ОСНОВНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ДЕТЕЙ в СЕТИ «Интертнет»

- Сайты, разжигающие национальную рознь и расовое неприятие
- Депрессивные молодежные течения
- Пропаганда наркотиков
- Сайты знакомств
- Секты
- Контентные риски
- Электронная безопасность
- Вредоносные программы
- Спам
- Кибермошенничество
- Киберпреследование

ПРАВИЛА

Рассказывай родителям если у тебя есть страхи, связанные с Интернетом. Помни, что информация не всегда бывает полезной и достоверной. Всегда сообщай взрослым, если что-то вызывает неприязнь и дискомфорт

Если при общении в Интернете тебе угрожают или пишут что-то неприятное, ничего не отвечай и расскажи об этом родителям

Если незнакомый человек, с которыми ты познакомился в Интернете, приглашает, настаивает на встрече с тобой, сообщи родителям. Назначай встречу в общественном месте и в присутствии взрослых.

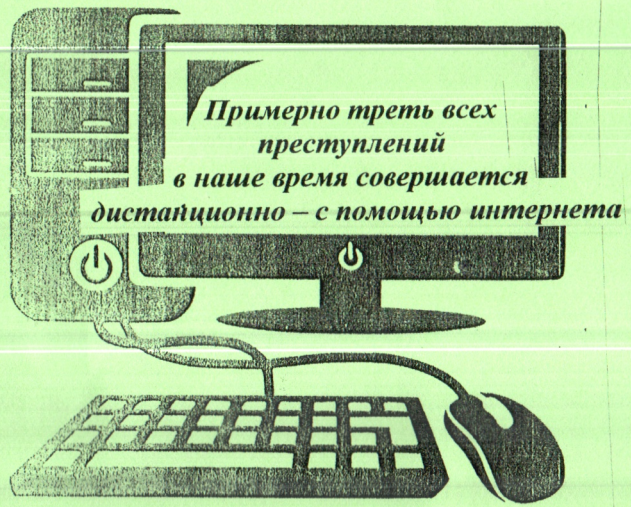
ИНФОРМАЦИЯ, КОТОРУЮ НЕ СЛЕДУЕТ РАЗМЕЩАТЬ НА СТРАНИЦАХ СОЦИАЛЬНЫХ СЕТЕЙ

- О своём местоположении
- О планах на длительные поездки
- Фото дорогих вещей и подарков
- Фото квартиры или дома
- Свой домашний адрес
- Электронную почту, номера телефонов
- Фото личных документов
- Личный пароль

ПРОКУРАТУРА ДЕМИДОВСКОГО РАЙОНА

ОСНОВНЫЕ ПРАВИЛА ИНТЕРНЕТ БЕЗОПАСНОСТИ

ПАМЯТКА



Демидов
2024

ОСТОРОЖНО!
МОЩЕННИЧЕСКИЕ СХЕМЫ

Схема 1. Ваш номер нужно подтвердить

Обман, который чаще всего срабатывает. Идет звонок якобы от оператора сотовой связи. Мошенники пугают, что действующий договор на оказание услуг связи заканчивается и его необходимо продлить, иначе номер передадут другому абоненту. Идти никуда не нужно, все можно сделать по телефону, уверяет собеседник. Достаточно продиктовать код из смс. Цель одна - получить доступ к аккаунту человека на Госуслугах.

Схема 2. Предложение от лжеброкеров

Аферисты предлагают вам выгодно вложить свои средства, обещая процент гораздо выше, чем у банков. Откажитесь от услуг компании или её представителей, если они просят перевести деньги за услуги на карту физического лица либо через электронный кошелек.

Схема 3. Вам предлагают выгодную работу

Аферисты размещают лжевакансии на популярных сайтах объявлений. Пройти собеседование с работодателям мошенники предлагают сделать онлайн по видеозвонку, где просят кандидата заполнить анкету прямо во время зума. Один из её пунктов – номер карты и другие финансовые данные. Такая информация им нужна якобы для перечисления зарплаты в будущем. Вместо пополнения с банковской карты соискателя в будущем происходит списание, а ни о какой работе речи не идет.

Находясь в поиске работы, можно не только потерять деньги, но и нарушить закон, став дроппером.

Схема 4. Друг просит о помощи

Тактика кибермошенников - рассылка сообщений с просьбой одолжить денег близким иди друзьям. Мошенники играют на чувствах человека и сообщают, что его родственник попал в беду. Аферисты взламывают аккаунт пользователя. Скачивают голосовые сообщения и на их основе генерируют монолог для дальнейшего обмана.

Существует и другой сценарий - просьба проголосовать за детей в конкурсе. За ссылкой для голосования, которую мошенники отправляют со взломанного аккаунта владельца, скрыт вирус, который откроет им доступ к вашему гаджету.

Схема 5. Оплата услуг по фейковому QR-коду

Такой QR-код ведет не на официальный сайт сервиса, а на поддельный ресурс, через который аферисты крадут деньги и данные карты.

Чтобы не потерять деньги, оплачивайте услугу только через официальное приложение сервиса, а не через камеру гаджета.

Схема 6. Звонки из банка

- Мошенники звонят с лживыми угрозами об оформлении кредита на имя владельца банковской карты другим человеком или подозрительной операции по ней.
- Мошенники под видом специалистов техподдержки банков предлагают установить на смартфон приложение для поиска вирусов. Это вредоносное программное обеспечение, которое дает доступ к телефону жертвы и его данным.
- Аферисты предлагают помощь в сохранении денежных средств. Под видом сотрудников Банка сообщают человеку, что кто-то пытается похитить деньги со счета. Чтобы их спасти, надо перевести средства на «безопасный» счет в ЦБ РФ. По легенде это временная мера- на период поиска преступников. А потом всю сумму человеку якобы возместят наличными в Банке.

Пользуйтесь только официальными ресурсами финансовых организаций.

Схема 7. Представляются госслужащими

Мошенники звонят или пишут человеку якобы от лица следователя, сотрудника прокуратуры, ФСБ, налоговой, портала «Госуслуги».

Самая распространенная уловка-предложение получить какую-либо госвыплату, или с угрозой блокировки счета оплатить штраф.

Не верить этим звонкам!