Внимание!

БАНКОВСКИЕ ТРОЯНЫ АТАКУЮТ ПРЕДПРИЯТИЯ

КАК ЗАЩИТИТЬСЯ

- Не открывать вложения от неизвестных источников
- Не оставлять в компьютере подключенным USB-ключ
- Не использовать служебные e-mail в личных целях
- Своевременно обновлять ПО, антивирус, браузеры и т.д.

Управление информации и общественных связей 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**.

Управление информации и общественных связей 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

МОШЕННИЧЕСКАЯ СХЕМА “ЧЕЛОВЕК ПОСЕРЕДИНЕ”:

ЗАЩИТИТЕ СВОЮ ЭЛЕКТРОННУЮ ПОЧТУ!

НИКОМУ НЕ СООБЩАЙТЕ ПАРОЛИ, НЕ ИСПОЛЬЗУЙТЕ АВТОСОХРАНЕНИЕ В БРАУЗЕРЕ

ПРОВЕРЯЙТЕ ПРАВИЛЬНОСТЬ АДРЕСА КОНТРАГЕНТА

НЕ ИСПОЛЬЗУЙТЕ В ЛИЧНЫХ ЦЕЛЯХ СЛУЖЕБНЫЕ ЭЛ.ЯЩИКИ

ПРЕЖДЕ, ЧЕМ ОТПРАВИТЬ ПЕРЕВОД, СОЗВОНИТЕСЬ С ПОЛУЧАТЕЛЕМ

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.

© Инфографика БЕЛТА