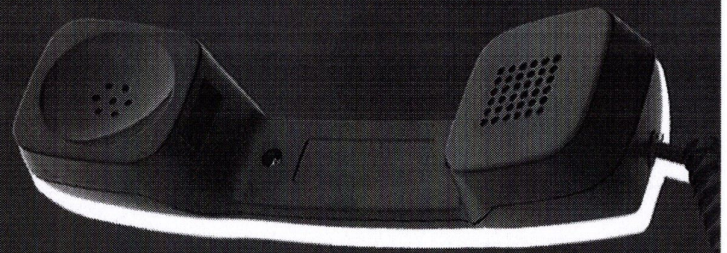
ВНИМАНИЕ!

IT-МОШЕННИКИ

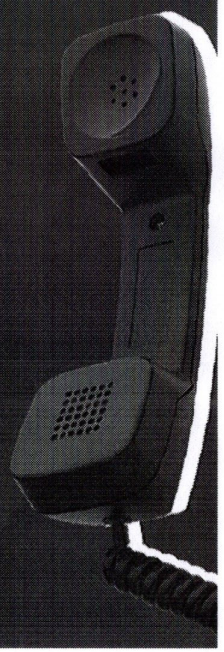
Памятка



Не передавать любой конфиденциальной информации о себе другим лицам, в том числе по телефону (номера банковских карт и коды доступа к ним, пароли, PIN-коды и т. п.). При возникновении каких-либо проблем **обращайтесь в службу поддержки** Вашего банка или оператора связи по телефону, указанному в договоре или на самой карте.

Не переводите денежные средства по звонкам и SMS-сообщениям, где Вам сообщают, что Ваш родственник попал в беду, в этом случае обязательно **перезвоните ему** и выясните обстоятельства произошедшего и только после этого предпринимайте какие-либо действия.

Игнорируйте поступающие звонки или SMS-сообщения о причитающемся Вам выигрыше, либо компенсации за лекарства и необходимости перевода денежных средств.



При получении SMS-сообщения или звонке лица, представившегося сотрудником Вашего оператора связи, о необходимости устранения каких-либо технических проблем и перечисления денежных средств, отправки SMS-сообщений с Вашими персональными данными, приобретения карт оплаты услуг, предложении перейти на более выгодный тариф, а также оплаты каких-либо услуг, штрафов и т. п. не предпринимайте указанных действий и **лично обратитесь в сервисный центр** Вашего оператора связи, или же справочную службу за разъяснениями, либо сообщайте по номеру «02», для любых операторов мобильной связи — «112».

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ

ОБ ОСНОВНЫХ СПОСОБАХ МОШЕННИЧЕСТВ

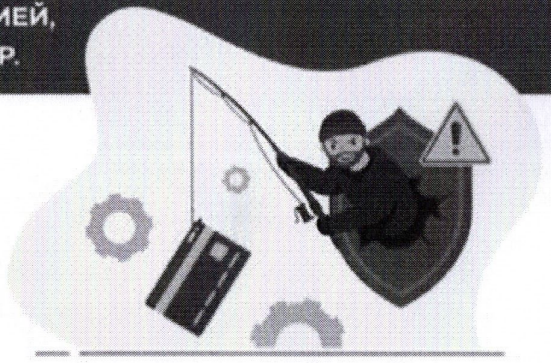
1 ЗВОНОК ПОД ВИДОМ СОТРУДНИКА БАНКА, ЛИБО ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ.

Сообщают о попытке перевода/снятия денег с карты; подачи заявки на кредит; смене номера телефона; участии в специальной операции по поимке мошенников; необходимости перевода денег на «безопасные/резервные счета», требуют действовать незамедлительно, могут использовать технологию подмены номера (вы можете видеть реальный номер телефона госструктур и банков), сообщают о необходимости соблюдать конфиденциальность разговора.

2 ЗВОНОК С ПРЕДЛОЖЕНИЕМ ДОП. ЗАРАБОТКА ПУТЕМ ИНВЕСТИРОВАНИЯ НА БИРЖЕ ПО ТОРГОВЛЕ ЦЕННЫМИ БУМАГАМИ, КРИПТОВАЛЮТОЙ И ДР.

Представляются сотрудниками «очень популярной» и «крутой» иностранной биржи, обещают сверхприбыль за короткий промежуток времени.
Для коммуникации могут использовать Skype, WhatsApp и др.

3 БЛИЗКИЙ ЧЕЛОВЕК (ДРУГ, РОДСТВЕННИК) ПОПАЛ В БЕДУ: ДТП, ЗАДЕРЖАН ПОЛИЦИЕЙ, ПОПАЛ В БОЛЬНИЦУ И ДР.

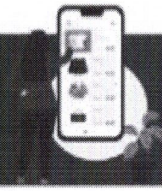


Представляются близким человеком и сообщают, что нужна крупная сумма денег; звонящий представляется сотрудником правоохранительных органов и требуют денежные средства для решения вопроса.

4 ВАМ СООБЩИЛИ, ЧТО ПОЛОЖЕНА КОМПЕНСАЦИЯ ЗА ПРИОБРЕТЕННЫЕ РАНЕЕ ЛЕКАРСТВА/УСЛУГИ, ЛИБО НАЧИСЛЕНИИ БОНУСОВ, ВЫИГРЫШЕ.

Звонивший представляется сотрудником любых коммерческих или государственных организаций, просит назвать номера банковских карт для якобы зачисления денежных средств, либо требует осуществить оплату налога, комиссии за перевод, за услуги юриста, курьера и т.д.

5 КУПИТЬ ИЛИ ПРОДАТЬ ЧТО-ЛИБО НА ИНТЕРНЕТ ПЛОЩАДКАХ (АВИТО, ЮЛА, ДРОМ, АВТО.РУ И ДР), ЛИБО НА САЙТАХ ИНТЕРНЕТ-МАГАЗИНОВ.



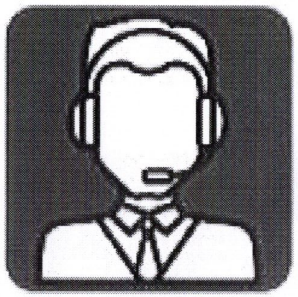
Покупатель/продавец предлагает совершить сделку дистанционно, предлагает внести предоплату, при этом общение осуществляется в стороннем мессенджере.
Отправляет интернет-ссылку для оплаты товара, либо получения оплаты за продаваемый товар, где требуется ввести реквизиты банковской карты. Цена товара на сайте значительно ниже рыночной, в доменном имени (адресная строка) популярных магазинов имеются дополнительные символы.

БУДЬТЕ БДИТЕЛЬНЫ!

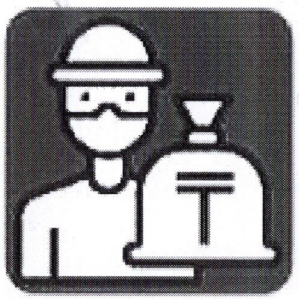
При поступлении подозрительных звонков, не паникуйте, действуйте спокойно, рационально и логично. При наличии хотя бы одного из перечисленных признаков мошенничества, не переводите и не передавайте никому деньги, не сообщайте информацию о банковских картах и пароли из смс, немедленно прекратите разговор. При необходимости обратитесь в банк, свяжитесь с родственниками, обратитесь за помощью в полицию. При желании зарабатывать на торговле ценными бумагами или валютой, используйте официально зарегистрированные компании, имеющие лицензию Центрального банка России (можно проверить на сайте ЦБ РФ).
При покупке/продажи товаров не переходите для общения в сторонние мессенджеры, это требуется злоумышленнику для направления Вам мошеннической ссылки, поскольку официальные площадки блокируют распространение таких ссылок. Покупайте товары на проверенных сайтах, используйте мобильные приложения интернет-магазинов, чтобы избежать оплаты на фишинговом (поддельном) сайте.

Остерегайтесь мошенников!

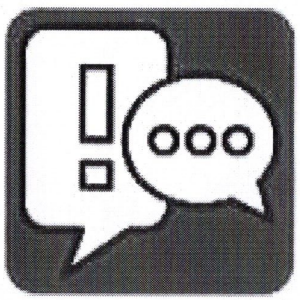
нят с похожих
леров банка



представляются
сотрудниками
банка

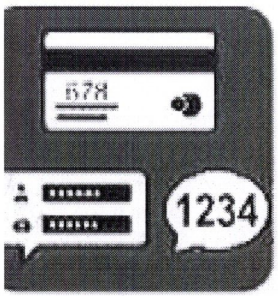


говорят, что кто-то
пытается украсть
ваши средства

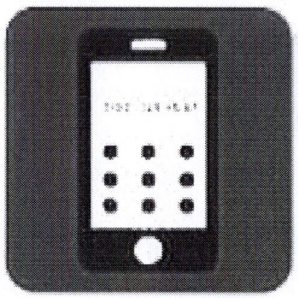


спрашивают
или просят ввести
данные карты
и коды из SMS

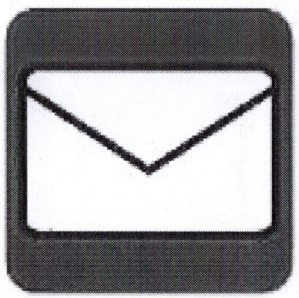
Чтобы защититься от мошенников



бщайте посторонним
із SMS, номер карты,
ействия, ПИН-код,
VC и логин/пароль
nartbank



не меняйте номер
телефона
для Smartbank
по чьей-либо просьбе



не открывайте
письма
от подозрительных
адресатов

не переходите по
полученным
из сомнительного
источника

БУДЬТЕ ОСТОРОЖН

Ежедневно злоумышленни
изобретают новые способ
хищения средств с банковск
карт, поэтому невозможно
предугадать все сценарии
развития событий. Однако п
соблюдении указанных
элементарных мер безопасно
любой пользователь сможе
предотвратить нанесение ущ
от действий мошенников.