что их аккаунты могут быть взломаны. 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

7. Не сообщать свои персональные данные посторонним, а при возникновении сомнений незамедлительно обращаться к родителям.

Советы родителям по защите детей от мошенничеств в сети Интернет:

- Установите на телефон ребенка или иное устройство антивирусные программы и регулярно обновлять их. Дополнительной мерой обеспечения безопасности может служить функция родительского контроля на телефоне и компьютере. Она будет автоматически блокировать переходы на подозрительные и потенциально опасные сайты.

- 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.

ОБК УМВД России по Липецкой области