

ВАЖНО! Как не стать жертвой киберпреступлений

Достижения науки и техники, создание всемирной сети Интернет позволили преступности выйти на новый уровень и захватить киберпространство.

Теперь преступнику не нужен прямой контакт с жертвой, он может стать угрозой для каждого пользователя «глобальной паутины», крупных корпораций и целых государств.

Преступность в виртуальном пространстве – явление относительно новое, но часть преступлений, совершаемых в сфере высоких технологий, – это знакомые кражи, мошенничества, вымогательство.

Киберпреступность – незаконные действия, которые осуществляются людьми, использующими информационные технологии для преступных целей. Среди основных видов киберпреступности выделяют распространение вредоносных программ, взлом паролей, кражу номеров кредитных карт и других банковских реквизитов, а также распространение противоправной информации с использованием сети Интернет.

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, реквизиты, 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**

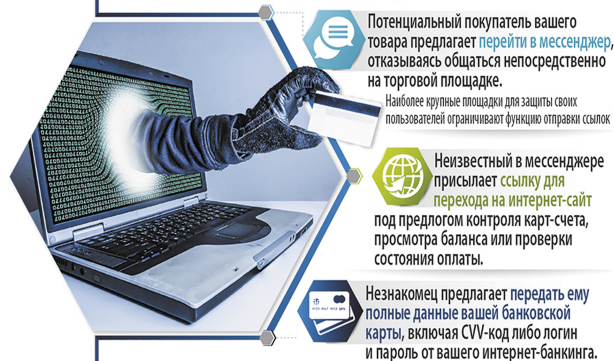


ФИШИНГ: КАК ЗАЩИТИТЬ СВОЙ БАНКОВСКИЙ СЧЕТ

НИКОГДА НЕ ПЕРЕХОДИТЕ ПО НЕЗНАКОМЫМ ССЫЛКАМ.

ПРИСЛАННЫМ ВАМ В МЕССЕНДЖЕРАХ, ПО ЭЛ.ПОЧТЕ, В SMS-СООБЩЕНИИ

Признаки явного мошенничества



ПОДРОБНОСТИ - ПО QR-ССЫЛКЕ

Совместная инфографика:



ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД РЕСПУБЛИКИ БЕЛАРУСЬ

Правила, которые помогут Вам не стать жертвой киберпреступлений:

- храните номер карточки и ПИН-коды в тайне;
- не используйте один пароль для всех интернет-ресурсов;
- к своей основной карте в Вашем банке выпустите дополнительную, которой будете расплачиваться в интернете. Туда легко можно будет переводить небольшие суммы денег, и в случае компрометации данных достаточно просто заблокировать ее;
- регулярно проверяйте состояние своих банковских счетов, чтобы убедиться в отсутствии «лишних» и странных операций;
- поставьте лимит на сумму списаний или перевода в личном кабинете банка;
- не перечисляйте деньги на электронные кошельки и счета мобильных телефонов при оплате покупок, если Вы не убедились в благонадежности лица/организации, которым предназначаются Ваши средства;

- не переводите денежные средства на счета незнакомых лиц;
- не перезванивайте и не направляйте ответные SMS, если Вам поступило сообщение о блокировании банковской карты. Свяжитесь с банком, обслуживающим Вашу карту;
- будьте осмотрительны в отношении писем с вложенными картинками, поскольку файлы могут содержать вирусы. Открывайте вложения только от известных Вам отправителей. И всегда проверяйте вложения на наличие вирусов, если это возможно;
- не переходите необдуманно по ссылкам, содержащимся в спам-рассылках. Удостоверьтесь в правильности ссылки, прежде чем переходить по ней из электронного письма;
- не заполняйте полученные по электронной почте формы и анкеты. Личные данные безопасно вводить только на защищенных сайтах;
- насторожьтесь, если от Вас требуют немедленных действий или представляется чрезвычайная ситуация. Это тоже может быть мошенничеством. Преступники вызывают у Вас ощущение тревоги, чтобы заставить Вас действовать быстро и неосмотрительно;
- не размещайте в открытом доступе и не передавайте информацию личного характера.

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 SMS-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 БЕЛТА

ВНИМАНИЕ! ОПЕРАЦИЯ «ВИШИНГ»!

АФЕРИСТ МОЖЕТ
ПОВОНИТЬ 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,
SMS-ОПОВЕЩЕНИЕ, И Т.Д.)

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

ГУП КМ МВД РЕСПУБЛИКИ БЕЛАРУСЬ

