

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.

© Инфографика





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!

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.



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! ОПЕРАЦИЯ «ВИШИНГ»!

АФЕРИСТ МОЖЕТ
ПОЗВОНИТЬ ПО ПОВОДУ
ТОВАРА НА ТОРГОВОЙ
ПЛОЩАДКЕ И
ПРЕДЛОЖИТЬ СДЕЛКУ С
ПРЕДОПЛАТОЙ



АФЕРИСТ МОЖЕТ
ПРЕДСТАВИТЬСЯ
БАНКОВСКИМ РАБОТНИКОМ И
ВЫМАНИТЬ
КОНФИДЕНЦИАЛЬНЫЕ
ДАННЫЕ



АФЕРИСТ СООБЩАЕТ,
ЧТО РОДСТВЕННИК
ЖЕРТВЫ ПОПАЛ В БЕДУ
И ЕМУ НУЖНА
ФИНАНСОВАЯ ПОМОЩЬ



ВИШИНГ - СПОСОБ МОШЕННИЧЕСТВА С ПОМОЩЬЮ ТЕЛЕФОНА, КОГДА МОШЕННИК ПОД РАЗЛИЧНЫМ ПРЕДЛОГОМ ПЫТАЕТСЯ ВЫМАНИТЬ ПЕРСОНАЛЬНУЮ ИНФОРМАЦИЮ ЖЕРТВЫ ДЛЯ ПОСЛЕДУЮЩЕГО ХИЩЕНИЯ ДЕНЕГ С ЕЕ БАНКОВСКОГО СЧЕТА

- НИКОГДА НЕ СООБЩАЙТЕ
НЕЗНАКОМОМУ СВОИ
ПЕРСОНАЛЬНЫЕ ДАННЫЕ

- НЕ ТОРОПИТЕСЬ ВЫПОЛНЯТЬ
ТО, ЧТО ОТ ВАС ПРОСИТ
СОБЕСЕДНИК. МОШЕННИКИ
ОЧЕНЬ ИЗОБРЕТАТЕЛЬНЫ И
УБЕДИТЕЛЬНЫ!



- НАДЕЖНО ЗАЩИЩАЙТЕ СВОИ
ДАННЫЕ (ДВУХФАКТОРНАЯ
АВТОРИЗАЦИЯ,
СМС-ОПОВЕЩЕНИЕ, И Т.Д.)

- В СЛУЧАЕ УТЕРИ ИЛИ КРАЖИ
КАРТЫ ЗАБЛОКИРУЙТЕ ЕЕ ПО
ТЕЛЕФОНУ ИЛИ В БАНКЕ

ГУПК КМ МВД РЕСПУБЛИКИ БЕЛАРУСЬ

ВНИМАНИЕ! ОТКРЫТЫЙ WI-FI

УГРОЗА для владельцев WI-FI:



УГРОЗА для пользователей:

- ЗЛОУМЫШЛЕННИК МОЖЕТ ВНЕДРИТЬ
ВРЕДОНОСНЫЕ ПРОГРАММЫ НА ВАШЕ
УСТРОЙСТВО ЧЕРЕЗ ОТКРЫТОЕ
WI-FI-СОЕДИНЕНИЕ

- ВАШ ТРАФИК МОЖЕТ БЫТЬ ПЕРЕХВАЧЕН
ЗЛОУМЫШЛЕННИКОМ, ВКЛЮЧАЯ
ПЕРСОНАЛЬНЫЕ ДАННЫЕ, РЕКВИЗИТЫ КАРТ, И
Т.Д.

- ВАШ КОМПЬЮТЕР МОЖЕТ БЫТЬ ПОДКЛЮЧЕН К
БОТ-СЕТИ, ОСУЩЕСТВЛЯЮЩЕЙ DDOS-АТАКИ,
ЧТО МОЖЕТ ПОВЛЕЧЬ УГОЛОВНУЮ
ОТВЕТСТВЕННОСТЬ

- ВВОДИМЫЕ ВАМИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ
МОГУТ БЫТЬ ПЕРЕХВАЧЕНЫ ХАКЕРОМ
(ПЛАТЕЖНАЯ ИНФОРМАЦИЯ, РЕВИЗИТЫ,
КОНТАКТЫ НА ТЕЛЕФОНЕ, ПАРОЛИ)

- ЗЛОУМЫШЛЕННИК МОЖЕТ ПОЛУЧИТЬ
ДОСТУП К ВАШИМ ПЕРСОНАЛЬНЫМ ДАННЫМ,
ФОТО-ВИДЕО, ХРАНЯЩИМСЯ НА УСТРОЙСТВЕ,
И Т.Д.

- ЗЛОУМЫШЛЕННИК МОЖЕТ ВЗЛОМАТЬ ВАШИ
ПРОГРАММЫ И СОЦИАЛЬНЫЕ СЕТИ,
СОВЕРШАЯ ЗАТЕМ РАЗЛИЧНЫЕ ДЕЙСТВИЯ ОТ
ВАШЕГО ИМЕНИ



**ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ
КРИМИНАЛЬНОЙ МИЛИЦИИ МВД РЕСПУБЛИКИ БЕЛАРУСЬ**



ВНИМАНИЕ, ОПАСНОСТЬ!

ВРЕДОНОСНЫЕ РАСШИРЕНИЯ ДЛЯ БРАУЗЕРОВ!

ЧТО УМЕЮТ ДЕЛАТЬ ВИРУСНЫЕ РАСШИРЕНИЯ?

- Размещать навязчивую рекламу в вашем браузере
- Совершать действия от имени пользователя в соцсетях (лайкать нужные материалы, делать рекламные посты)
- Перенаправлять на фишинговые или зараженные сайты
- Незаметно для пользователя кликать на вредоносные или рекламные ссылки, активировать скрипты
- Подсовывать пользователю для скачивания вирусное ПО, или веб-приложения
- Самовосстанавливаться после удаления
- Подменять контент, видоизменять кнопки, интерфейс страницы, оформление
- Следить за серфингом пользователя в интернете: куда он ходит, какие сайты посещает, чем интересуется



КАК ОНИ ПОПАДАЮТ В ВАШ КОМПЬЮТЕР?

- В комплекте с другими программами (“в нагрузку” с какими-то нужным файлом или программой)
- Выдает себя за полезное ПО (наряду с полезными функциями программа может иметь и несколько “неполезных”)
- Обманом и шантажом (мошенники не дают пользователю уйти с их сайта, пока тот не установит программу или приложение)

В КАКИХ БРАУЗЕРАХ ОНИ УСТАНАВЛИВАЮТСЯ?

Дополнительные расширения поддерживают такие браузеры:

GOOGLE CHROME

OPERA

MOZILLA FIREFOX

EDGE

SAFARI

ЯНДЕКС.БРАУЗЕР

INTERNET EXPLORER

AMIGO, и др.



КАК ЗАЩИТИТЬСЯ ОТ "ВРЕДОНОСА"?



- Внимательно следить за ПО, которое устанавливаете
- Устанавливайте расширения ТОЛЬКО из официальных источников!
- Проверяйте права доступа, которые запрашивает приложение
- Используйте браузер со встроенной защитой
- Быть бдительным при открытии файлов *.exe, .vbs, .scr
- Удалите все подозрительные файлы и расширения, затем просканируйте компьютер
- Если расширение появляется и после удаления - удалите приложение и создайте новый ярлык браузера
- Обновите антивирус и просканируйте компьютер. Если антивирус не помог - восстановите систему до более ранней версии
- В крайнем случае, напишите разработчику браузера

**ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ
КИБЕРПРЕСТУПНОСТИ КМ МВД РЕСПУБЛИКИ БЕЛАРУСЬ**



ФИШИНГ: КАК ЗАЩИТИТЬ СВОЙ БАНКОВСКИЙ СЧЕТ

НИКОГДА НЕ ПЕРЕХОДИТЕ ПО НЕЗНАКОМЫМ ССЫЛКАМ,
ПРИСЛАННЫМ ВАМ В МЕССЕНДЖЕРАХ, ПО ЭЛ.ПОЧТЕ, В SMS-СООБЩЕНИИ

Признаки явного мошенничества



Потенциальный покупатель вашего товара предлагает **перейти в мессенджер**, отказываясь общаться непосредственно на торговой площадке.

Наиболее крупные площадки для защиты своих пользователей ограничивают функцию отправки ссылок



Неизвестный в мессенджере присылает **ссылку для перехода на интернет-сайт**

под предлогом контроля карт-счета, просмотра баланса или проверки состояния оплаты.



Незнакомец предлагает передать ему полные данные вашей банковской карты, включая CVV-код либо логин и пароль от вашего интернет-банкинга.



ПОДРОБНОСТИ - ПО QR-ССЫЛКЕ

© Совместная инфографика:



ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД РЕСПУБЛИКИ БЕЛАРУСЬ