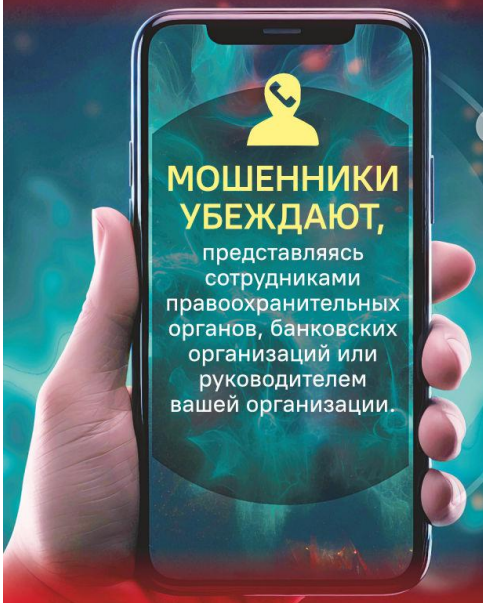
Кибербезопасность

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО:



МОШЕННИКИ УБЕЖДАЮТ, представляясь сотрудниками правоохранительных органов, банковских организаций или руководителем вашей организации.

- **Получить кредит,** чтобы отменить якобы оформленный неизвестными на ваше имя другой кредит и перевести деньги на специальный счет
- **Установить программное обеспечение,** якобы для предотвращения мошеннической атаки на ваш счет
- **Перевести накопления** на якобы безопасный счет, чтобы не изъяли при обыске
- **Передать личные данные и код из смс,** такие сведения предоставляют мошенникам доступ к счету или сервису

ОСТОРОЖНО! МОШЕННИЧЕСТВО!

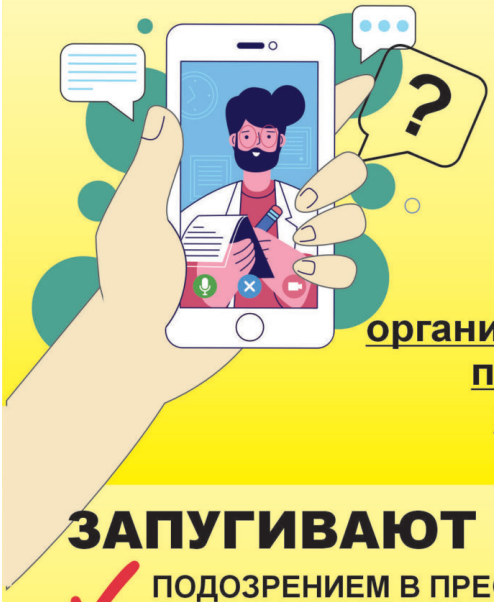
В СОЦИАЛЬНЫХ СЕТЯХ И НА ТОРГОВЫХ ПЛОЩАДКАХ:

- **Перевести предоплату за несуществующий товар** в лжемагазине или по измененным реквизитам банка
- **Перейти по поддельной ссылке** банковской системы и ввести личные данные (логин и пароль, номер и трехзначный код с оборотной стороны банковской карты, код из СМС, кодовое слово)
- **Перечислить деньги на карту или оплатить** родственнику, другу, любящему человеку
- **На поддельной бирже вложить деньги в проект,** якобы для получения пассивного дохода

МОШЕННИКИ УБЕЖДАЮТ, представляясь продавцами, друзьями, партнерами по бизнесу, руководителями инвестиционных проектов

Больше информации на сайте https://mvd.gov.by

Главное управление по противодействию киберпреступности КМ МВД Республики Беларусь



ТЕЛЕФОННЫЕ МОШЕННИКИ

представляются работниками:
коммунальных служб
(энергонадзора, водоканала, газовой службы),
организаций связи (Белтелеком, Белпочта, МТС, А1),
правоохранительных органов и банков
продавцами, инвесторами, брокерами

ЗАПУГИВАЮТ ИЛИ ЗАВЛЕКАЮТ:

- ПОДОЗРЕНИЕМ В ПРЕСТУПЛЕНИИ, ПРОВЕДЕНИЕМ ОБЫСКА
- СЛОЖНОЙ СИТУАЦИЕЙ С РОДСТВЕННИКОМ
- БЫСТРЫМ ЗАРАБОТКОМ И ПОЛУЧЕНИЕМ ПРИБЫЛИ
- ОКОНЧАНИЕМ ДЕЙСТВИЯ ПРИБОРА УЧЕТА
- ОКОНЧАНИЕМ ДЕЙСТВИЯ ДОГОВОРА ИЛИ УСЛУГИ СВЯЗИ
- ДЕЙСТВИЕМ АКЦИЙ, СКИДОК, ПРОВЕДЕНИЕМ РОЗЫГРЫШЕЙ

УБЕЖДАЮТ:

- ОФОРМИТЬ «ВСТРЕЧНЫЙ» КРЕДИТ
- СООБЩИТЬ ЛИЧНЫЕ ДАННЫЕ И КОД ИЗ УВЕДОМЛЕНИЯ
- ВНЕСТИ ПРЕДОПЛАТУ ЗА ТОВАР ИЛИ УСЛУГ
- ПЕРЕВЕСТИ ДЕНЬГИ НА «БЕЗОПАСНЫЙ» СЧЕТ
- СКАЧАТЬ И УСТАНОВИТЬ ФАЙЛ ПРИЛОЖЕНИЯ (*.APK)
- ВНЕСТИ СУММУ НА СЧЕТ ДЛЯ НАЧАЛА ИНВЕСТИРОВАНИЯ

УБЕДИТЕСЬ В ДОСТОВЕРНОСТИ ЗВОНКА

ПО ДРУГИМ КАНАЛАМ СВЯЗИ

Главное управление
по противодействию
киберпреступности
МВД Республики Беларусь

Телефонные мошенники

ПРЕДСТАВЛЯЮТСЯ:

- сотрудниками гос. органов и банков
- продавцами, инвесторами, брокерами
- работниками служб связи (Белпочта, Белтелеком, А1, МТС)
- работниками коммунальных служб (энергонадзора, водоканала, газовой службы)

УГРОЖАЮТ И ЗАПУГИВАЮТ:

- подозрением в преступлении и проведением обыска
- сложной ситуацией с родственником
- окончанием действия прибора учета или услуги

УБЕЖДАЮТ И ЗАСТАВЛЯЮТ:

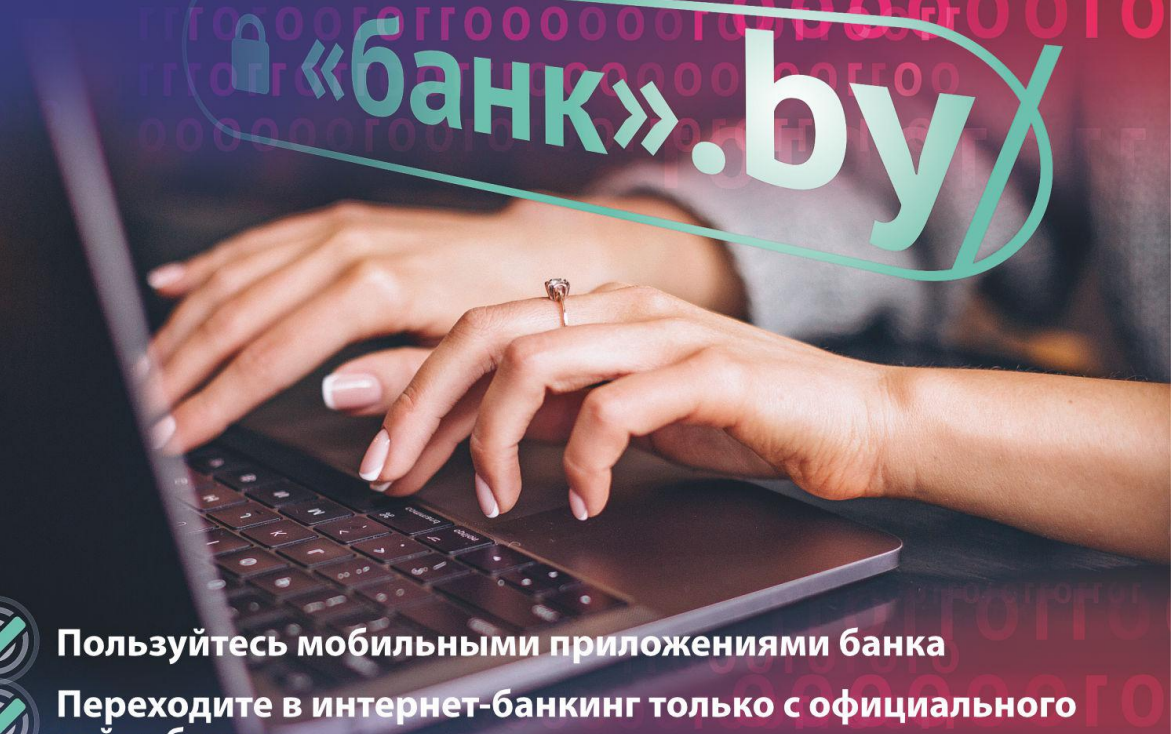
- под предлогом декларирования перевести деньги на “безопасный” счет
- внести предоплату за товар или взнос в инвестиционный проект
- передать личные данные и коды из сообщения, установить приложение

Не дайте себя обмануть!

Главное управление по противодействию киберпреступности
КМ МВД Республики Беларусь

ПОЛЬЗУЙСЯ БЕЗОПАСНО

«банк».by



- Пользуйтесь мобильными приложениями банка
- Переходите в интернет-банкинг только с официального сайта банка
- Проверяйте адрес интернет-банкинга в адресной строке, между последней точкой и первой наклонной чертой должно быть только так .by/
- Активируйте на карте, используемой для онлайн-платежей, услугу 3-D Secure (подтверждение платежей SMS-кодом)
- Не переходите в интернет-банкинг по ссылкам в поисковых системах
- Не используйте SMS-коды от банка и код с оборотной стороны карты для получения денежных средств
- Не переходите по ссылкам из сообщений для доступа к интернет-банкингу и иным сервисам или услугам

Главное управление
по противодействию
киберпреступности
КМ МВД Республики Беларусь

Больше информации
на сайте
https://mvd.gov.by

УВД МОГИЛЁВСКОГО ОБЛИСПОЛКОМА
ПРЕДУПРЕЖДАЕТ

КАК НЕ СТАТЬ ЖЕРТВОЙ ПРЕСТУПЛЕНИЯ?

БЛОКИРОВКА ICLOUD

ОСНОВНЫЕ СХЕМЫ ЗЛОУМЫШЛЕННИКОВ:

1 ПОМОЩЬ НЕИЗВЕСТНОМУ

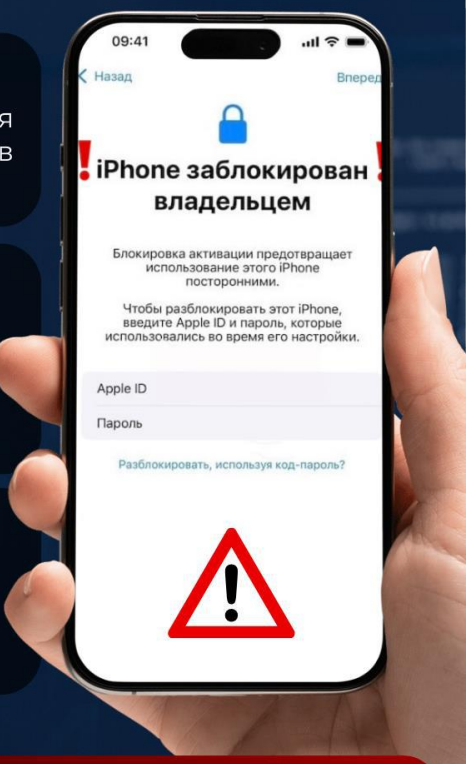
Неизвестные просят помощи для восстановления данных после чего просят авторизоватсья в предоставленную учётную запись iCloud

2 УСТАНОВКА ПРИЛОЖЕНИЙ

С целью установки бесплатной версии приложения (Яндекс Музыка, Spotify, Minecraft и т.п.), неизвестный предлагает помощь и просит авторизоваться в его учётную запись iCloud

3 УДАЛЁННАЯ РАБОТА

Для трудоустройства на вакансию удалённой работы неизвестный требует войти в “корпоративную” учётную запись iCloud



ВХОД В ЧУЖОЙ ICLOUD = ПОТЕРЯ ДОСТУПА К УСТРОЙСТВУ

Войдя в чужую учётную запись iCloud вы предоставляете злоумышленнику доступ к вашему устройству. Неизвестный, в чью учётную запсиь iCloud вы вошли, блокирует мобильное устройство в статусе “устройство потеряно/заблокировано”, после чего злоумышленник требует за разблокировку устройства деньги

КАК ИЗБЕЖАТЬ БЛОКИРОВКИ УЧЁТНОЙ ЗАПИСИ ICLOUD

- Не сообщайте никому реквизиты своей учётной записи
- Не вводите данные Apple ID на неизвестных рессурсах
- Не входите на своём устройстве в чужую учётную запись iCloud

БУДЬТЕ БДИТЕЛЬНЫ, НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!