ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ КРАСНОДАРСКОГО КРАЯ
«КУЩЕВСКИЙ КОМПЛЕКСНЫЙ ЦЕНТР СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ НАСЕЛЕНИЯ»

«ШКОЛА БЕЗОПАСНОСТИ»

ДЛЯ ГРАЖДАН ПОЖИЛОГО ВОЗРАСТА И ИНВАЛИДОВ

Правила финансовой безопасности

2022 ГОД

Низкая финансовая грамотность пенсионеров — причина, по которой они часто становятся легкой добычей мошенников. Но защититься от денежных потерь можно. Для этого познакомьтесь с правилами финансовой безопасности.

Главные правила безопасности банковских карт
Как защитить свои средства

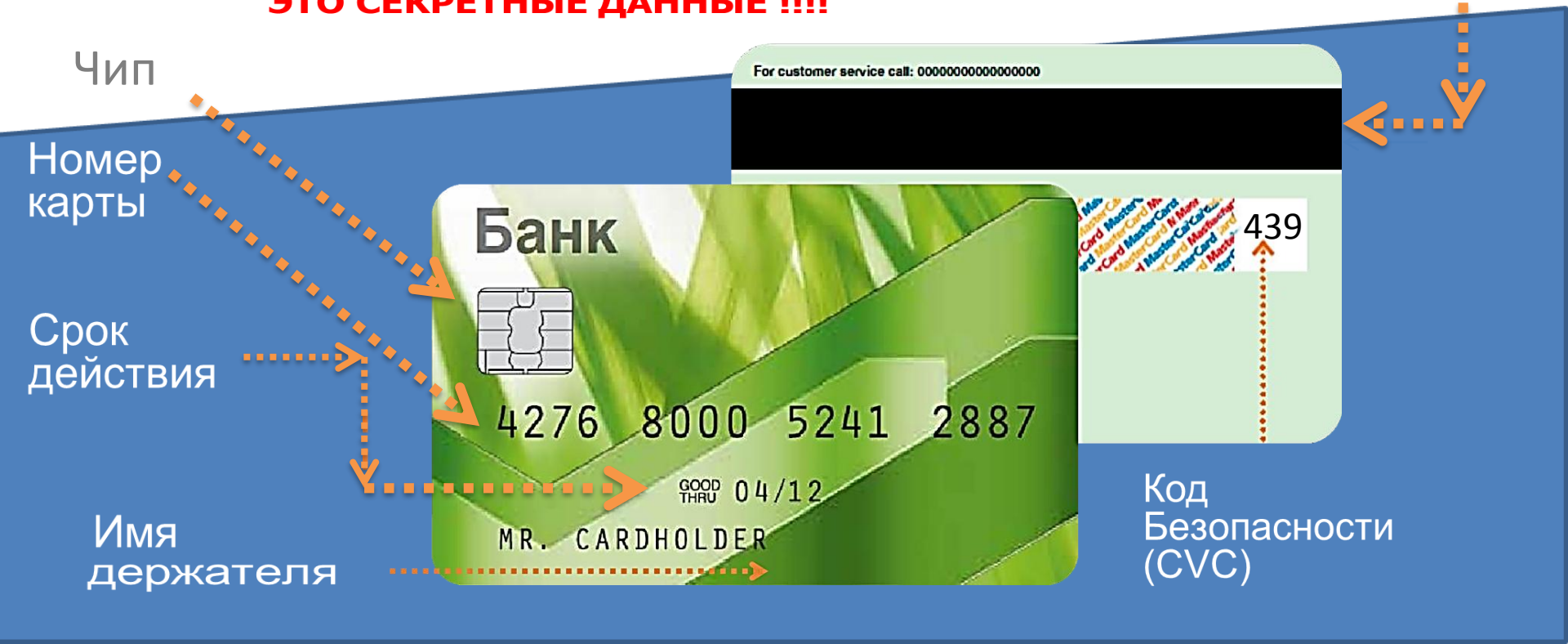
Банковская карта

Банковская карта – пластиковая карта, привязанная к одному или нескольким расчётным сетям в банке. Это инструмент, дающий возможность доступа к своему личному счету в банке. Используется для оплаты товаров и услуг, в том числе через Интернет, а так же снятия наличных.

РЕКВИЗИТЫ ПЛАТЕЖНОЙ КАРТЫ

- Номер карты
- Имя и фамилия держателя карты
- Срок действия карты
- Код CVV2/CVC2
- ПИН-код

ЭТО СЕКРЕТНЫЕ ДАННЫЕ !!!!



Правило 1

Не сообщайте ПИН-код другим лицам, в том числе родственникам, знакомым и сотрудникам банков.

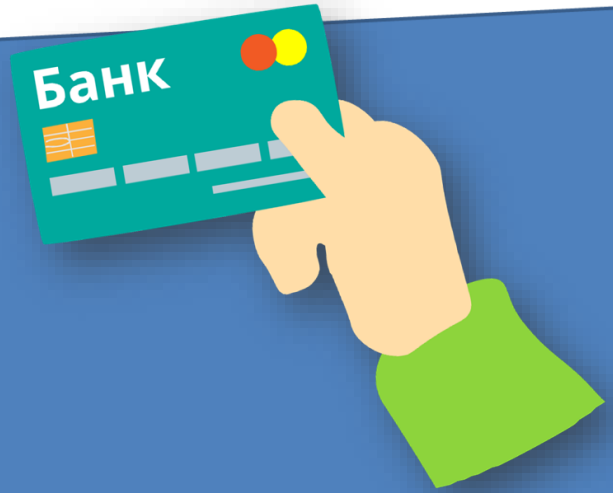
Правило 2

Не записывайте ПИН-код на карте и не храните его рядом с картой (в сумке, кошельке, в сотовом телефоне)

Правило 3

Не оставляйте карту без присмотра и НИКОМУ не передавайте.

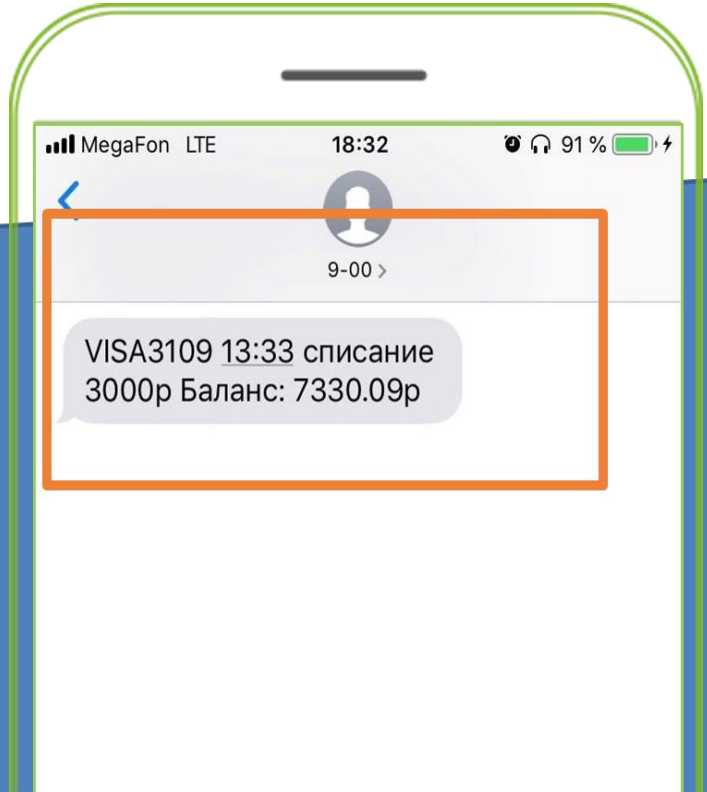
Даже если вы расплачиваетесь в кафе, требуйте, чтобы вам принесли терминал для оплаты или сами сходите до него с картой. Скопировать ее мошенники могут за пару минут, достаточно лишь переписать данные с карты.



Правило 4

Получайте SMS-оповещения.

Подключите услугу SMS-информирования об операциях, совершаемых по карте, — это позволит не только мгновенно узнать, если со счета без ведома владельца были сняты деньги, но и постоянно отслеживать сумму доступного остатка средств. Эта услуга называется «Мобильный банк».



Запомните и объясните близким следующее.

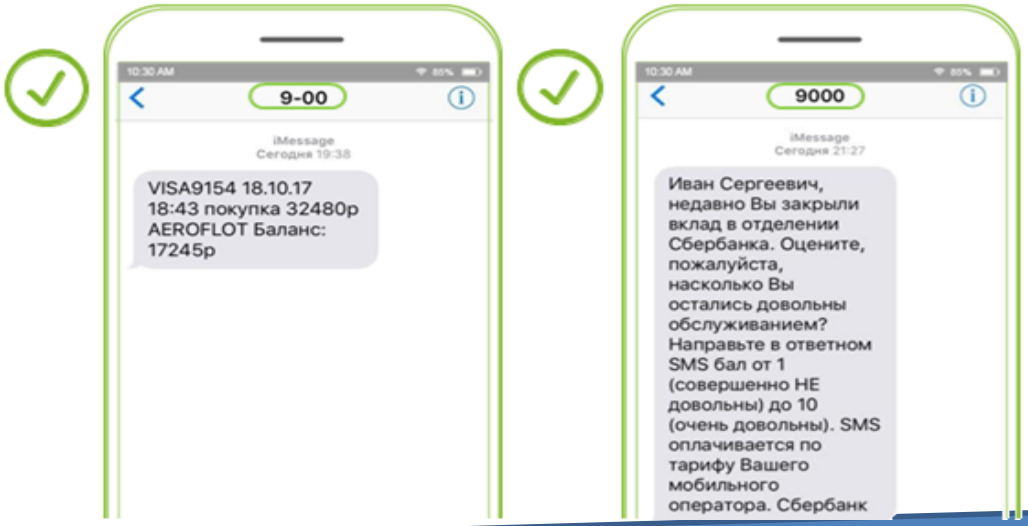
Вы не обязаны НИКОМУ сообщать свои личные данные, данные карты и одноразовые пароли! Если у банка будут подозрения в мошеннических действиях относительно вашей карты, ее сразу заблокируют. Либо сначала уточнят у вас, совершали ли вы подозрительные для них операции, а потом заблокируют. И лучше не сообщить реальному сотруднику банка нужную информацию и спровоцировать блокировку карты, чем сказать лишнее мошеннику и потерять деньги. Разблокировать карту недолго, а вернуть похищенные средства задача практически невыполнимая.

Вы не знаете наверняка, кто вам звонит, кем бы он ни представился. Хотите быть уверенным в том, что говорите не с мошенником, наберите номер банка сами.

Правило 5

Взаимодействуйте с банком только с использованием контактов, полученных непосредственно от банка, в его офисах или на сайте банка.

Так СберБанк — крупнейший банк в России, Центральной и Восточной Европе, один из ведущих международных финансовых институтов рассылает смс с номеров: 900 и 9000



Правило 6

В случае утери или кражи банковской карты, списания без вашего согласия денежных средств **немедленно сообщите об этом в банк для блокировки счета.**

Последующая инструкция при утере банковской карты

ШАГ 1

ЗАБЛОКИРОВАТЬ КАРТУ !

1. через личный кабинет на сайте банка
2. отправив СМС со специальным текстом банку
3. по телефону службы поддержки клиентов банка

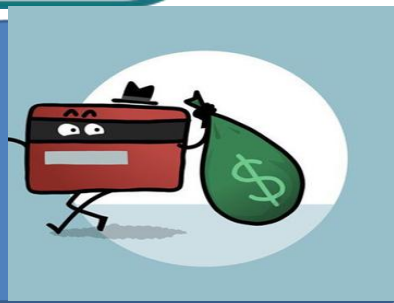
потребуется:

- кодовое слово
- данные паспорта
- номер карты

ШАГ 2

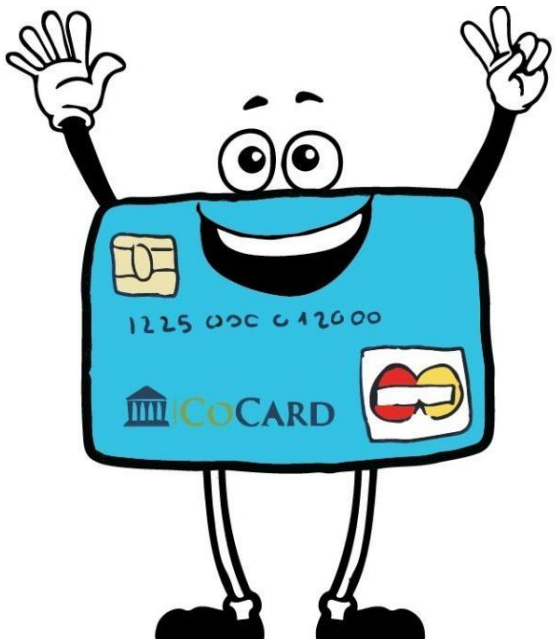
ПРИЙТИ В БАНК

написать заявление:
- о потере карты
- о перевыпуске карты



Правило 7

В случае утери телефона (замены SIM –карты) отключите услугу «мобильный банк». Помните, что услуга «мобильный банк», подключенная к номеру телефона, является доступом к вашему банковскому счету.



Правила безопасности банковских карт при использовании банкомата и терминала

Правило 1

Пользуйтесь только проверенными банкоматами и терминалами для снятия наличных денег: гос.учреждения, офисы банков, крупные торговые центры, гостиницы, аэропорты. Желательно выбрать банкоматы, которые расположены внутри помещения.

Правило 2

Не используйте банкомат, если рядом находятся посторонние лица, не вступайте в контакт с незнакомыми людьми у банкомата, не принимайте их помощь. Закрывайте клавиатуру от посторонних глаз при вводе ПИН-кода.

Правило 3

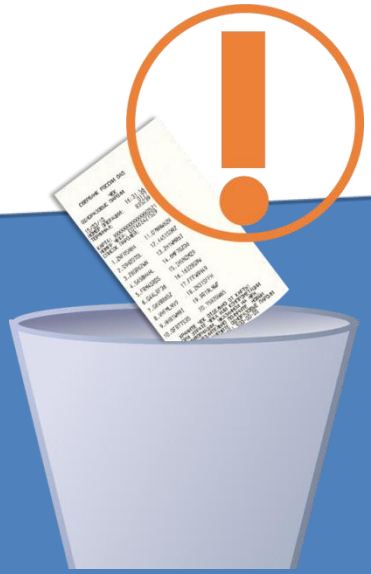
Воздержитесь от использования банкомата, если клавиатура или приемник карт оборудован подозрительными устройствами или накладками-«скиммерами». Их цель – кража Пин-кода.

Скимминг- кража данных банковской карты с помощью специальных устройств – скиммеров, которые незаметно крепятся к картоприёмнику банкомата и копируют данные с магнитной полосы карточки. Банкомат с прилепленным скиммером неспециалисту трудно отличить от оригинального оборудования – тот же рельеф и цвет. Скопированные данные «заливаются» на карту-болванку, с которой с помощью подсмотренного пин-кода снимается с карты любая сумма.

Правило 4

Проверяйте правильность суммы операции на чеке, сохраняйте выданные чеки, если оплата в банкомате или терминале была проведена некорректно.

Не выбрасывайте в урну чек, который печатает банкомат.



Правила безопасности банковских карт с использованием сети Интернет

Правило 1

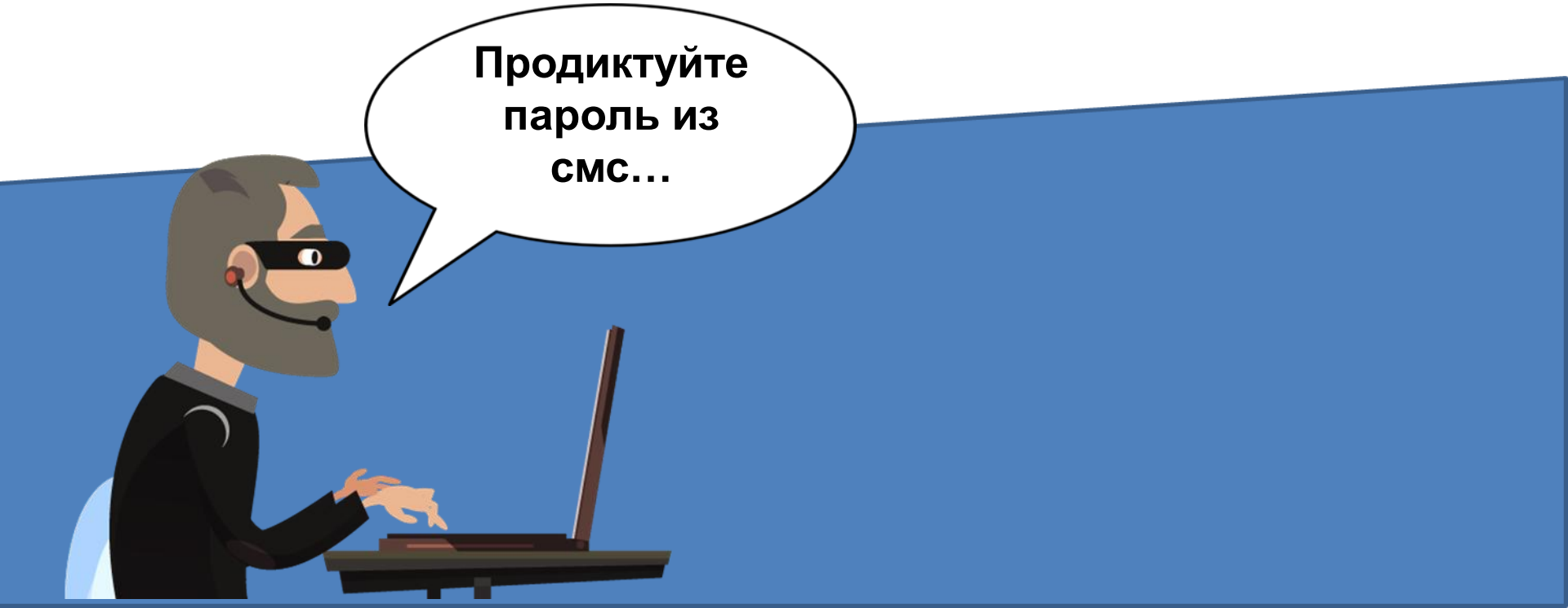
Совершайте покупки в сети Интернет на проверенных сайтах и желательно с помощью отдельной карты.

Обращайте внимание на адрес сайта, с которого осуществляется оплата. Он должен начинаться с «https://»

Мошенники могут перенаправить вас на поддельные сайты известных интернет-магазинов или сайтов, где у вас есть учетная запись. Если вы решите оплатить на них товар со своей карты, то потеряете деньги. А если попытаетесь войти на таком сайте на свою страницу, то раскроете свои учетные данные.

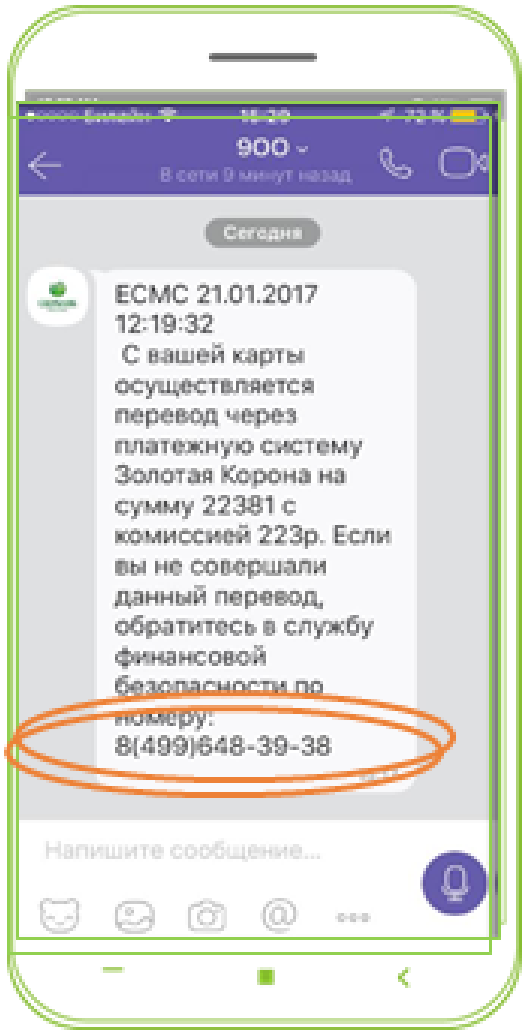
Правило 2

Не отвечайте на электронные письма и телефонные звонки, в которых от имени банка предлагается предоставить персональные данные или реквизиты карт.



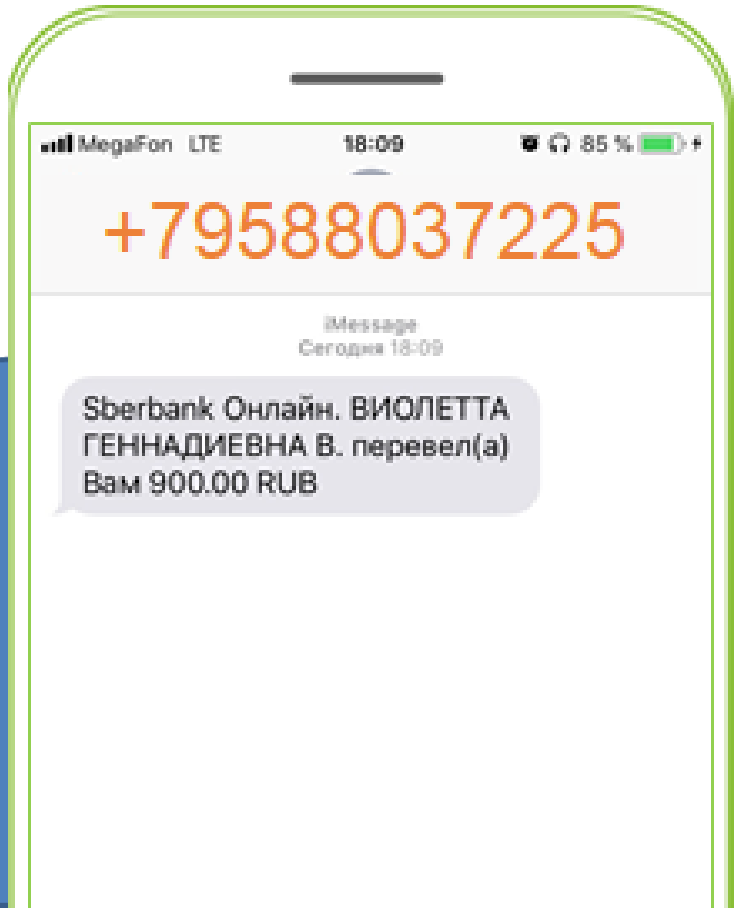
Правило 3

Не следуйте по «ссылкам», указанным в электронных письмах (включая ссылки на сайты банков), так как они могут вести на сайты – двойники.



Правило 4

Не совершайте какие-либо операции по инструкциям из СМС.



Правило 5

Установите на компьютер и мобильный телефон антивирусное программное обеспечение и регулярно обновляйте его.

Способы защиты:

- Антивирус
- Надежный пароль
- Идентификация
- Проверка адреса
- Дополнительная защита
- Чтение документации

Будьте осторожны и берегите свои деньги!