*Статья 1.*

**Прокуратура Кяхтинского района разъясняет: как не стать жертвой киберпреступников?**

С каждым годом преступления в цифровом пространстве становятся все более изощренными. Из года в год ущерб от кибермошенничеств в России увеличивается. Прокуратура района призывает граждан проявлять бдительность и соблюдать простые, но эффективные правила безопасности.

Почему это важно?

Каждый третий россиянин хотя бы раз сталкивался с попыткой мошенничества в интернете. Жертвами становятся не только пенсионеры, но и технически подкованная молодежь. Преступники используют психологические уловки и технические ухищрения, чтобы обмануть даже осторожных пользователей.

Самые опасные схемы обмана.

1. *«Это сотрудник банка/оператора связи/полиции».*

Мошенники звонят или пишут, представляясь сотрудниками банка, полиции, сотового оператора, и требуют срочно перевести деньги «на безопасный счет». Ни один настоящий банк не просит клиентов переводить средства по телефону!

1. *«Это ты на фото/видео?»*

С использованием вредоносных программ мошенники получают доступ к вашему телефону и снимают денежные средства. Не открывайте сомнительные ссылки!

*3. «Вы выиграли приз»*

Вам приходит сообщение о крупном выигрыше, но для его получения нужно «оплатить комиссию». Это 100% обман.

*4. «Мама, срочно нужны деньги»*

Злоумышленники взламывают социальные сети и мессенджеры и просят у друзей или родственников «в долг». Всегда перезванивайте близким, чтобы проверить информацию!

Как защитить себя?

1. Никому не сообщайте:

- пароли, PIN-коды и CVC карты;

- коды из SMS (их запрашивают только мошенники);

- паспортные данные по телефону или в мессенджерах;

2. Проверяйте ссылки – официальные сайты банков и госорганов имеют домены .ru или .рф, а адрес начинается с https://.

3. Не подключайтесь к публичному Wi-Fi при оплате покупок или входе в интернет-банк.

4. Не разговаривайте с неизвестными абонентами!

Что делать, если вас обманули?

1. Немедленно позвоните в банк и заблокируйте карту.

2. Подайте заявление в полицию – чем быстрее, тем выше шансы сохранить деньги.

3. Сохраните все доказательства: скрины переписки, номера телефонов, чеки переводов.

*Помните: ваша безопасность – в ваших руках! Не дайте мошенникам заработать на вашей доверчивости. Делитесь этой информацией с родными – особенно с пожилыми людьми, которые чаще всего становятся жертвами.*