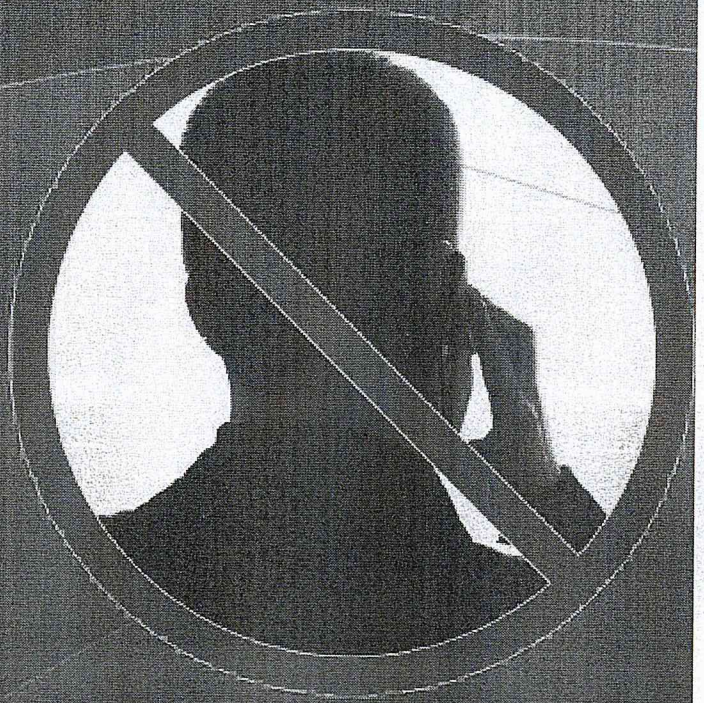
!СТОП!
МОШЕННИК!



Не дай себя обмануть!
Звоните в полицию
102 или 112 !

ГУ МВД России по Ростовской области

! Подумай, кому переводишь деньги

! Будь внимателен и бдителен

! Не дай себя обмануть

ЕФОННЫЕ МОШЕННИЧЕСТВА

ШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ
СТВ СОТОВОЙ СВЯЗИ СОВЕРШАЮТСЯ
ОСНОВНОМ, ПУТЕМ СООБЩЕНИЯ
РАЖДАНАМ ЗАВЕДОМО ЛОЖНОМ
ИНФОРМАЦИИ:

общают, что кто-то из близких попал в ДТП,
ицу, совершил преступление, и ему срочно
ны деньги, после чего просят передать их
лично или куда-либо перевести.

○

пает звонок или СМС от якобы сотрудника
жбы безопасности банка. Вам сообщают
окировке карт, аресте счетов, незаконном
ии средств с вашей карты и т.п., после чего
ят сообщить им реквизиты карты и ваши
персональные данные.

○

лучаете СМС или звонящий сам сообщает,
стали обладателем приза или победителем
са, далее следует просьба перечислить ему
под благовидным предлогом, как гарантию
го, что награда попадет именно к Вам.

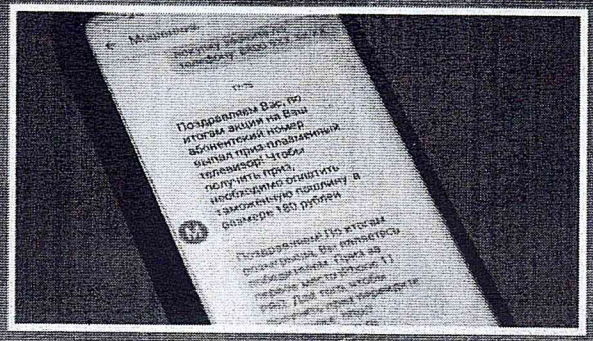
ЕЛАТЬ, ЧТОБЫ УБЕРЕЧЬ СВОИ ДЕНЬГИ

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

гда не передавайте и не переводите деньги
незнакомым людям

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 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 обратится в контактный центр банка для блокировки услуги.

МОШЕННИЧЕСТВА В СЕТИ ИНТЕРНЕТ

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.

ОСТОРОЖНО, МОШЕННИКИ!

Сотрудники полиции напоминают о том, как не стать жертвой мошенников.

В большинстве случаев мошенники звонят жертве на мобильный телефон и представляются «сотрудником службы безопасности банка». Звонящий сообщает о сомнительном переводе денежных средств с банковской карты либо о попытке несанкционированного снятия денежных средств. Преступник просит у вас полные данные карты, CVV- или CCV-код, код из СМС или пароли от системы Сбербанк Онлайн.

Чтобы не стать жертвой преступления необходимо соблюдать несколько правил:

- при поступлении подобных звонков ни в коем случае не сообщайте персональные данные неизвестным лицам, даже если они представляются сотрудниками службы безопасности банка;

- помните, что сотрудники банков никогда не совершают подобных звонков и не запрашивают ваши персональные данные;

-сотрудники банков не предлагают оформить кредит и разместить денежные средства на указанных ими счетах, якобы для получения выгодных дивидендов, дистанционно пытаясь узнать данные карты или личного кабинета, не отправляют в другой банк взять кредит наличными и перевести денежные средства на указанный ими счет.

- сразу завершайте разговор, обязательно перезвоните по официальному номеру банка и уточните нужные сведения сами. Помните, банк никогда не запрашивает подобным образом информацию.

- не совершайте никаких операций по инструкциям звонящего. Все операции для защиты карты сотрудник банка делает сам;

- пользуясь мобильным телефоном не переходите по ссылкам полученных в электронных письмах и СМС сообщениях с неизвестных адресов и телефонных номеров чтобы не скачать вредоносную программу.

Не верьте сообщениям о блокировании ваших карт и банковских счетов, иным уловкам приглашающим перейти по ссылкам. Помните это кибермошенники желающие получить ваши персональные данные с помощью вредоносных программ.

УМВД России по г.Шахты.