

Прокуратура Куйтунского района разъясняет «Профилактика мошенничества в сети «Интернет»

За 11 месяцев 2025 года на территории Иркутской области зафиксировано хищение денежных средств путем дистанционного мошенничества на сумму более 2 млрд. рубл.

Что делать, если Вам написал или позвонил мошенник:

- Прерывать телефонный звонок.
- Никогда не сообщать никаких кодов по телефону.
- Не соглашаться устанавливать приложения, программы на телефоны, компьютеры и другие гаджеты.
- Не переходить по неизвестным ссылкам по просьбе мошенников.
- Не отправлять денежные средства неизвестному человеку.
- Не раскрывать личную информацию о себе.

К личной информации относятся: паспортные данные, пароли, пин-коды, данные банковских карт.

- Проверять отправителей письма или сообщения.
- Не открывать вложения из писем от незнакомцев.
- Не доверять сообщениям о выигрыше в лотерею или розыгрыше.
- Если Вам позвонили якобы из службы безопасности банка и сообщают о подозрительных операциях, необходимо незамедлительно прервать разговор и перезвонить в банк самостоятельно по официальному номеру телефона. Указанному на сайте банка или Вашей банковской карте.
- Не отвечайте на звонки с неизвестных номеров. Часто мошенники используют подмену номера, чтобы выглядеть как официальная организация.
- Внимательно проверяйте адреса сайтов в сети «Интернет».

Перед вводом личных данных убедитесь, что сайт использует защищенное соединение (адрес начинается с <https://>). Обратите внимание на орфографические ошибки и неточности в названии сайта.

- Мошенники часто обещают быстрые и легкие деньги, но взамен просят предоставить личные данные или внести предоплату. Помните, что бесплатный сыр бывает только в мышеловке.

Принятие мер безопасности:

- Для учетных записей в Госуслугах, электронной почте и других приложениях использовать сложные пароли.
- Включите двухфакторную аутентификацию для всех важных аккаунтов. Это добавит дополнительный уровень защиты при входе в систему.
- Будьте внимательны к публичным Wi-Fi сетям:
Избегайте ввода личной информации (например, банковских реквизитов) при использовании общественных сетей Wi-Fi. Эти сети могут быть небезопасными.
- Регулярно делайте резервные копии данных:
Хранение важной информации в облачных сервисах или на внешних носителях поможет предотвратить потерю данных в случае взлома.
- Обновляйте операционные системы и приложения:
Устаревшие версии программного обеспечения могут содержать уязвимости, которыми могут воспользоваться злоумышленники. Регулярные обновления помогут закрыть эти дыры.
- Обращайтесь за помощью при необходимости:
Если у вас возникли подозрения относительно безопасности ваших данных, свяжитесь со службой поддержки вашего провайдера услуг или банком.

- Установить надёжное антивирусное ПО на все устройства (компьютеры, смартфоны) и регулярно обновлять его базы. Программы блокируют фишинговые сайты и вредоносные файлы в письмах.
- Защитить персональные данные в соцсетях настройками приватности, не делиться личной информацией в публичных чатах.