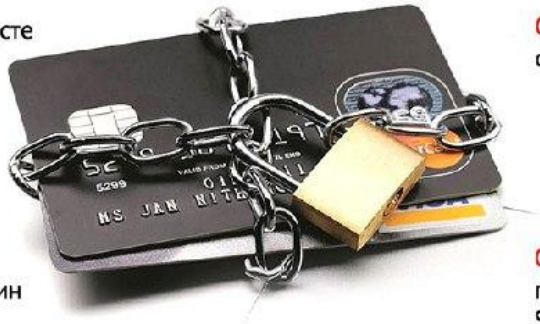
ВНИМАНИЕ!

ЗАЩИТИ СВОЮ БАНКОВСКУЮ КАРТУ

НЕЛЬЗЯ

Хранить пинкод вместе с картой

Сообщать CVV-код или отправлять его фото



Распространять личные данные, логин и пароль доступа к системе «Интернет-банкинг»

Сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации и т.д.

Сохрани эту информацию и поделись с другими

ОСТОРОЖНО!

МОШЕННИКИ В ИНТЕРНЕТЕ

НЕ следуй инструкциям незнакомцев, позвонившим с неизвестного номера

НЕ совершай никаких действий на смартфоне по просьбе посторонних лиц

НЕ сообщай неизвестным лицам свои персональные данные

НЕ переводи деньги незнакомым людям в качестве предоплаты

Сохрани эту информацию и поделись с другими

ВНИМАНИЕ!

ЦИФРОВАЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

УСТАНОВИТЕ АНТИВИРУС НА ВСЕ ВАШИ УСТРОЙСТВА

НЕ переходите по ссылкам и письмам от незнакомцев, не нажимайте на картинки и кнопки

НЕ сообщайте свои персональные данные и данные банковской карты

НЕ верьте обещаниям внезапных выигрышей

НЕ указывайте личную информацию в открытых источниках

НЕ используйте одинаковые пароли для всех аккаунтов

Сохрани эту информацию и поделись с другими

ВНИМАНИЕ!

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ СОЦСЕТЕЙ, МЕССЕНДЖЕРОВ И ЭЛЕКТРОННОЙ ПОЧТЫ!

НЕЛЬЗЯ

Размещать персональную и контактную информацию о себе в открытом доступе

Реагировать на письма от неизвестного отправителя

Использовать указание геолокации на фото в постах

Открывать подозрительное вложение к письму

Отвечать на агрессию и обидные выражения

Сохрани эту информацию и поделись с другими

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