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 указывайте личную информацию в открытых источниках

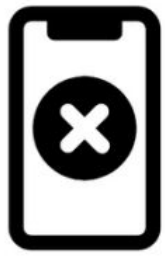
НЕ используйте одинаковые пароли для всех аккаунтов

Сохрани эту информацию и поделись с другими

ОСТОРОЖНО!
МОШЕННИКИ В ИНТЕРНЕТЕ

НЕ следуй инструкциям незнакомцев, позвонившим с неизвестного номера

НЕ сообщай неизвестным лицам свои персональные данные



НЕ совершай никаких действий на смартфоне по просьбе посторонних лиц

НЕ переводи деньги незнакомым людям в качестве предоплаты

Сохрани эту информацию и поделись с другими

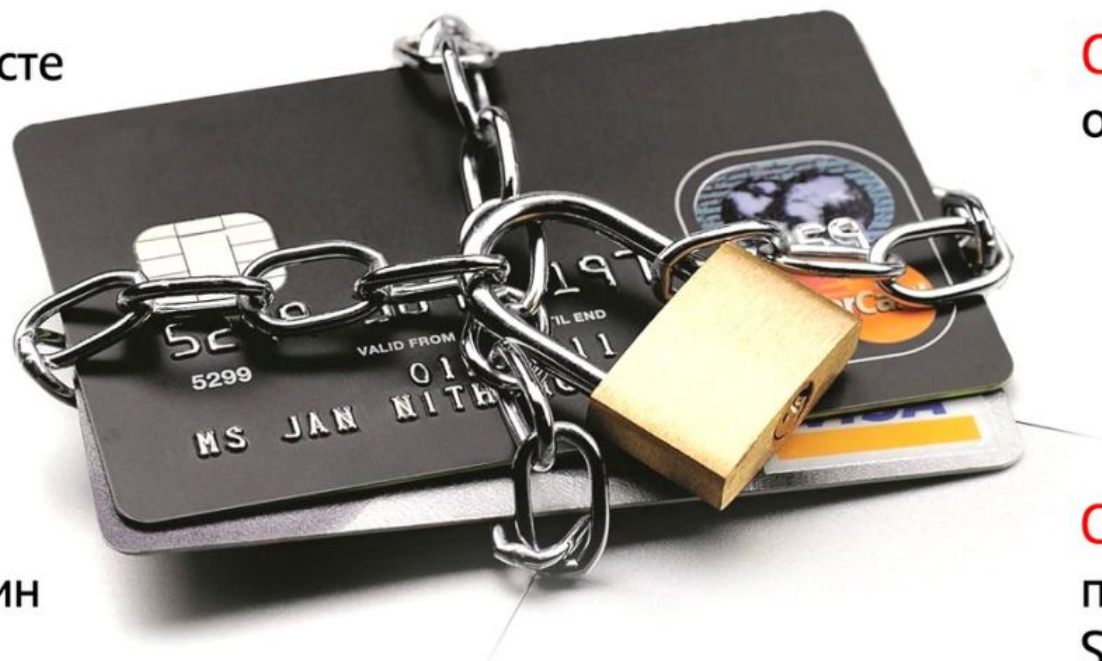
ВНИМАНИЕ!

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

ВНИМАНИЕ!
АТАКА НА ГОСОРГАНИЗАЦИИ!

СПЕЦИАЛИСТЫ ОТМЕЧАЮТ УВЕЛИЧЕНИЕ ЧИСЛА ФИШИНГОВЫХ АТАК НА ЭЛЕКТРОННЫЕ ПОЧТОВЫЕ ЯЩИКИ ГОСОРГАНИЗАЦИЙ!

ПРИ РАБОТЕ С ЭЛЕКТРОННОЙ ПОЧТОЙ

НЕ НАДО:

... ОТКРЫВАТЬ ВЛОЖЕНИЯ ПОЧТОВЫХ СООБЩЕНИЙ ОТ НЕИЗВЕСТНЫХ ОТПРАВИТЕЛЕЙ

... ПЕРЕХОДИТЬ ПО ССЫЛКАМ, ПОЛУЧЕННЫМ ОТ НЕИЗВЕСТНЫХ

... ХРАНИТЬ И ПЕРЕДАВАТЬ В ОТКРЫТОМ ВИДЕ ВАЖНЫЕ ДАННЫЕ (ЗААРХИВИРУЙТЕ ИХ И УСТАНОВИТЕ ПАРОЛЬ)

... ПРИ РЕГИСТРАЦИИ ЯЩИКА УКАЗЫВАТЬ БИОГРАФИЧЕСКИЕ ДАННЫЕ, ИСПОЛЬЗОВАТЬ ПРОСТЫЕ ПАРОЛИ И ПОВТОРЯЮЩИЕСЯ СИМВОЛЫ

НАДО:

... ПОДКЛЮЧИТЬ 2-ФАКТОРНУЮ АУТЕНТИФИКАЦИЮ

... РЕГУЛЯРНО МЕНЯТЬ ПАРОЛЬ ОТ ЭЛ.ПОЧТЫ

... ИСПОЛЬЗОВАТЬ НЕСКОЛЬКО ПОЧТОВЫХ ЯЩИКОВ ДЛЯ РАЗНЫХ РЕСУРСОВ (ПЕРЕПИСКА, РЕГИСТРАЦИЯ, ДЕЛОВАЯ ПОЧТА)

... ИСПОЛЬЗОВАТЬ УНИКАЛЬНЫЕ ПАРОЛИ ДЛЯ РАЗНЫХ ИНТЕРНЕТ-РЕСУРСОВ

... ВВОДИТЬ ИНФОРМАЦИЮ ТОЛЬКО НА ЗАЩИЩЕННЫХ САЙТАХ (HTTPS)

ВНИМАНИЕ!

ЕДИНСТВЕННЫЙ НАДЕЖНЫЙ СПОСОБ ЗАЩИТЫ - ЭТО ВАША БДИТЕЛЬНОСТЬ!

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД БЕЛАРУСИ

Как не стать жертвой киберпреступника.

ЗАЩИТА БАНКОВСКОЙ КАРТОЧКИ

Основные правила информационной безопасности по защите банковской карточки:

- хранить в тайне пин-код карты
- прикрывать ладонью клавиатуру при вводе пин-кода
- оформлять отдельную карту для онлайн-покупок
- деньги зачислять только в размере предполагаемой покупки
- использовать услугу 3-D Secure* и лимиты на максимальные суммы онлайн-операций
- скрыть CVV-код** на карте (трехзначный номер на обратной стороне), предварительно сохранив его
- подключить услугу "SMS-оповещение"

Не рекомендуется

- хранить пин-код вместе с карточкой/на карточке
- сообщать CVV-код или отправлять его фото
- распространять личные данные (например паспортные), логин и пароль доступа к системе "Интернет-банкинг"
- сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли***, код авторизации, пароли 3-D Secure

** Услуга 3-D Secure - для подтверждения онлайн-платежа держатель карточки вводит особый код (получает его в смс-сообщении на телефон).*

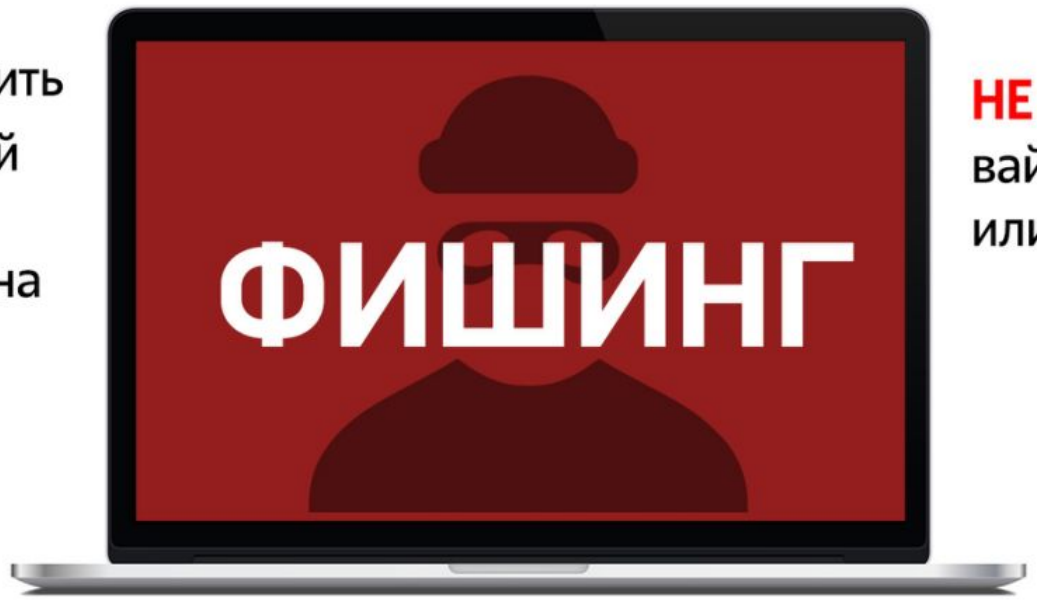
*** Код CVV - последние 3 цифры номера на обратной стороне платежной карты справа на белой линии, предназначенной для подписи. Код дает возможность распоряжаться средствами, находящимися на счету, физически не контактируя с картой.*

**** Сеансовый пароль - предоставляется при входе в интернет-банкинг, действителен лишь в течение одного платежного сеанса.*

Источник: МВД Беларуси.

ОСТОРОЖНО!
МОШЕННИКИ В ИНТЕРНЕТЕ

Не торопись переходить по ссылке, полученной от незнакомца: возможно, она ведет на фишинговый сайт



НЕ пользуйся открытыми вай-фай-сетями в кафе или на улице

Не спеши переходить по ссылке: введи адрес вручную

Фишинговая ссылка может прийти в мессенджере, по электронной почте, в смс-сообщении

Сохрани эту информацию и поделись с другими

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:

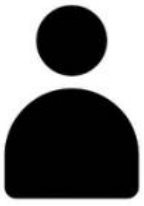
- не переходите по прикрепленной ссылке, никуда не пересылайте свои данные;
- проверьте баланс своей карты в банкомате, инфокиоске, мобильном или интернет-банкинге;
- обратитесь в службу безопасности банка.

Главное управление по противодействию киберпреступности криминальной милиции МВД Республики Беларусь

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

Отвечать на агрессию и обидные выражения

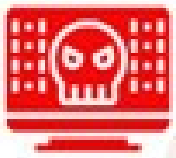
Открывать подозрительное вложение к письму

Сохрани эту информацию и поделись с другими

КАК ЗАЩИТИТЬ ПРЕДПРИЯТИЕ ОТ КИБЕРУГРОЗ

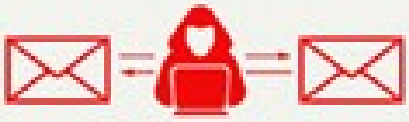
В 2018-2020 ГГ ПРЕДПРИЯТИЯМ ПРИЧИНЕН УЩЕРБ НА СУММУ БОЛЕЕ 2 МЛН. РУБЛЕЙ

ОСНОВНЫЕ СХЕМЫ КИБЕРПРЕСТУПНИКОВ



Шифрование коммерческой информации

Хакеры получают доступ к данным организации, превращают их в бессмысленный набор символов и оставляют письмо с предложением расшифровать данные за деньги.



Подмена реквизитов для перевода средств

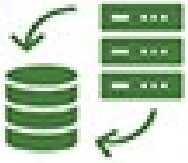
Эта криминальная схема используется в длительных и успешных деловых отношениях белорусской фирмы и зарубежного контрагента, которые активно контактируют по электронной почте. Злоумышленники получают доступ к одному из ящиков, участвующих в переписке. Когда у компаний намечается крупная сделка, со взломанного email предприятия (или же другой электронной почты с максимально похожим адресом) хакеры высылают письмо, в котором от имени юрлица уведомляют партнеров об изменении реквизитов для перевода средств.

Фишинговое письмо

На электронную почту учреждения приходит письмо с вложением-вредоносом, способным превращать ценную для компании информацию в бесполезный набор символов.

КАК ЗАЩИТИТЬСЯ ОТ КИБЕРУГРОЗ

воспользоваться услугами профессионалов по защите данных



регулярно выполнять резервное копирование данных

пользоваться актуальными антивирусами

настроить специальное программное обеспечение, блокирующее таргетированные атаки на информационные системы

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД РБ

КРАЖИ ЧЕРЕЗ МОБИЛЬНЫЙ БАНКИНГ

РАЗНОВИДНОСТЬ КИБЕРПРЕСТУПЛЕНИЙ - КРАЖА ДЕНЕГ АБОНЕНТОВ СОТОВОЙ СВЯЗИ ЧЕРЕЗ МОБИЛЬНЫЙ БАНКИНГ.

- Злоумышленники ищут жертв в общественных местах или обращаются к знакомым и просят телефон, чтобы сделать звонок.
- Делая вид, что набирает номер, при помощи USSD-запроса или выхода в интернет преступник активирует услугу мобильного банкинга. С ее помощью можно совершить платежные операции с лицевого счета абонента и получить у оператора сотовой связи лимитированный микрозайм.
- Сумма, поступившая хозяину гаджета, и средства с баланса телефона переводятся на абонентские номера или банковские счета злоумышленника.

КАК ЗАЩИТИТЬ МОБИЛЬНОЕ УСТРОЙСТВО

- использовать ПИН-код, а также дополнительные способы блокирования устройства (графический ключ, пароль, отпечаток пальца и др.);
- своевременно обновлять операционную систему устройства, антивирус;
- устанавливать приложения из PlayMarket, AppStore или только из проверенных источников;
- обращать внимание, к каким функциям гаджета запрашивает доступ приложение;
- включить встроенные функции устройства для определения его местонахождения;
- в случае утери (кражи) устройства, незамедлительно сменить пароли к интернет-банкингу, электронной почте и другим сервисам, а также обратиться в правоохранительные органы;
- при смене абонентского номера обязательно изменить привязку интернет-сервисов к новому номеру;
- при продаже устройства произвести его сброс до заводских настроек.

ЧЕГО ДЕЛАТЬ НЕЛЬЗЯ

- передавать незнакомым мобильный телефон или сим-карту, а в случае передачи - контролировать все действия, которые производятся с устройством;
- устанавливать приложения с низким рейтингом и отрицательными отзывами;
- перезванивать на незнакомые иностранные номера;
- хранить важную информацию на мобильном устройстве;
- делать полное снятие ограничения на устройстве.

Источник: МВД Беларуси.

Безопасный интернет для детей

СОХРАНИ ИНФОРМАЦИЮ

- не сообщай незнакомцам свой логин и пароль
- не открывай файлы из непроверенных источников
- не заходи на сайты, которые защита компьютера считает подозрительными

РОДИТЕЛИ! Научите детей пользоваться интернетом правильно!

ГЛАВНЫЕ ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

НЕ отправляй незнакомцам свои фото и видео

Злоумышленники могут узнать что-то нужное им о твоей жизни

НЕ встречайся с людьми, с которыми знаком только в интернете

За маской онлайн-собеседника может скрываться злоумышленник

НЕ сообщай в интернете свой реальный адрес и телефон

Злоумышленник может встретить тебя с недобрыми намерениями

НЕ отправляй личные данные для участия в конкурсах на малоизвестных сайтах

Информацией могут завладеть и воспользоваться недоброжелатели

Всегда важно помнить: неправильное поведение в интернете может принести большой вред.

Не дай себя обмануть!

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ

круглосуточный единый номер 102

БЕЗОПАСНЫЙ WI-FI

Рекомендуется:

- отключить общий доступ к своей точке Wi-Fi, даже если у вас безлимитный интернет;
- использовать надежный пароль для доступа к своей точке Wi-Fi;
- выключить автоматическое подключение своих устройств к точкам Wi-Fi.

ВАЖНО ПОНИМАТЬ,

что многие уязвимости в защите возникают из-за устаревшего ПО, поэтому обязательно установите все последние обновления для своего ноутбука или телефона.

Не рекомендуется:

- доверять открытым точкам Wi-Fi: именно такие сети используют злоумышленники для воровства личных данных пользователей;
- вводить свой логин и пароль доступа к учетной записи или системе банковского обслуживания при подключении к бесплатным точкам Wi-Fi.

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД БЕЛАРУСИ

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.

Управление по раскрытию преступлений в сфере высоких технологий МВД Республики Беларусь