

КИБЕРГИГИЕНА В СОЦ. СЕТЯХ



ЦИФРОВАЯ
РОССИЯ

Что такое кибермошенничество?



Кибермошенничество — это обман, который происходит в интернете.



Мошенники используют разные хитрости и уловки, чтобы украсть деньги или личные данные у людей.



Их цель - чтобы ты ввёл свои данные или заплатил им деньги



Важно быть осторожным и не доверять тому, что кажется слишком хорошим, чтобы быть правдой!



Сколько денег потеряли россияне в 2024 году?

□ **200 млрд**

больше, чем в 2024 г.

на **36%**



*Можно купить **200,000** автомобилей. Представьте, сколько машин это будет — можно заполнить целый город!*



*Можно купить **40,000** квартир. Это как целый район с десятками зданий, где люди живут.*



*Можно отправить **4,000** человек в путешествие на неделю. Это будет незабываемое приключение для многих подростков!*



*Можно купить **6,666,667** приставок. Это значит, что почти все друзья в городе могут играть вместе в новом формате!*



СОЦИАЛЬНЫЕ СЕТИ



Фальшивые аккаунты



Сценарий: Мошенники создают фальшивые профили, выдавая себя за популярных людей или друзей.

Как это работает:



запрос на дружбу или сообщение от фальшивого аккаунта, который выглядит как аккаунт знаменитости или знакомого.

Они могут предложить «приз» или «эксклюзивный контент», прося при этом личные данные или деньги.



Урок:

Всегда проверяйте истинность аккаунтов, особенно если они просят о деньгах или личной информации.



Мошенничество с выигрышами



Сценарий:

Пользователь получает сообщение о том, что он выиграл конкурс или приз.



Как это работает:

сообщают, что ты выиграл смартфон, подарочную карту или косметику, но для получения приза требуется заполнить форму с личными данными или внести небольшую плату.



Урок:

Будьте осторожны с предложениями о «выигрышах», особенно если они требуют личных данных или платежей для получения подарков.



Лайк -ловушка



Сценарий:

Пользователь получает сообщение о том, что он может заработать XX тысяч рублей, делая простую работу. Зарабатывайте на лайках! Всего 2 часа в день — и вы получите 5000 рублей»



Как это работает:

Вам предлагают простую работу, не требующую особых усилий. Могут для убедительности создать фейковые сайты популярных соцсетей, копирующие популярные оригиналы. После того как человек соглашается, ему советуют установить для работы специальное мобильное приложение и внести незначительную сумму (обычно от 100 до 1000 рублей) для активации аккаунта.



Урок:

Будьте осторожны с предложениями о легкой работе, вы собственноручно переводите мошенникам не только деньги, он даете им доступ к персональным данным. Так как под видом «приложение для работы» распространяется вредоносное ПО

Звонки и сообщения от государственных ведомств



Сценарий:

Вы получаете сообщение или звонок якобы от лица сотрудников ФСБ, МВД, Росфинмониторинга, ФНС, Социального фонда России, портала «Госуслуги» и прочих.

Как это работает:

Самая распространенная уловка – предложение получить какую-либо государственную выплату. Схема классическая: вы нам данные карты, мы вам – деньги.

Схема не одна, их очень много!!!

Урок:

Будьте осторожны и знайте, что ни один сотрудник государственных ведомств не будет вам ни звонить, ни писать! Не ведите никаких переговоров, а сразу обратитесь к родителям ил по телефону 112



Взлом аккаунта



Сценарий:

вы получаете угрозы публикацией личных данных или компрометирующей информации, если не заплатите ХХ сумму. Также мошенники могут просто похитить аккаунт под свои цели, и рассылать вашим знакомым и друзьям информацию (конкурс в школе-голосование, помощь, оплата по QR кодам и пр.



Как это работает:

Вы переходите по фишинговому сайту и вбиваете свои логин и пароль, при голосовании у вас снова просят логин и пароль (только при наличии 2х факторной идентификации), тем самым вы передаете все доступы к вашим сетям



Урок:

Не переходите и не вбивайте свои логин/пароль на непроверенном сайте, всегда используйте 2х факторную идентификацию (минимум 2 пароля/отпечаток пальца)





Мыслите критически

Проверяйте информацию

Не доверяйте в сети

**НЕ ПОПАДАЕЙТЕСЬ НА
УЛОВКИ МОШЕННИКОВ**

