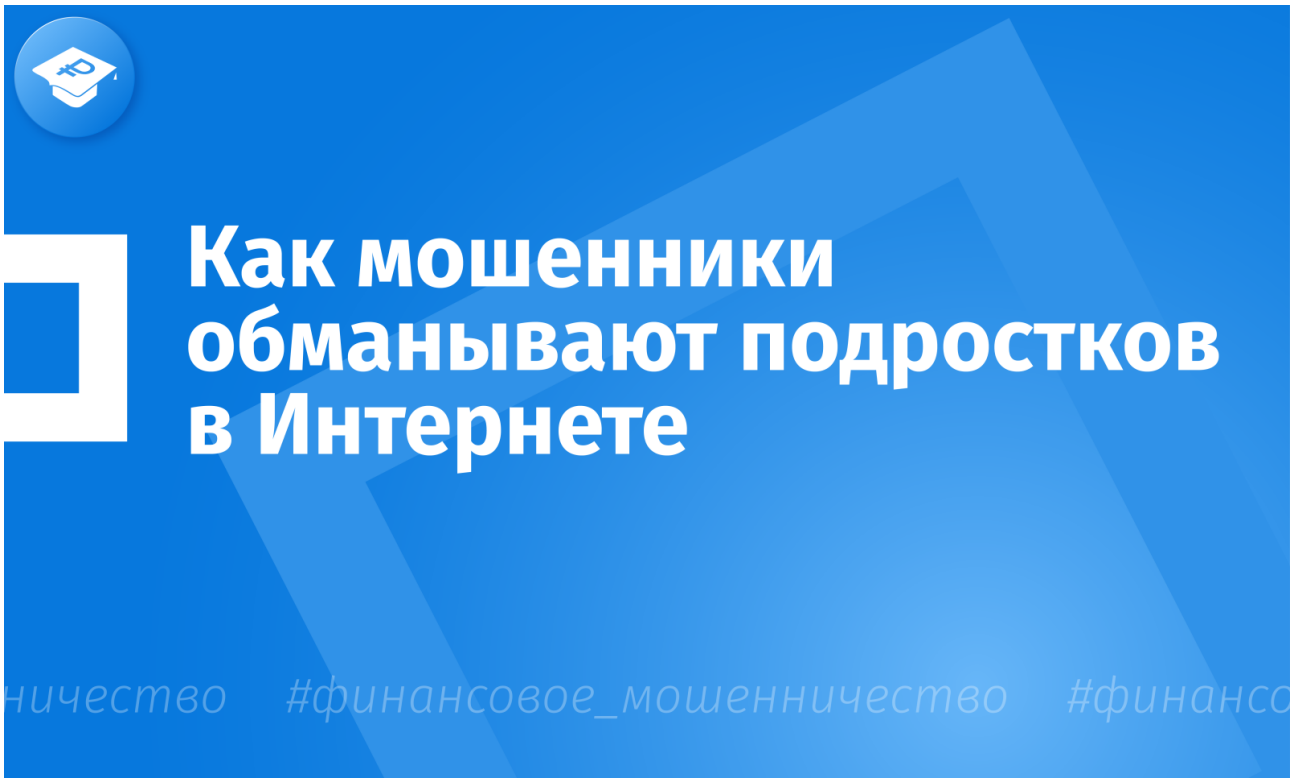
7 МАРТА, ЧЕТВЕРГ

Открытый бюджет города Москвы

Распространенные виды мошенничества в сети Интернет в отношении подростков



Как мошенники обманывают подростков в Интернете

В современном мире дети и подростки рано получают возможность распоряжаться карманными деньгами. Мошенники пользуются недостаточным уровнем финансовых знаний молодых людей, их стремлением к самореализации и желанием заработать свои первые денежные средства.

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

- **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;
- **Размещение объявлений о быстром и легком заработке.** Злоумышленники

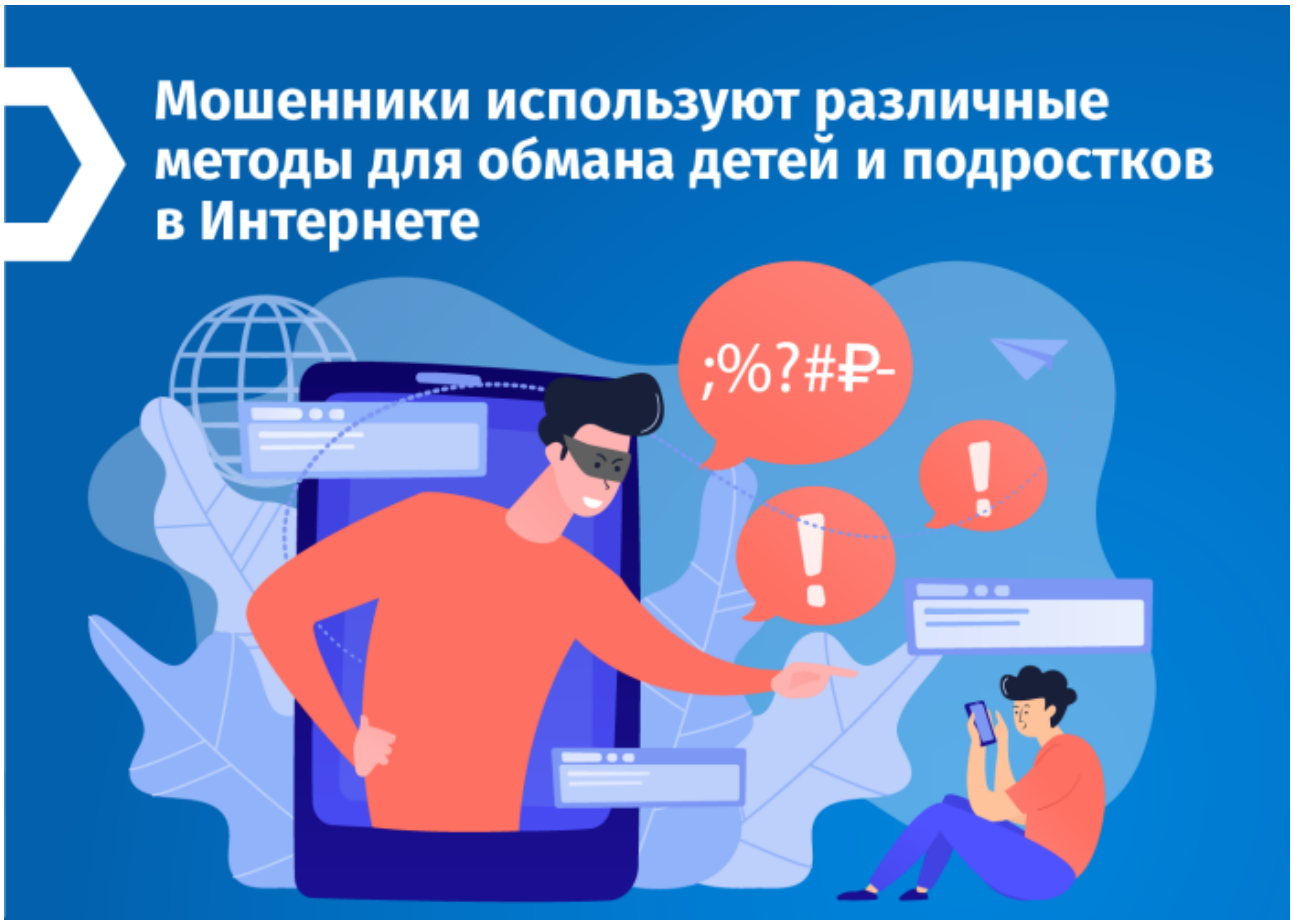
приглашают подростков выполнить простые онлайн-задания за вознаграждение, после чего просят подтвердить, что они являются реальными людьми. Как правило, для этого требуется оплатить небольшой взнос. После совершения такой операции мошенники присваивают денежные средства себе и перестают выходить на связь,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

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

- 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;
- Не переходить по сомнительным ссылкам, содержащимся в сообщениях и электронных письмах;
- 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);
- Остерегаться сообщений о выгодных покупках, беспроигрышных лотереях и других возможностях быстрого заработка;
- Не переводить денежные средства, если имеются сомнения в личности получателя;
- Относиться критически к просьбам знакомых в сети Интернет, помнить, что их аккаунты могут быть взломаны;
- Не сообщать свои персональные данные посторонним, а при возникновении сомнений незамедлительно обращаться к родителям.

Для защиты ребенка от мошенников следует установить на его телефон 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.



По материалам портала Правительства Москвы "Открытый бюджет города Москвы": https://budget.mos.ru/