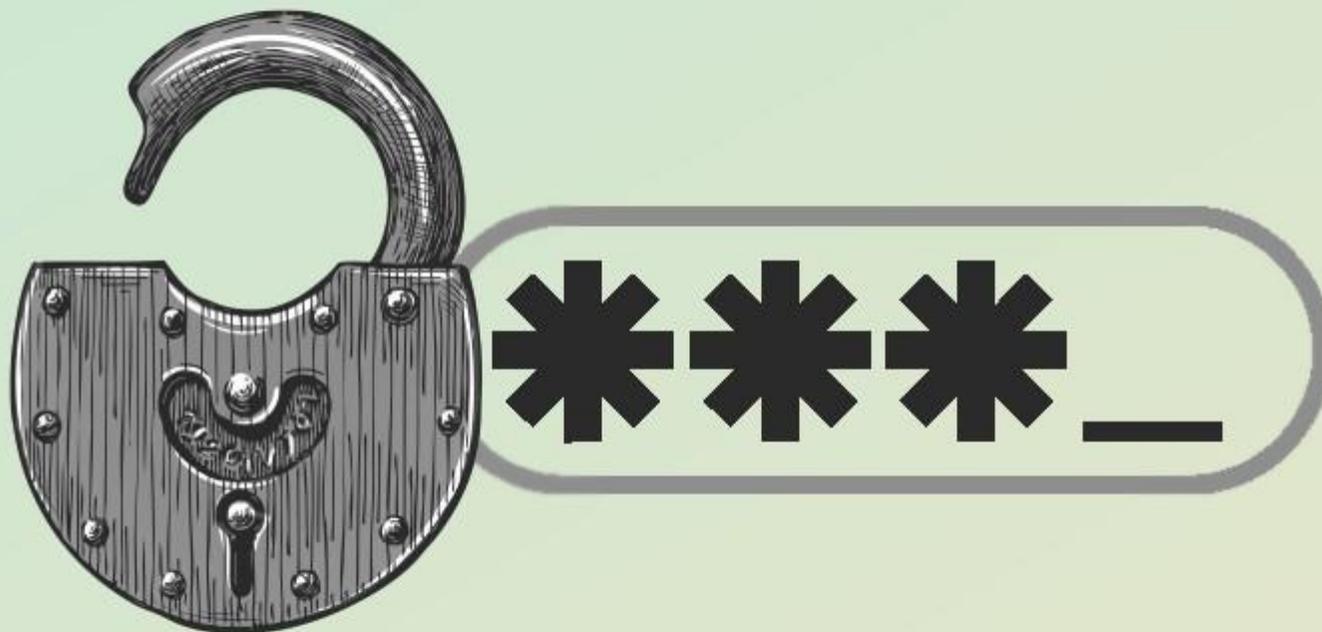


Настоящий сотрудник банка
никогда не спросит секретные
реквизиты карты,
ПИН-коды и пароли.



2 С вами говорят о деньгах

Основная задача
мошенников — получить доступ
к чужим деньгам.

Вам могут предложить:



перевести все деньги
на «безопасный счет»



оплатить «страховку
для получения кредита»



«очень выгодно» инвестировать
свои сбережения.



И многое другое. Главное:
речь всегда будет идти о деньгах.



1 Незнакомец неожиданно связывается с вами сам

Например, от имени банка, полиции, магазина. Способы могут быть разные – звонок, СМС или ссылка в мессенджере.

Общее у них одно – кто-то сам вышел на связь с вами. Значит, ему что-то от вас нужно.





5

На вас давят:



торопят



принуждают к чему-то



ставят условия:

«сейчас или будет поздно».

Такие ситуации полозрительны.

Никогда не принимайте поспешных решений, особенно если они касаются ваших денег.

Звонят из банка с тревожными новостями? Положите трубку и наберите номер горячей линии банка сами, чтобы прояснить реальное положение дел.



ААААА
МНЕ ТУТ
ЗВОНЯТ,

Не беспокойтесь,
ваши деньги
в порядке

ПРАВИЛО № 3

ПО ВОЗМОЖНОСТИ ПОЛЬЗУЙТЕСЬ АНТИВИРУСАМИ

Рекомендуем установить и регулярно обновлять защитные программы на своих гаджетах.

Они могут защитить устройство от вируса, спама или вредоносного сайта, с помощью которых мошенники крадут деньги.



ПРАВИЛО № 4

ПОСЕЩАЙТЕ БЕЗОПАСНЫЕ САЙТЫ

Злоумышленники часто создают фишинговые сайты – они очень похожи на официальные сайты банков или компаний.

Внимательно проверяйте адрес сайта:
у поддельных название отличается от настоящего всего парой символов,
а в строке браузера может отсутствовать значок безопасного соединения (замочек).

ПРАВИЛО № 5

НЕ ПЕРЕХОДИТЕ ПО ССЫЛКАМ ОТ НЕЗНАКОМЦЕВ

Даже если ссылку прислал кто-то из друзей, не спешите ее открывать. Мошенники могли взломать его аккаунт и разослать вредоносное сообщение.

Рекомендуем позвонить знакомому и уточнить, скидывал ли он вам эту ссылку.



ПРАВИЛО № 6

ПРОВЕРЯЙТЕ ИНФОРМАЦИЮ

Если близкие в сообщениях просят перечислить деньги, обязательно позвоните им.

Убедитесь, что это именно родственник или друг обращается за помощью, а не мошенник.



4

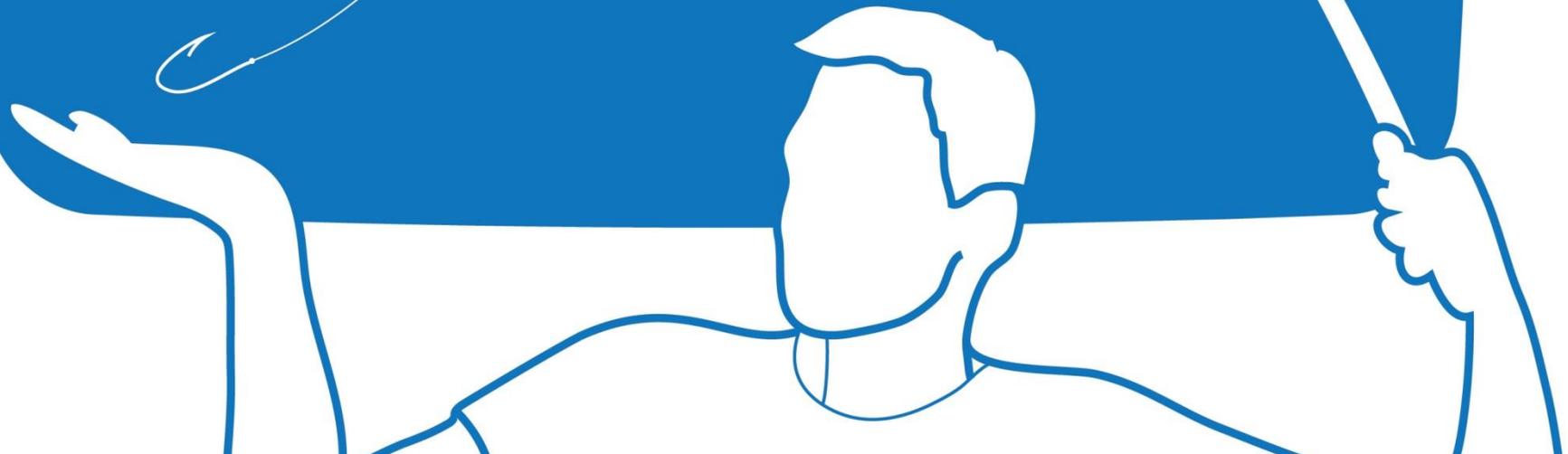
**ВАША ПОСЫЛКА ДОСТАВЛЕНА
В ПУНКТ ВЫДАЧИ ЗАКАЗОВ**

Вы можете заказать
доставку на дом по ссылке:
www.kjhdnj...



СООБЩЕНИЕ ОТ БАНКА

Мы проводим актуализацию
данных клиентов.
Подтвердите информацию
по ссылке: www.fdggh1j



ПРОВЕРЬТЕ У КОМПАНИИ ЛИЦЕНЗИЮ БАНКА РОССИИ

Сверьтесь со Справочником по кредитным организациям и Справочником участников финансового рынка на сайте cbr.ru

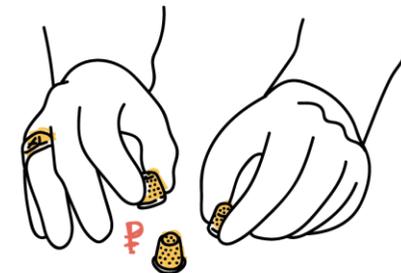


12

МОШЕННИЧЕСТВО НА ФИНАНСОВЫХ РЫНКАХ

Как обманывают на рынке Форекс?

- Недобросовестные форекс-дилеры посулят вам доход, но прибыль вы не получите и вложения потеряете
- Не стоит связываться с бинарными опционами — вы просто потеряете деньги



14

2

ВАША КАРТА ЗАБЛОКИРОВАНА

Для разблокировки
перезвоните сотруднику
безопасности Банка –
Петру Иванову
8-910-***-**-**



КИБЕРМОШЕННИЧЕСТВО. КАКИМ ОНО БЫВАЕТ?

Легенды могут быть какими угодно:

- Сообщение о подозрительной операции по счету или карте
- Известие о выигрыше в лотерею
- Уведомление о штрафе или выплате социального пособия
- Реклама суперскидок на популярные товары
- Просьба о помощи от друга
- Приглашение вложиться в сверхдоходный проект



Любые звонки, СМС, электронные письма или сообщения в соцсетях могут оказаться от мошенников.

7

ВИДЫ ФИНАНСОВОГО МОШЕННИЧЕСТВА



С БАНКОВСКИМИ
КАРТАМИ



НА ФИНАНСОВЫХ
РЫНКАХ



КИБЕРМОШЕН-
НИЧЕСТВО



ФИНАНСОВЫЕ
ПИРАМИДЫ

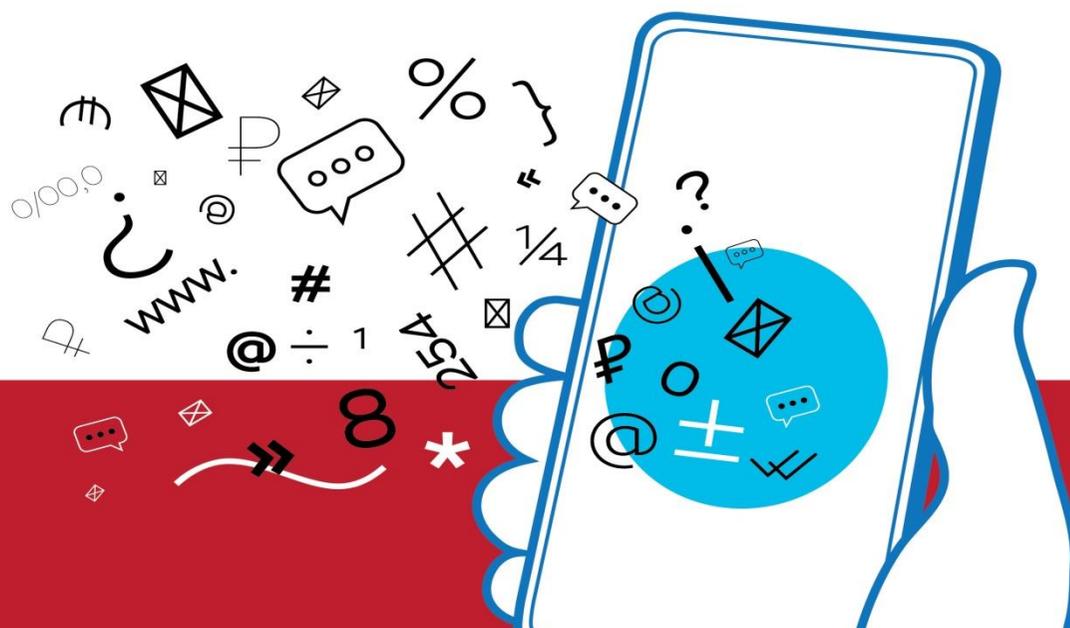
3



Банк России

ЦИФРОВАЯ ГИГИЕНА:

как защититься от телефонных
и кибермошенников?





Банк России

ОСТОРОЖНО: ТЕЛЕФОННЫЕ МОШЕННИКИ!

5 ПРИЗНАКОВ ОБМАНА

1 НА ВАС ВЫХОДЯТ САМИ

Аферисты могут представиться службой безопасности банка, налоговой, прокуратурой

Любой неожиданный звонок, СМС или письмо – повод насторожиться

2 РАДУЮТ ВНЕЗАПНОЙ ВЫГОДОЙ ИЛИ ПУГАЮТ

Сильные эмоции притупляют бдительность



ЗВОНЯТ
из банка, полиции
или другой организации?

УБЕДИТЕСЬ,
что это не мошенники!

3 НА ВАС ДАВЯТ

Аферисты всегда торопят, чтобы у вас не было времени все обдумать

4 ГОВОРЯТ О ДЕНЬГАХ

Предлагают спасти сбережения, получить компенсацию или вложиться в инвестиционный проект

5 ПРОСЯТ СООБЩИТЬ ДАННЫЕ

Злоумышленников интересуют реквизиты карты, пароли и коды из банковских уведомлений



НИКОГДА НИКОМУ



Банк России

КАК ЗАЩИТИТЬСЯ

ОТ ОНЛАЙН-МОШЕННИКОВ

Чтобы добраться до ваших банковских счетов, мошенникам нужны ваши персональные данные и реквизиты карт

Какие схемы используют аферисты?

ОБЕЩАЮТ ЗОЛОТЫЕ ГОРЫ

Опросы за вознаграждение, социальные выплаты или сверхприбыльные инвестиционные проекты. Гарантия быстрого обогащения – признак обмана

ЗАМАНИВАЮТ НА РАСПРОДАЖИ

Огромные скидки и низкие цены могут оказаться мошеннической уловкой

СПЕКУЛИРУЮТ НА ГРОМКИХ СОБЫТИЯХ

Например, объявляют сбор денег на разработку вакцин, обещают вернуть деньги за отмененные рейсы или предлагают получить государственные дотации

МАСКИРУЮТСЯ

Разыгрывают роль продавцов и покупателей на популярных сайтах объявлений

Как обезопасить свои деньги в интернете?

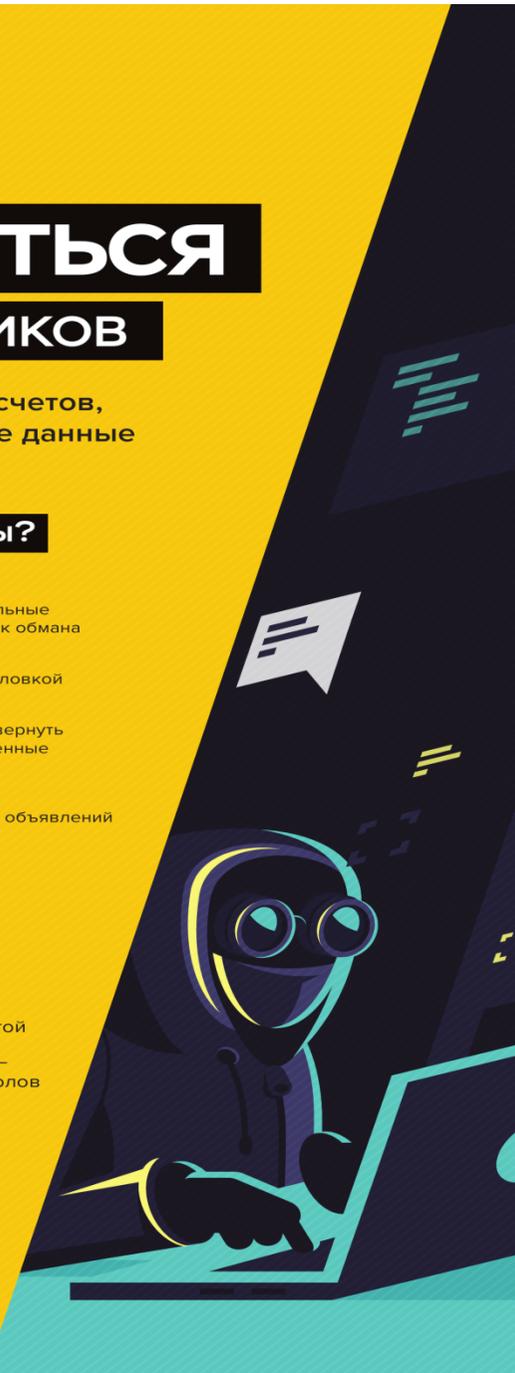
- 1 Установите антивирус и регулярно обновляйте его
- 2 Заведите отдельную дебетовую карту для платежей в интернете и кладите на нее нужную сумму перед оплатой
- 3 Всегда проверяйте адреса электронной почты и сайтов – они могут отличаться от официальных лишь парой символов
- 4 Не переходите по ссылкам от незнакомцев – сразу удаляйте сомнительные сообщения
- 5 Никому не сообщайте свои персональные данные



Подробнее о правилах кибергигиены читайте на fincult.info



Финансовая культура





Банк России

ЧТО ДЕЛАТЬ, ЕСЛИ С КАРТЫ УКРАЛИ ДЕНЬГИ?

1 ЗАБЛОКИРОВАТЬ КАРТУ



- по номеру телефона банка на банковской карте или на официальном сайте
- через мобильное приложение
- через личный кабинет на официальном сайте банка
- в отделении банка

2 НАПИСАТЬ ЗАЯВЛЕНИЕ О НЕСОГЛАСИИ С ОПЕРАЦИЕЙ



- Заявление должно быть написано:
- в течение суток после сообщения о списании денег
 - на месте в отделении банка

3 ОБРАТИТЬСЯ В ПОЛИЦИЮ



Чем больше людей подадут заявления, тем выше вероятность, что преступников поймают

КАК ОБЕЗОПАСИТЬ ДЕНЬГИ НА СЧЕТАХ?

НИКОМУ НЕ СООБЩАЙТЕ:

- срок действия карты и трехзначный код на ее оборотной стороне (CVV/CVC)
- пароли и коды из уведомлений
- логин и пароль от онлайн-банка

НЕ ПУБЛИКУЙТЕ

персональные данные в открытом доступе

УСТАНОВИТЕ

антивирусы на все устройства

КОДОВОЕ СЛОВО

называйте только сотруднику банка, когда сами звоните на горячую линию



Банк не компенсирует потери, если вы нарушили правила безопасного использования карты



Подробнее о правилах безопасности
читайте на fincult.info



Финансовая
культура