

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 БЕЛАТА

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,
СМС-ОПОВЕЩЕНИЕ, И Т.Д.)

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



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ 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

© ИНФОГРАФИКА:

SB.BY
БЕЛАРУСЬ СЕГОДНЯ

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД РЕСПУБЛИКИ БЕЛАРУСЬ



БЫТЬ ХАКЕРОМ: не развлечение, а преступление!



Уголовная ответственность за киберпреступления наступает:



Статья 212 УК Беларуси

с 14
лет

Хищение путем использования компьютерной техники или введения в компьютерную систему ложной информации наказывается вплоть до лишения свободы на срок **до 3 лет**.



Те же действия, совершенные **повторно или группой лиц по предварительному сговору**, наказываются лишением свободы на срок **до 5 лет**.



Если хищение **крупное**, то предусмотрено наказание в виде лишения свободы на срок **до 7 лет**.



За хищение, совершенное **организованной группой или в особо крупном размере**, грозит **до 12 лет** лишения свободы.



Статья 349 УК Беларуси

с 16
лет

Несанкционированный доступ к компьютерной информации, совершенный из корыстной или иной личной заинтересованности, либо группой лиц по предварительному сговору, наказывается вплоть до лишения свободы на срок **до 2 лет**.



За несанкционированный доступ к компьютерной информации, повлекший по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные **тяжкие последствия**, грозит наказание вплоть до лишения свободы на срок **до 7 лет**.