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

Как не стать жертвой киберпреступника.

ЗАЩИТА БАНКОВСКОЙ КАРТЫ

Наиболее распространенные методы работы злоумышленников

выманивание реквизитов банковских платежных карт с использованием взломанных аккаунтов знакомых в социальных сетях

ЛЖЕПОКУПАТЕЛЬ - под видом покупателя злоумышленник связывается с продавцом, предлагает внести залог перед покупкой товара, а для получения денежного перевода предоставляет ему ссылку на мошеннический сайт, визуально похожий на официальный сайт банка

ВИШИНГ - представляясь по телефону сотрудником банка, злоумышленник пытается узнать у держателя карты конфиденциальную информацию (ее реквизиты, а также номер паспорта, личный идентификационный номер, логины, пароли, СМС-коды)

НЕ СООБЩАЙТЕ НИКОМУ

- информацию, размещенную на вашей банковской платежной карте (на обеих сторонах): номер, дату, код
- цифровые или буквенные коды
- паспортные данные

ЕСЛИ ВАМ ПОСТУПИЛ СОМНИТЕЛЬНЫЙ ЗВОНОК

- немедленно завершите разговор
- обратитесь в контакт-центр банка, выпустившего карту
- следуйте рекомендациям сотрудника банка

Для защиты денежных средств клиентов у банка есть вся необходимая информация

Работники банка по телефону не должны спрашивать ни реквизиты карты, ни паспортные данные

Не давайте никому свой мобильный телефон и предупредите об этом ваших близких, особенно детей и лиц пожилого возраста

Источник: Национальный банк Беларуси.

© Инфографика

ВНИМАНИЕ: ВИШИНГ!

Публичный центр правовой информации

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

АФЕРИСТ МОЖЕТ ПРЕДСТАВИТЬСЯ БАНКОВСКИМ РАБОТНИКОМ И ВЫМАНИТЬ КОНФИДЕНЦИАЛЬНЫЕ ДАННЫЕ

АФЕРИСТ МОЖЕТ СООБЩИТЬ, 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 НЕЗНАКОМЫМ ЛЮДЯМ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

- НЕ ТОРОПИТЕСЬ ВЫПОЛНЯТЬ ТО, ЧТО ОТ ВАС ПРОСЯТ СОБЕСЕДНИКИ. 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