Мобильное мошенничество

Типичные ситуации:

Вам позвонили/прислали SMS с неизвестного номера с просьбой о помощи близкому человеку

- Не впадайте в панику, не торопитесь делать перевод
- Перезвоните родным и узнайте, все ли у них в порядке
- Уточните, где находится близкие, подключите услугу «Маячок»

Вам позвонили/прислали SMS «из банка» с неизвестного номера

- Не торопитесь следовать инструкциям и отвечать на запрос
- Не сообщайте персональные данные неизвестным лицам, даже если они представляются сотрудниками банка
- Проверьте информацию, позвонив в контактный центр банка

Ваш аккаунт в социальных сетях заблокирован. Для разблокировки вас просят отправить SMS на «короткий» номер

- Не торопитесь следовать инструкциям
- Обратитесь с запросом к администрации социальной сети и мобильному оператору
- Не доверяйте сомнительным источникам
- Не размещайте в социальных сетях конфиденциальную информацию

Вам прислали «Открытку» (MMS) с неизвестного номера

- Не открывайте вложенные файлы и не переходите по ссылкам
- Удалите сообщение с ссылкой
- Защитите свой телефон, подключите **БЕСПЛАТНУЮ** услугу «Стоп-контент»
- Используйте антивирусное программное обеспечение для телефонов только от официальных поставщиков

Как защитить себя и близких от мобильных мошенников:

Будьте бдительны
Узнавайте подробную информацию об актуальных схемах мошенничества в новостном разделе на портале stopfraud.megafon.ru или в средствах массовой информации.

Избегайте или сводите к минимуму передачу любой конфиденциальной информации
В последнее время участились случаи использования этой информации в мошеннических целях.

Не спешите действовать по инструкциям неизвестных людей
Убедитесь в достоверности информации, полученной с незнакомых номеров, через уполномоченные организации, родственников или знакомых.

Не переводите деньги на незнакомые номера

При использовании «коротких» номеров уточняйте у оператора стоимость предоставляемой услуги
Внимательно читайте условия предоставления услуг. Для проверки стоимости SMS воспользуйтесь БЕСПЛАТНЫМ сервисом «Мобильный прайс»: отправьте $ на «короткий» номер услуги. В ответном сообщении будет указана стоимость отправки SMS на данный номер и название контент-провайдера.

Не отдавайте телефон в руки незнакомцев
Предложите самостоятельно набрать нужный номер и передать информацию.

Помните, что «бесплатный сыр бывает только в мышеловке»
Не доверяйте неизвестным людям, которые обещают вам легкие выигрыши, быстрые исцеления и баснословные заработки.

ТЕЛЕФОННЫЕ МОШЕННИЧЕСТВА

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.

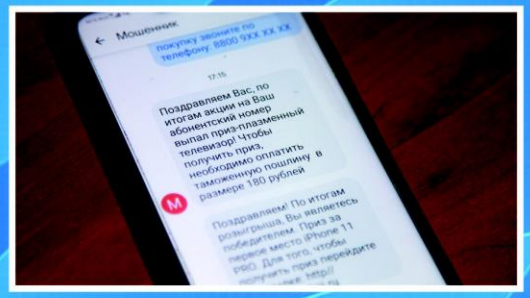
ЧТО ДЕЛАТЬ, ЧТОБЫ УБЕРЕЧЬ СВОИ ДЕНЬГИ

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

Никогда не передавайте и не переводите деньги незнакомым людям

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.

Проконсультироваться при возникшей проблеме или передать сообщение о возможных фактах посягательств можно по телефону или по адресу:

п. Зимовники ул. Ленина №114, тел. 8-863-76-3-13-62 Администрация Зимовниковского района;

п. Зимовники ул. Макарчука №64, тел. 8-863-76-3-25-02 отдел МВД России по Зимовниковскому району