

***Прокуратура Северного района г. Орла разъясняет:***

*Основные виды мошенничества   
с использованием Интернета:*

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.

*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 в сети Интернет, помнить,   
что их аккаунты могут быть взломаны.

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

Для защиты ребенка от мошенников **родителям 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.

Необходимо внимательно следить   
за актуальностью номера, к которому привязан аккаунт. От этого зависит безопасность персональных данных.

Используйте дополнительные инструменты защиты. Установите контрольный вопрос, который будут задавать при попытке восстановления аккаунта. Подпишитесь   
на уведомления о входе в аккаунт на электронную почту.

*Разъясняет помощник прокурора  
Т.А. Коптева*

**г. Орёл, 2025**