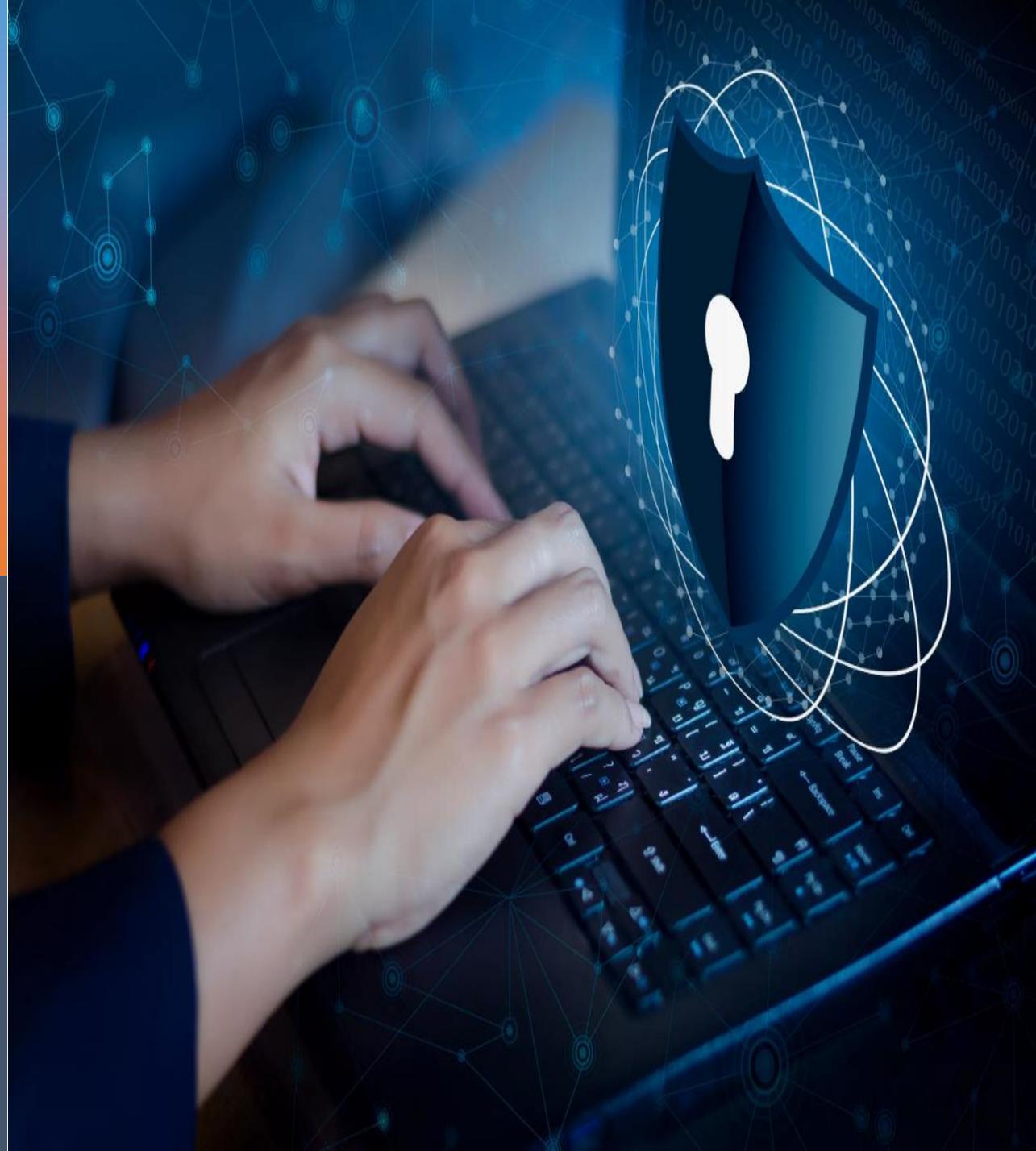




Банк России

**О мошеннических схемах
по замене банкнот, документов,
сим карт, смене тарифов**

Отделение Кемерово, 2024г





Финансовое кибермошенничество — это одна из самых распространенных и опасных форм преступлений в современном мире. Оно может нанести серьезный ущерб не только отдельным гражданам и организациям, но и всей экономике страны.

Проблема стоит очень остро!



Как мошенники крадут ваши деньги, представляясь оператором сотовой связи

Срок действия вашей сим-карты закончился, для ее продления необходимо оплатить комиссию...

Ваша сим-карта завтра будет заблокирована, для разблокировки пополните счет 40817810....





Банк России

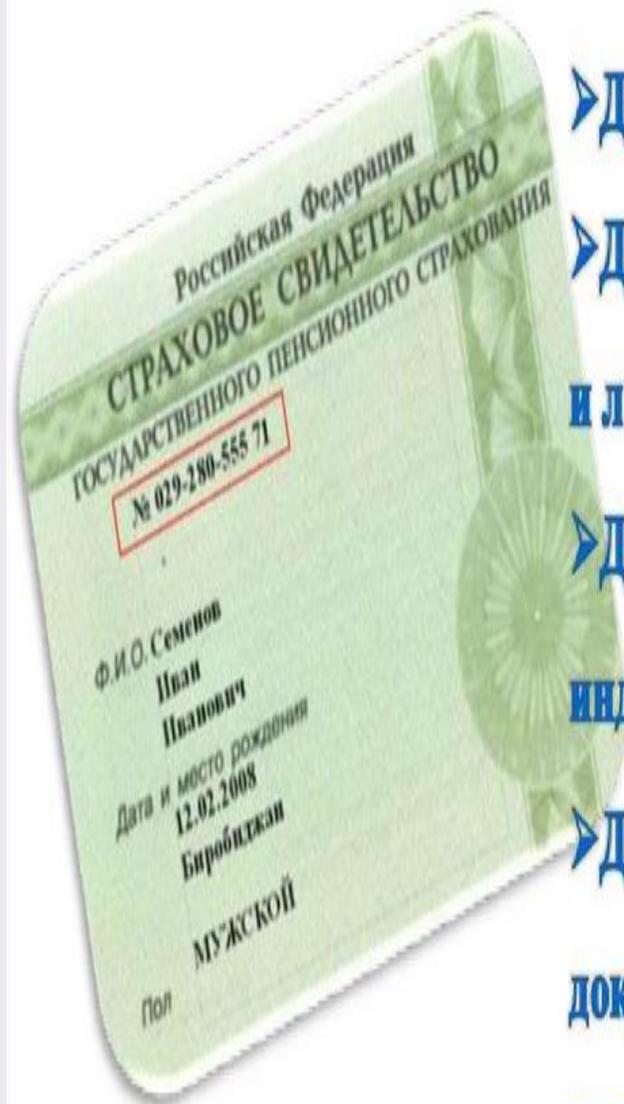
Как похищают деньги с помощью поддельного приложения Минздрава

Установите «**Приложение Минздрава**», которое на самом деле является фишинговой программой. Далее мошенники получают удалённый доступ к устройству и похищают деньги.



СНИЛС - страховой номер индивидуального лицевого счета гражданина в системе обязательного пенсионного страхования

1. номер не меняется в течение жизни, даже при смене паспорта и фамилии
2. номер относится к персональной информации



- Для формирования пенсии;
- Для получения государственных услуг и льгот, в том числе в электронном виде;
- Для контроля за состоянием индивидуального лицевого счета;
- Для сокращения количества документов при получении государственных услуг

Что нужно знать о новых банкнотах

! Старые банкноты **НЕ НУЖНО**
обменивать на новые

Если вас принуждают к обмену
— это **МОШЕННИКИ!**

О новой схеме мошенников — обмен старых денег на новые



ЧТО ДЕЛАТЬ, ЕСЛИ МОШЕННИКИ ПОХИТИЛИ ДЕНЬГИ С КАРТЫ?



**Заблокируйте
карту**



**Сообщите
в банк**



**Напишите
заявление в
полицию**

в мобильном приложении банка звонком на горячую линию банка личным обращением в отделение банка

при личном обращении в ближайший отдел ОВД



Сразу же



**В течении
суток**



**Как можно
скорее**

КАК РАСПОЗНАТЬ **МОШЕННИКА?**



Аккаунт отправителя. Отсутствие или подозрительно небольшое количество друзей и подписчиков является первым фактором, на который стоит обратить внимание.

Спешка. Мошенник использует такие слова как *быстрее, срочно, необходимо, сейчас, экстренно, желательно делать все быстрее, как можно скорее.*



Мошенники могут подражать официальным аккаунтам и копировать их фразы, смайлики.



Мошенники часто начинают переписку поздно вечером, в ночное время суток, готовы перезвонить, установить видеосвязь.



Настойчивость: аферисты повторяют отдельные слова и предложения.



В сообщении мошенника **много глаголов, которые называют определенные действия:** *заполните, пришлите, уточните, ответьте, перейдите.*

Используются слова и фразы, которые воздействуют на эмоциональное состояние: *мамы не стало, ребенок в реанимации.*

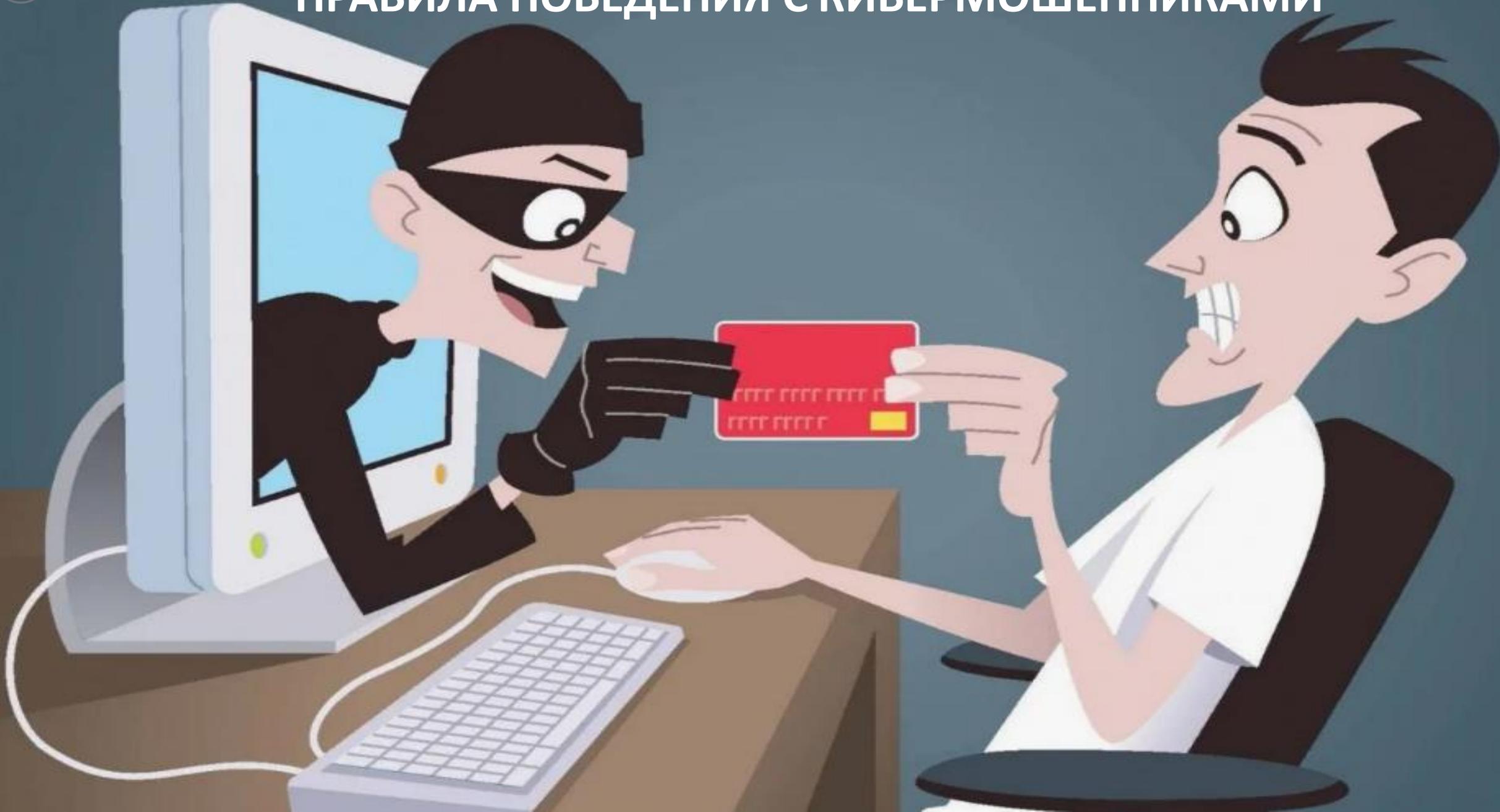
Мошеннические тексты включает приветствие, уточняющие вопросы, побуждение к действию.



В предложениях пропущены значимые слова.

В оформлении текста – опечатки и ошибки.

ПРАВИЛА ПОВЕДЕНИЯ С КИБЕРМОШЕННИКАМИ





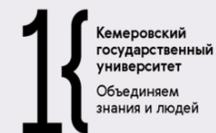
Банк России

СПАСИБО ЗА ВНИМАНИЕ!

Контактный центр Банка России
8-800-300-30-00

(для бесплатных звонков
из регионов России)

Интернет-приемная Банка России
cbr.ru/reception



Мы в Telegram



Мы в VK



Мы в ОК



<https://рцфгк42.рф>



ЯДзен



Мы в RuTube

Полезные
цифровые
сервисы:



Официальный сайт Банка России
cbr.ru



Информация доступным языком
fincult.info



Курсы для инвесторов любого уровня
school.moex.com/



Официальный портал о социально-экономической ситуации в России
obyasniam.rf



Официальный сайт Ассоциации развития финансовой грамотности
fincubator.ru



Персональный навигатор по финансам
moifinansy.rf