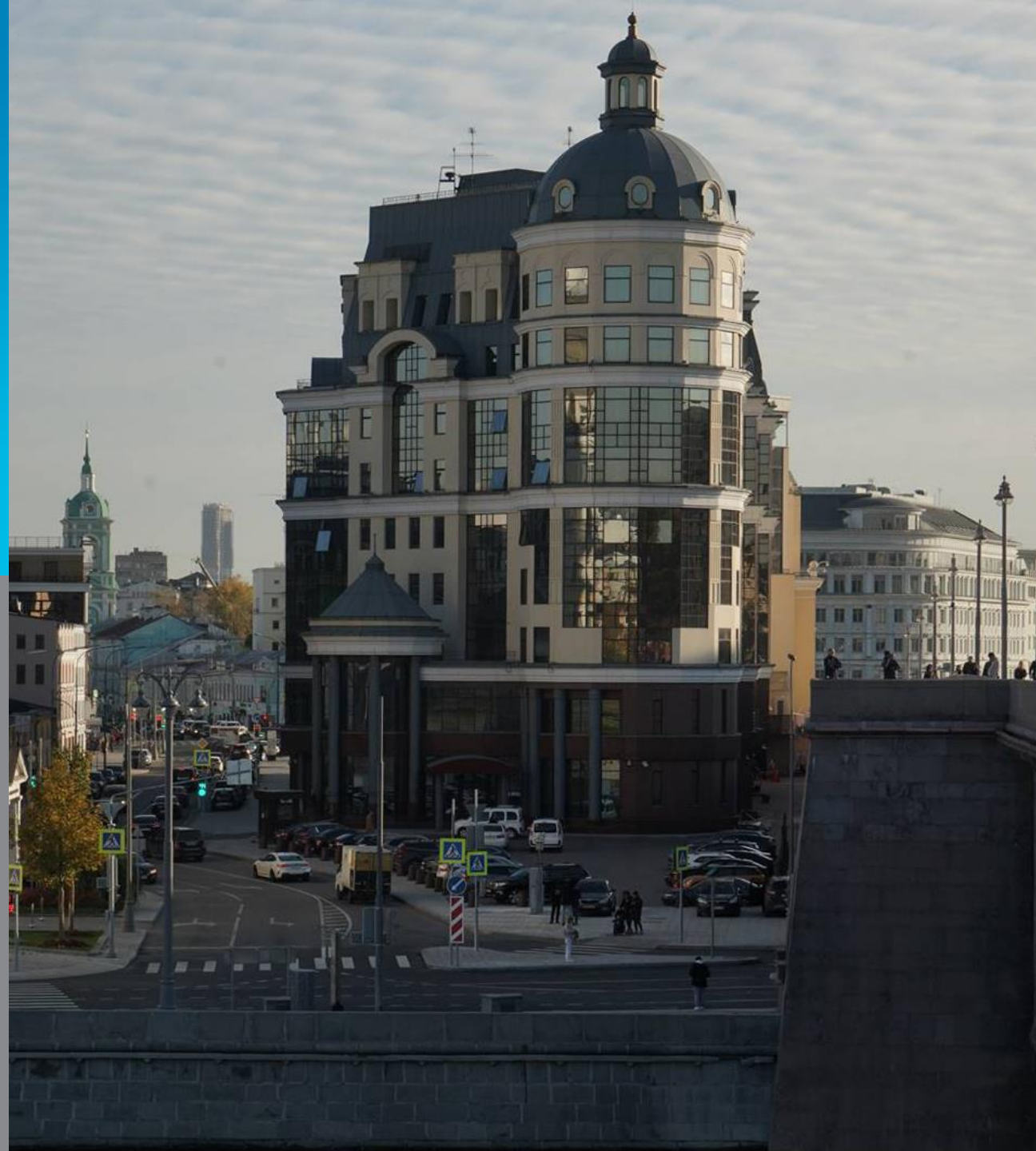
Банк России

ЦИФРОВАЯ ГРАМОТНОСТЬ И КИБЕРБЕЗОПАСНОСТЬ

2022 г.



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

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)

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:

- Склонность к рискованным инвестициям
- Онлайн-шопинг
- Открывание электронных писем от неизвестных отправителей
- Участие в розыгрышах и лотереях
- Участие в финансовых пирамидах

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

Хакерские атаки. Как защититься?

Мошенники все чаще используют в своих схемах приложения для смартфонов, планшетов и компьютеров

- Скачивайте приложение только в официальных магазинах приложений. Обратите внимание на количество скачиваний, рейтинг приложения, свежие комментарии
- Обновляйте антивирус
- Хакеры часто подделывают игровые приложения – будьте внимательны при переходе по ссылкам в игре
- Не кликайте по рекламным баннерам, не переходите по ссылкам от незнакомцев и не вводите данные банковской карты на подозрительных страницах

Заманчивые вакансии без опыта работы, без образования, с гарантией стабильного высокого дохода

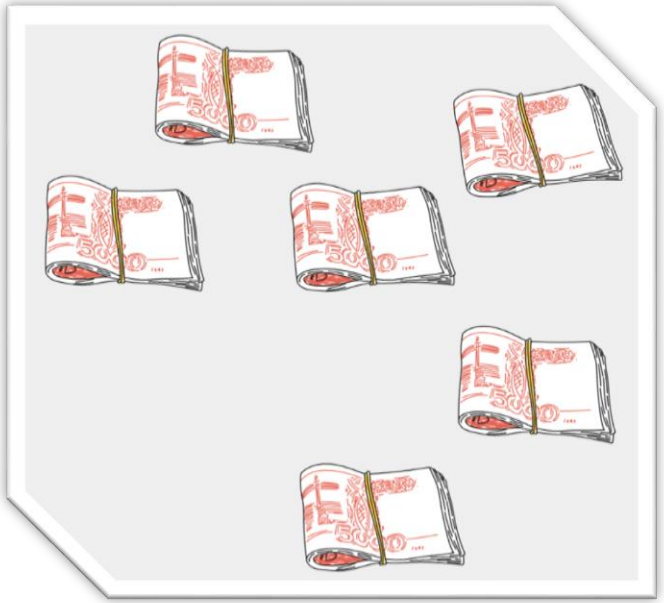
За подобными объявлениями могут скрываться:

Услуги по незаконному обналичиванию
и отмыванию денег

- Сетевой маркетинг, где доход формируется из продажи какого-то товара или услуги и комиссии за привлечение новых людей в фирму
- Ненастоящие вакансии с платным обучением (чаще всего дело не доходит не только до работы, но и даже до самого обучения)

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

Финансовые пирамиды – онлайн мошенничество

1. Пирамида всегда гарантируют высокий доход без всякого 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.
   Ни номеров телефонов, ни электронной почты,
   ни 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/

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
- Сбор статистики и анализ информации для повышения эффективности противодействия преступлениям
- Ведение просветительской работы

К связаться с Банком России?

Направить жалобу в Банк России

Ответы на часто задаваемые вопросы

Мобильное приложение «ЦБ онлайн» - можно задать вопрос специалисту в чате

Контакт-центр Банка России

8 800 300-30-00

круглосуточно, бесплатно для звонков с мобильных телефонов

300