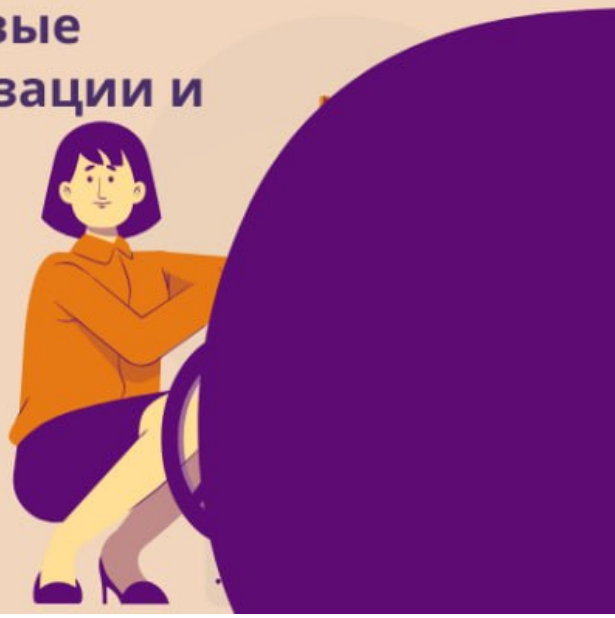
КАК ЗАЩИТИТЬ СВОЮ БАНКОВСКУЮ КАРТУ?!

НЕЛЬЗЯ

1. **Хранить** пинкод вместе с картой
2. **Распространять** личные данные, логин и пароль к системе “Интернет-банкинг”
3. **Сообщать** CVV-код или отправлять его фото
4. **Сообщать** данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации и т.д

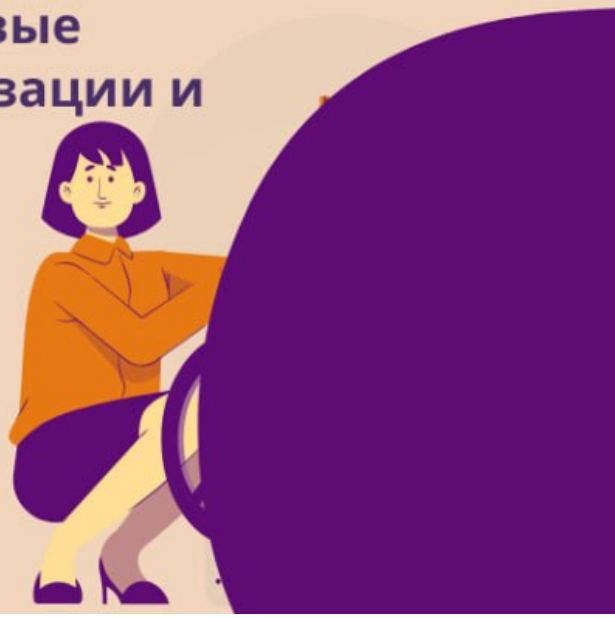


Отделение по противодействию киберпреступности криминальной милиции Ленинского РУВД г.Могилева

КАК ЗАЩИТИТЬ СВОЮ БАНКОВСКУЮ КАРТУ?!

НЕЛЬЗЯ

1. **Хранить** пинкод вместе с картой
2. **Распространять** личные данные, логин и пароль к системе “Интернет-банкинг”
3. **Сообщать** CVV-код или отправлять его фото
4. **Сообщать** данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации и т.д



Отделение по противодействию киберпреступности криминальной милиции Ленинского РУВД г.Могилева

ВИШИНГ

ЭТО ВИД МОШЕННИЧЕСТВА, ПРИ КОТОРОМ ЗЛОУМЫШЛЕННИКИ ЗВОНЯТ ВАМ ПО ТЕЛЕФОНУ, ПРЕДСТАВЛЯЯСЬ СОТРУДНИКАМИ БАНКОВ, ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ, ТЕХПОДДЕРЖКИ ИЛИ ДРУГИХ ОФИЦИАЛЬНЫХ СТРУКТУР, ЧТОБЫ ВЫМАНИТЬ ЛИЧНЫЕ ДАННЫЕ, КОДЫ ИЗ SMS И ДОСТУП К СЧЕТАМ.

КАК РАБОТАЮТ ВИШЕРЫ?

❌Звонок от "банка" – мошенник представляется сотрудником службы безопасности и сообщает, что с вашего счета пытаются снять деньги. Вас убеждают назвать данные карты или код из SMS "для отмены операции".

❌ Сообщение о родственнике в беде – мошенники говорят, что ваш близкий человек попал в ДТП или в полицию, и требуют срочно перевести деньги.

КАК ЗАЩИТИТЬСЯ?

✅ Никогда не сообщайте пароли, коды из SMS, CVC-код и другие конфиденциальные данные по телефону.

✅ Если звонят из "банка" – положите трубку и перезвоните на официальный номер, указанный на сайте банка.

✅ Не выполняйте срочные финансовые операции по просьбе звонящего.

✅ Будьте осторожны с номерами, похожими на номера официальных организаций.

✅ Настройте блокировку неизвестных и подозрительных номеров.

Отделение по противодействию киберпреступности криминальной милиции Ленинского РОВД г.Могилёва

ФИШИНГ

ЭТО ВИД ИНТЕРНЕТ-МОШЕННИЧЕСТВА, ПРИ КОТОРОМ ЗЛОУМЫШЛЕННИКИ ВЫМАНИВАЮТ КОНФИДЕНЦИАЛЬНЫЕ ДАННЫЕ, ТАКИЕ КАК ПАРОЛИ, НОМЕРА БАНКОВСКИХ КАРТ И ПЕРСОНАЛЬНЫЕ ДАННЫЕ.

КАК РАБОТАЮТ МОШЕННИКИ?

❌ Подделка сайтов – создают копии известных сайтов (банков, магазинов, соцсетей).
❌ Фальшивые письма – рассылают поддельные email-уведомления от "банков", "налоговых служб", "служб поддержки".
❌ Фальшивые акции и розыгрыши – обещают "подарки", если ввести личные данные.

КАК ЗАЩИТИТЬСЯ?

✅ Проверяйте URL сайтов перед вводом данных – всегда вводите адрес вручную.
✅ Не переходите по подозрительным ссылкам из email, мессенджеров и SMS.
✅ Используйте двухфакторную аутентификацию (2FA).
✅ Никогда не сообщайте пароли и коды из SMS, даже "банку".
✅ Используйте сложные пароли и уникальные комбинации для разных сайтов.
✅ Не пользуйтесь интернет-банком через общественные Wi-Fi сети.

Отделение по противодействию киберпреступности криминальной милиции Ленинского РОВД г.Могилёва

ВНИМАНИЕ!

ЦИФРОВАЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

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

УСТАНОВИТЕ АНТИВИРУС НА ВСЕ ВАШИ УСТРОЙСТВА

НЕ сообщайте свои персональные данные и данные банковской карты

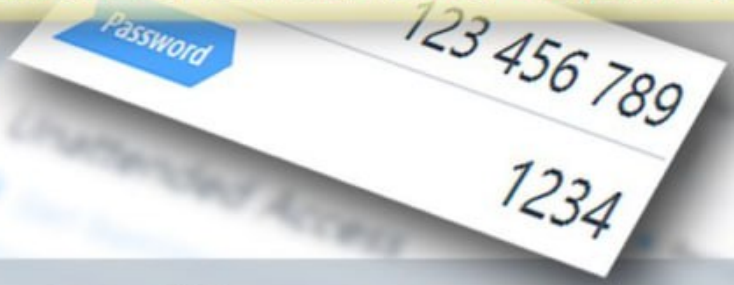
НЕ верьте обещаниям внезапных выигрышей

НЕ используйте одинаковые пароли для всех аккаунтов

НЕ указывайте личную информацию в открытых источниках

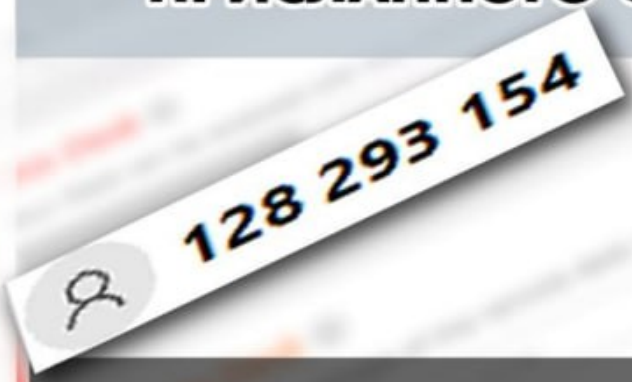
Сохрани эту информацию и поделись с другими

ВНИМАНИЕ!
ПОЯВИЛСЯ НОВЫЙ ВИД ВИШИНГА!



НЕ СОВЕРШАЙТЕ НИКАКИХ ДЕЙСТВИЙ НА СМАРТФОНЕ ПО ПРОСЬБЕ ПОСТОРОННИХ ЛЮДЕЙ! ТЕМ БОЛЕЕ, НЕ СООБЩАЙТЕ ИМ КОДЫ, ПАРОЛИ, И ДР.ИНФОРМАЦИЮ

НЕ СОХРАНЯЙТЕ В ПРИЛОЖЕНИЯХ И БРАУЗЕРАХ ПАРОЛИ, КОДЫ, ЛОГИНЫ. ПРЕСТУПНИК МОЖЕТ УЗНАТЬ КОД ИЗ ПРИСЛАННОГО SMS-СООБЩЕНИЯ



ПРЕСТУПНИК ПО ТЕЛЕФОНУ ПРОСИТ ВАС УСТАНОВИТЬ ПРОГРАММУ НА ТЕЛЕФОН ДЛЯ ДИСТАНЦИОННОГО ДОСТУПА И СООБЩИТЬ ЕМУ ПАРОЛЬ И КОД

УПРАВЛЕНИЕ «К» МВД БЕЛАРУСИ

6 правил информационной безопасности

главное управление по противодействию киберпреступности КМ МВД Беларуси

КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПНИКА

НАДЕЖНЫЕ ПАРОЛИ 01

НЕОБХОДИМО:

+ Создавать персональные (уникальные) пароли к разным сервисам
+ Использовать сложные пароли: минимум 10 символов, одновременно цифры, строчные и прописные символы, знаки пунктуации и другие символы
+ Доверять только проверенным менеджерам паролей

НЕ РЕКОМЕНДУЕТСЯ:

× Использовать повторения символов
× Хранить пароли на бумажных носителях
× Использовать в качестве пароля свой логин (имя пользователя, учетная запись, никнейм)
× Сохранять пароль автоматически в браузере
× Использовать биографическую информацию в пароле

БЕЗОПАСНЫЙ WI-FI 02

+ Отключить общий доступ к своей Wi-Fi точке, даже если у вас безлимитный Интернет
+ Использовать надежный (см. выше) пароль для доступа к вашей Wi-Fi точке
+ Деактивировать автоматическое подключение своих устройств к открытым Wi-Fi точкам

× Вводить свой логин и пароль доступа к учетной записи (странице) или системе банковского обслуживания при подключении к бесплатным (открытым) точкам Wi-Fi в кафе, транспорте, торговых центрах и т.д.

ПРОВЕРЕННЫЕ БРАУЗЕРЫ И САЙТЫ 03

+ Использовать специальное программное обеспечение (антивирус, расширение для браузера), чтобы избежать посещения сомнительных сайтов

× Переходить по непроверенным ссылкам
× Вводить информацию на сайтах, если соединение не защищено (нет https и 🔒)

ВНИМАНИЕ!

БЕРЕГИТЕ СВОИ ДЕНЬГИ!

УЧАСТИЛИСЬ СЛУЧАИ ХИЩЕНИЯ ДЕНЕГ С БАНКОВСКИХ КАРТ-СЧЕТОВ!

Если вам пришло сообщение в мессенджере, социальных сетях или по электронной почте...

... в котором говорится, что банковская карта заблокирована, и предлагается разблокировать ее, пройдя по ссылке...

... ни в коем случае не переходите по ссылке! Незамедлительно обращайтесь в службу безопасности банка!

Если вы получили сообщение о блокировке банковской карты:

- не переходите по прикрепленной ссылке, никуда не пересылайте свои данные;
- проверьте баланс своей карты в банкомате, инфокиоске, мобильном или интернет-банкинге;
- обратитесь в службу безопасности банка.

Главное управление по противодействию киберпреступности криминальной милиции МВД Республики Беларусь