

## ТЕЛЕФОННЫЕ МОШЕННИЧЕСТВА

## КИБЕРМОШЕННИЧЕСТВО

## МОШЕННИЧЕСТВА В СЕТИ ИНТЕРНЕТ

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



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.

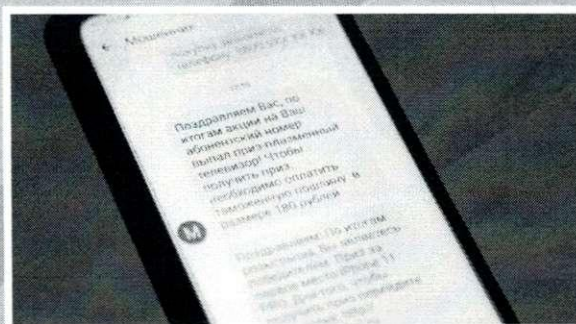
Вы получаете СМС или звонящий сам сообщает, что вы стали обладателем приза или победителем конкурса, далее следует просьба перечислить ему деньги под благовидным предлогом, как гарантию того, что награда попадет именно к Вам.

### ЧТО ДЕЛАТЬ, ЧТОБЫ УБЕРЕЧЬ СВОИ ДЕНЬГИ

Позвоните своему близкому человеку, в больницу, в органы внутренних дел и проверьте информацию

Никогда не передавайте и не переводите деньги незнакомым людям

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 нелицензионное 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

В случае потери мобильного телефона с подключенной услугой «Мобильный банк», следует срочно обратиться в контактный центр банка для блокировки услуги.

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



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. Проверьте дату регистрации сайта, если продавец работает недавно, лучше найти альтернативу.

Никому не сообщайте данные своей банковской карты.