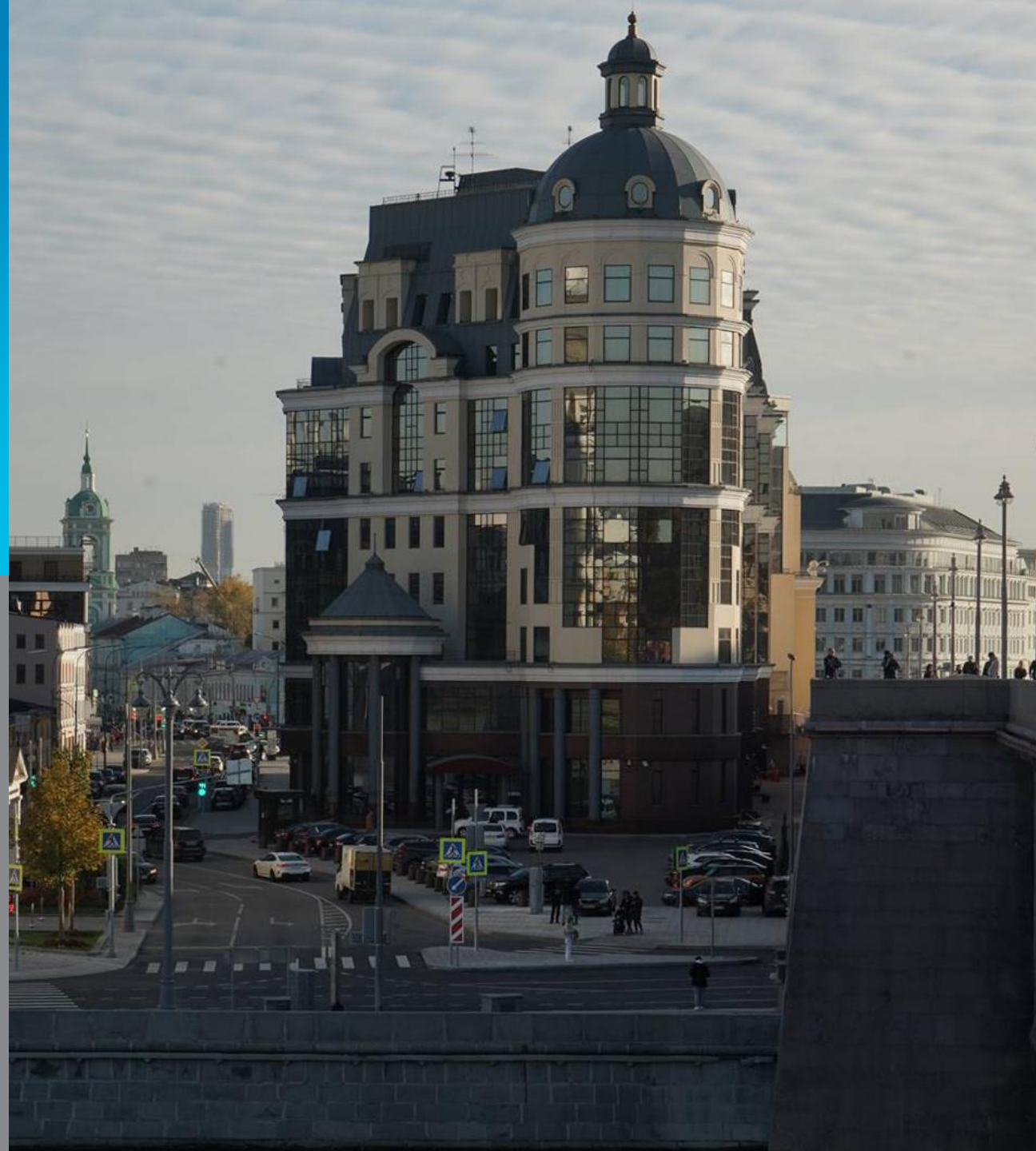
Банк России

НОВЫЕ СПОСОБЫ ФИНАНСОВОГО МОШЕННИЧЕСТВА

2023 г.



Деньги – это информация

Информация используется для управления деньгами:

- Данные карты (Номер, срок действия, Ф.И.О. владельца, код подтверждения (CVV2 или CVC2)
- Логин и пароль от личного кабинета (онлайн-банк)
- Кодовое слово (для обращения в банк по телефону)
- Код в СМС-сообщении или уведомлении в приложении банка (как второй фактор аутентификации)

Цель мошенника – получение информации

Мотивация мошенника – деньги

Используемый инструментарий:

- Социальная инженерия
- Сбор информации из открытых источников (OSINT)
- Поддельные сервисы и сайты
- Вирусы и другое вредоносное ПО

Кто может стать жертвой мошенников?

Жертвой мошенников может стать любой человек независимо от уровня образования, возраста и предпочтений

Импульсивность и толерантность к риску – два главных фактора, увеличивающих шанс стать жертвой мошенников:

- Открывание электронных писем от неизвестных отправителей
- Переход по заманчивым ссылкам
- Склонность к рискованным инвестициям
- Участие в розыгрышах и лотереях
- Участие в финансовых пирамидах

Телефонное мошенничество

Сразу завершите разговор, если в момент входящего звонка вам:

- задают вопросы о персональных данных: номерах карт, пароле из СМС, паспортных данных, последних совершённых операциях, кодовых словах.
- сообщают, что для сохранности ваших денег нужно установить дополнительное программное обеспечение или перевести деньги на другой счёт.

Сохраняйте бдительность при получении звонка с неизвестного номера.

Не совершайте никакие операции и действия по инструкциям звонящего.

Помните, сотрудники банка никогда:

- не запрашивают персональные данные: логин, пароль, код из смс, номер карты, счета. пин-код, CVV, кодовое слово и т.д.
- не просят клиентов устанавливать на устройства программы и приложения.
- не направляют в мессенджерах документы, подтверждающие мошеннические действия в отношении клиента или документы от имени банка, подтверждающие предоставление «защищенной ячейки», временного счета для сохранения средств.

Преступники в Сети

Мошенники используют в своих схемах веб-ресурсы, приложения для смартфонов, планшетов и компьютеров

- Скачивайте приложение только в официальных магазинах приложений. Обратите внимание на количество скачиваний, рейтинг приложения, реальные комментарии.
- Используйте антивирус.
- Используйте антиспам.
- Не кликайте по рекламным баннерам, не переходите по ссылкам от незнакомцев и не вводите данные банковской карты на подозрительных страницах.
- Старайтесь использовать проверенные ресурсы для совершения онлайн-покупок.

Финансовые пирамиды – онлайн мошенничество

1. Пирамиды всегда гарантируют высокий доход без риска.
2. За каждого привлеченного вкладчика обещают начислить процент от их взноса.
3. Компания ведет очень агрессивную рекламную политику.
4. У финансовой пирамиды никогда нет подтверждения инвестиций.
5. На сайте компании нет контактов для связи: номеров телефонов, электронной почты, почтового адреса.

Как проверить финансовую организацию:

1. Наличие лицензии ЦБ на инвестиционную деятельность (проверить ее актуальность).
2. Не занесена ли компания в список компаний с выявленными признаками нелегальной деятельности на финансовом рынке.

https://www.cbr.ru/inside/warning-list/

https://www.cbr.ru/fmp_check/

Черные кредиторы в интернете

За 2022 год Банк России выявил 1722 нелегалов, которые незаконно выдавали кредиты и займы. Это почти вдвое больше, чем годом раньше.
Мошенники рекламируют свои услуги на сайтах объявлений под видом займов «от частных лиц».

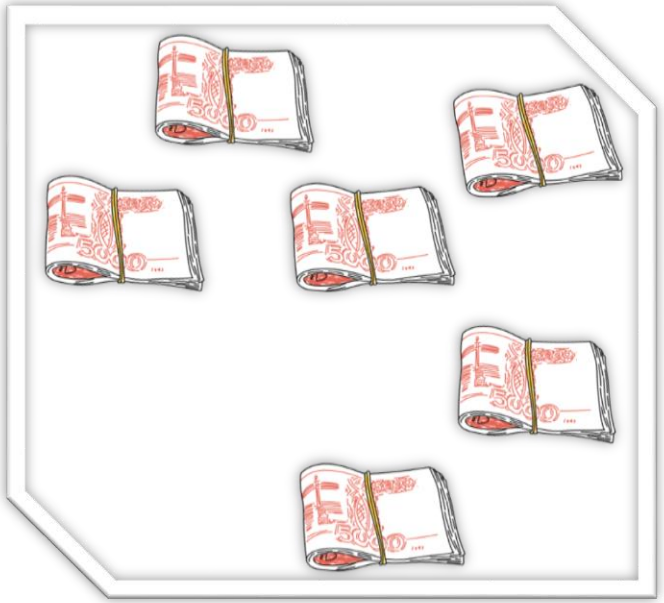
Там они оставляют ссылки на закрытые каналы в мессенджерах, группы в соцсетях, где и договариваются о нелегальных ссудах.

Риски при оформлении займов у черных кредиторов:

- высокий процент;
- на словах обещают одни условия, а в договоре другие;
- выбивают долги угрозами, шантажом или силой;
- используют личные данные клиентов, чтобы набрать кредиты и займы для себя.

Вовлечение в преступную деятельность

- **Мошенники присылают деньги и просят их снять со счета (обналичить) и внести наличные на счет в другом банке за вознаграждение**
- **Соглашаясь на обналичивание средств вы становитесь соучастником преступления**



Как поступить?

- Прервать разговор, перезвонить самостоятельно в банк по номеру горячей линии вашего банка (указан на обратной стороне карты).
- Зафиксировать с сотрудником службы безопасности банка ситуацию.
- Не переводить, не снимать и не тратить «пришедшие» деньги.

Кибермошенники быстро адаптируются к ситуации

Мошенники оперативно реагируют на изменения в информационном пространстве и адаптируют свои схемы под текущую ситуацию:

- На фоне новостей о распространении коронавируса.
- На фоне ограничительных мер и санкций мошенники эксплуатируют панические настроения граждан.
- Мошенники пользуются недостаточной осведомленностью, играют на чувствах жертв – волнении и страхе.
- Лучшая защита от мошеннических действий – ваши знания и осмотрительность.

Новые способы обмана

Мошенники выманивают деньги и ПДн, прикрываясь именем Росфинмониторинга

Мошенники от имени Росфинмониторинга сообщают, что банковский счет адресата якобы заморожен из-за подозрительной активности, и требуют уплатить некую комиссию за разблокировку.

В качестве причины мнимой блокировки аферисты могут назвать нарушение законодательства о противодействии легализации преступных доходов (отмывание денег) или финансирование терроризма. В некоторых фейковых письмах присутствует имитация символики и печатей Росфинмониторинга.

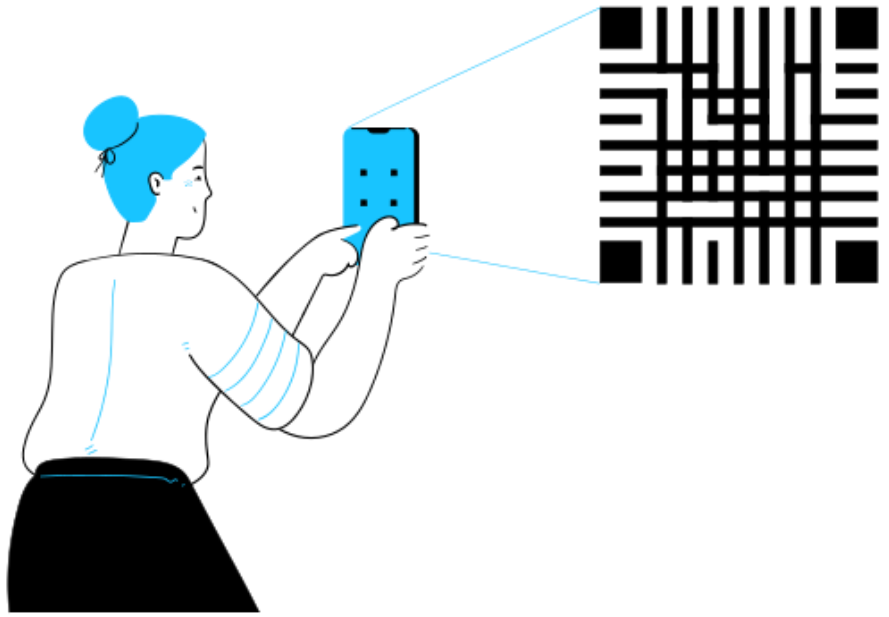
РОСФИНМОНИТОРИНГ

QR-коды

Мошенники используют как приманку тематику повышения тарифов и выдачи пособия

Аферисты расклеивают на улицах и в подъездах QR-коды; если их отсканировать, попадешь в мессенджер с чат-ботом, сообщающим о некой социальной выплате.

Для ее оформления нужны персональные данные и банковские реквизиты, которые затем оседают в базах мошенников.



Безопасность в мессенджерах

Мессенджеры становятся все более функциональными: общение, магазины, банкинг.

Кибермошенники активно перебираются в мессенджеры.

В мессенджерах создаются фальшивые магазины, похищаются данные карт, крадутся деньги, «угоняются» аккаунты.

Чтобы защитить себя:
обязательно установите пароли на вход в мессенджеры, а лучше используйте двухфакторную аутентификацию;

никому не сообщайте коды аутентификации;

будьте осторожны, переходя по любым ссылкам;

сохраняйте бдительность.

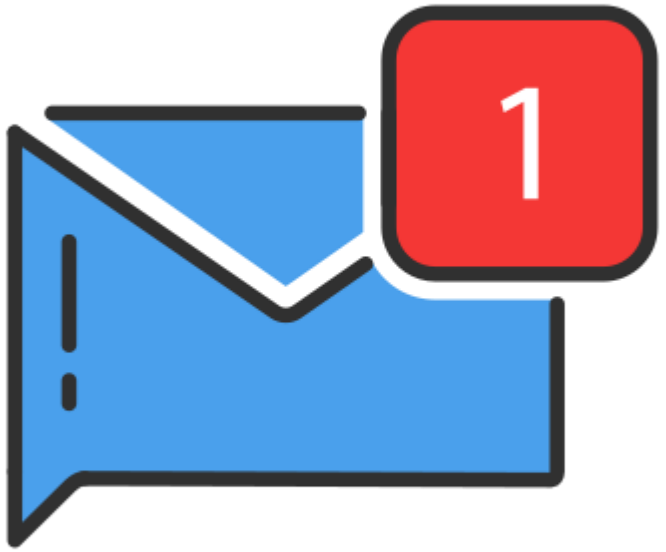
Фишинговые сообщения

От имени Роскомнадзора рассылают фишинговые сообщения.

В сообщениях говорится о якобы обнаруженных на ресурсах адресатов запрещенных материалах или уведомляется о предстоящей блокировке.

Чтобы узнать адрес сайта, нарушившего требования законодательства, необходимо открыть вложение.

Вложение заражено: в нем содержится вредоносный код.



Подозрительные письма на корпоративной почте

Что делать если вы получили подозрительное письмо по электронной почте?

- Обращайте внимание на адрес электронной почты, с которого пришло письмо от контрагента.
- Всегда проверяйте вложения в письме на предмет вирусов.
- После окончания работы с банком обязательно отключайте токен от компьютера.
- Внимательно проверяйте реквизиты при подтверждении операции
- Если подозрительное письмо пришло от вашего контрагента – свяжитесь с ним по другому каналу (мессенджер, телефон)
- Будьте внимательны при просмотре почты, изучите признаки фишинговых писем.

Признаки фишингового письма

- **Неизвестный доменный адрес**

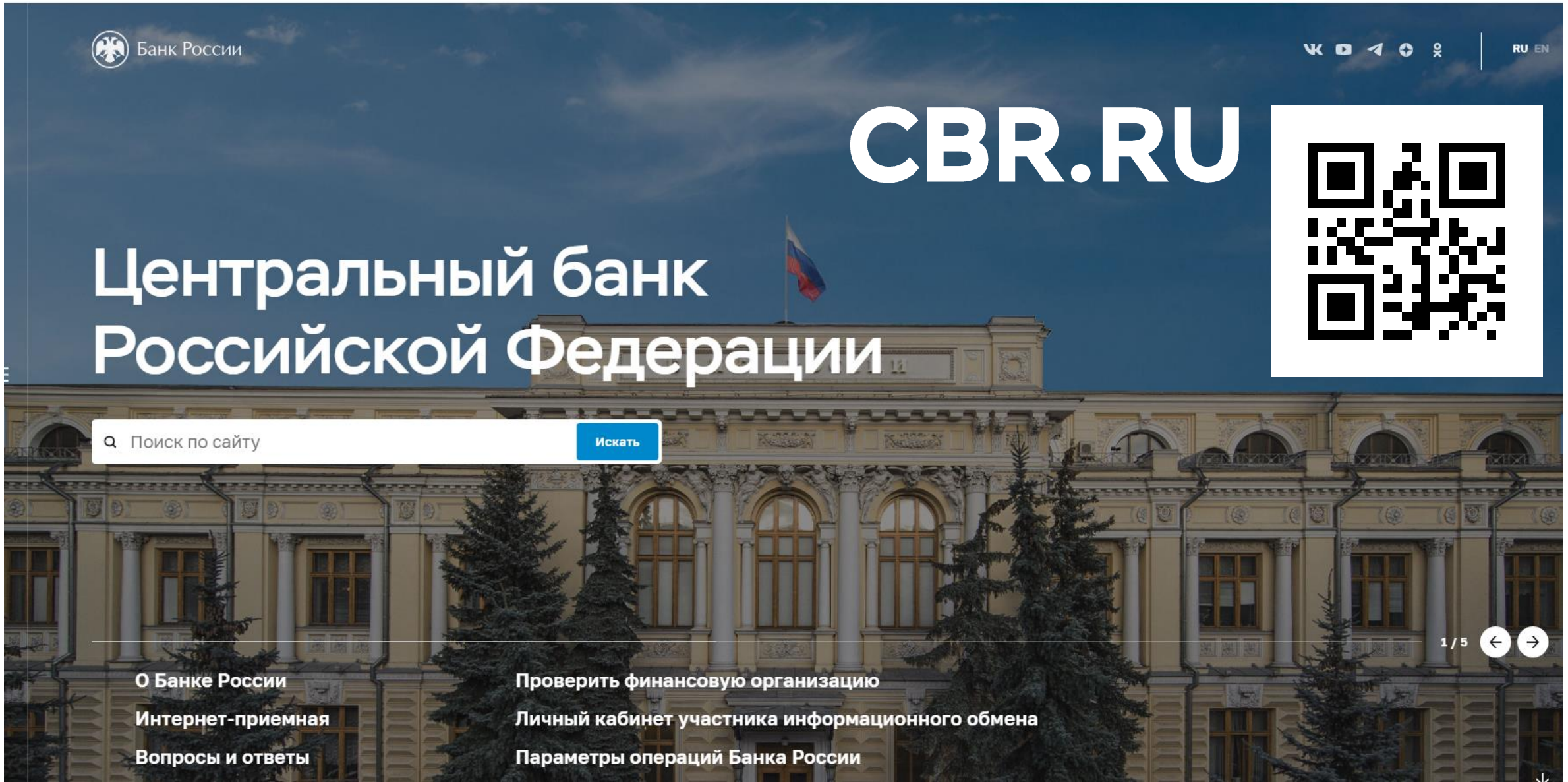
Мошенники незначительно меняют имя домена:
lvanovII@company1.ru

- **Измененные названия известных брендов**:
aplle.com, fnc.ru
- **Ошибки в словах для обхода спам-фильтров**
«Отправьтепароль» или «отправте пароль»
- **Обезличенное обращение**
«Уважаемый сотрудник»!
- **Просьба ввести логин или пароль**
Письмо от «ИТ-службы» с просьбой сменить пароль для того …
- **Предложение перейти по сомнительной ссылке**
- **Срочность**
«срочная проверка», «заблокируется через 30 минут!!!»

Деятельность Банка России по пресечению киберпреступлений

- ФинЦЕРТ – Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере.
- Разработка и совершенствование стандартов обеспечения информационной безопасности в финансовой сфере.
- Сбор статистики и анализ информации для повышения эффективности противодействия преступлениям.
- Ведение просветительской работы.

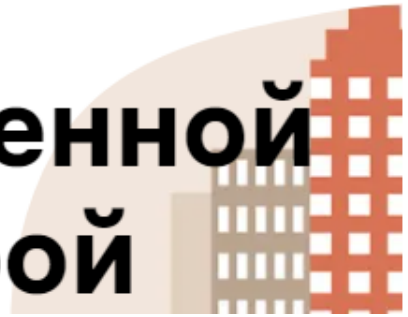
МЕРЫ ЗАЩИТЫ ФИНАНСОВОГО РЫНКА



Банк России сохранил ключевую ставку на уровне 7,5%

Что это значит?

Сделка с заложенной квартирой



Истории о мошенничестве — грабли, на которые лучше не наступать

Банковская карта | Звонки | Мошенничество | Мошенничество на финансовом рынке | Программы и приложения | Сайты | Сервис объявлений | Смартфон | СМС | Социальные сети и мессенджеры | Украли деньги | Электронная почта

«Скинь 500 рублей до вечера. Меня не взломали — вот фото карты»

«Введите номер карты, а три цифры с оборота мы подсмотрим сами»

«Вам звонит Росфинмониторинг. Заплатите штраф за отмывание доходов, иначе заблокируем счета»

«Увеличу ваш капитал в пять раз за сутки. Переведите деньги моему помощнику»

Банк России

СПАСИБО
ЗА ВНИМАНИЕ