

Профилактика телефонного мошенничества



Избегайте телефонного мошенничества, следуя этим пяти советам

- 1 Не отвечайте на неизвестные номера
- 2 Будьте осторожны с заманчивыми и выгодными предложениями
- 3 Не передавайте конфиденциальную информацию
- 4 Проверьте наличие средств на банковском счете
- 5 Не нажимайте на ссылки в подозрительных сообщениях



1

Не отвечайте на неизвестные номера

Если вы не знаете, кто звонит, не отвечайте на звонок.



2

Не передавайте конфиденциальную информацию

Никогда не передавайте конфиденциальную информацию, такую как СНИЛС или номер кредитной карты, по телефону.



3

Не нажимайте на ссылки в подозрительных сообщениях

Не нажимайте на ссылки в подозрительных сообщениях или электронных письмах.



4

Будьте осторожны с заманчивыми и выгодными предложениями

Будьте осторожны с предложениями, которые кажутся слишком хорошими, чтобы быть правдой.



5

Проверьте наличие средств на банковском счете

Регулярно проверяйте свой счет, чтобы убедиться, что нет никаких подозрительных транзакций.



Следуя этим пяти советам, вы можете защитить себя от телефонного мошенничества!

**БУДЬТЕ БДИТЕЛЬНЫ!
НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!**



**Если вам поступают звонки
от службы безопасности банка,
различных правоохранительных органов
о необходимости перевода
денежных средств
на другие лицевые счета,
ЗНАЙТЕ - ЭТО МОШЕННИКИ!**



! СТОП ! МОШЕННИК !



ТЕЛЕФОННЫЕ МОШЕННИЧЕСТВА

МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ СОТОВОЙ СВЯЗИ СОВЕРШАЮТСЯ В ОСНОВНОМ, ПУТЕМ СООБЩЕНИЯ ГРАЖДАНАМ ЗАВЕДОМО ЛОЖНОЙ ИНФОРМАЦИИ:

Вам поступает звонок якобы сотрудника правоохранительных органов (ФСБ, СК, прокуратура, полиция). Звонящий сообщает, что вы стали жертвой мошенника и требует оказать помощь в их поимке, угрожая уголовной ответственностью за отказ или разглашение информации. Под страхом наказания запрещают говорить о случившемся даже родственникам и близким. Следующий звонок поступает уже от якобы сотрудника банка, он предлагает произвести операции для поимки мошенников: перечислить деньги на безопасный счет, оформить кредит, пока на вас его не оформили злоумышленники и др.

Вам сообщают, что кто-то из близких попал в ДТП, больницу, совершил преступление, и ему срочно нужны деньги, после чего просят передать их лично или куда-либо перевести.

Поступает звонок или СМС от якобы сотрудника службы безопасности банка. Вам сообщают о блокировке карт, аресте счетов, незаконном списании средств с вашей карты и т.п., после чего просят сообщить им реквизиты карты и ваши персональные данные.

Вы получаете СМС или звонящий сам сообщает, что вы стали обладателем приза или победителем конкурса, далее следует просьба перечислить ему деньги под благовидным предлогом, как гарантию того, что награда попадет именно к Вам.

ЧТО ДЕЛАТЬ, ЧТОБЫ УБЕРЕЧЬ СВОИ ДЕНЬГИ

Позвоните своему близкому человеку, в больницу, в органы внутренних дел проверьте информацию. Никогда не передавайте и не переводите деньги незнакомым людям. Не верьте в безопасный счет – это уловка

КИБЕРМОШЕННИЧЕСТВО

ВИРУСНОЕ ЗАРАЖЕНИЕ ПК ИЛИ СМАРТФОНА ДЛЯ ПОЛУЧЕНИЯ ДОСТУПА К ДАННЫМ СИСТЕМ ОНЛАЙН БАНКИНГА И ПОХИЩЕНИЯ ДЕНЕГ С ВАШЕГО СЧЕТА:

На Ваш смартфон или компьютер поступает сообщение, либо письмо с любой информацией, которая способна Вас заинтересовать, при этом в данном сообщении содержится ссылка, по которой необходимо перейти.

Вы сами устанавливаете на свой смартфон или компьютер не лицензионное программное обеспечение.

При этом не обращаете внимание, что предоставляете этой программе доступ к сети интернет, отправке СМС и т.д. Вы теряете свой мобильный телефон с подключенной услугой «Мобильный банк».

ЧТО ДЕЛАТЬ, ЧТОБЫ УБЕРЕЧЬ СВОИ ДЕНЬГИ

Не переходите по ссылкам и не устанавливайте приложения/обновления, пришедшие по СМС, ММС, электронной почте, мессенжерам, в том числе от имени банка

МОШЕННИЧЕСТВА В СЕТИ ИНТЕРНЕТ

МОШЕННИЧЕСТВА ПРИ ПОКУПКАХ ИЛИ ПРОДАЖАХ ЧЕРЕЗ СЕТЬ ИНТЕРНЕТ (ОНЛАЙН МАГАЗИНЫ, СОЦ. СЕТИ, РЕСУРСЫ ОБЪЯВЛЕНИЙ).

В сети широко распространена реклама биржевых площадок, обещающих крупные заработки от инвестиций в короткие сроки. Стоит зарегистрироваться и ввести данные, как вам сразу же позвонит лжеброкер и расскажет о том, как много вы можете заработать не выходя из дома. Причем заработок будет тем больше и быстрее, чем больше средств вы внесете на свой счет на торговой площадке. Как только вы перечислите средства на якобы ваш счет, вы их не сможете вернуть обратно. И виртуальные заработки на бирже так и останутся виртуальными

Мошенники создают сайты-клоны торговых площадок с отличной репутацией (копируют интерфейс оригинального сайта), с небольшим отличием в доменном имени сайта. Вы отдаете деньги мошенникам, думая что покупаете товар.

Мошенники создают собственные интернет-магазины, как правило с товарами по цене существенно ниже среднерыночной, либо с большими скидками.

Вы размещаете в сети интернет объявление о продаже какого-либо товара. Вам звонит мошенник и сообщает о своем намерении купить ваш товар, при этом просит сообщить данные вашей банковской карты для перевода на нее денежных средств.

ЧТО ДЕЛАТЬ, ЧТОБЫ УБЕРЕЧЬ СВОИ ДЕНЬГИ

Проверьте правильно ли Вы написали доменное имя сайта. Зайдите в раздел сайта, где размещены контактные данные сайта. Если указан лишь адрес электронной почты или телефон, воздержитесь от покупки. Никому не сообщайте данные своей банковской карты. Относитесь с осторожностью к предложениям получения прибыли в короткие сроки, таким предлогом пользуются аферисты, пытающиеся похитить деньги!