УВАЖАЕМЫЕ ПАССАЖИРЫ!

ПОЗАБОТЬТЕСЬ О СОХРАННОСТИ СВОЕГО ИМУЩЕСТВА В ПУТИ СЛЕДОВАНИЯ ЖЕЛЕЗНОДОРОЖНЫМ ТРАНСПОРТОМ

Помните!

БОЛЬШИНСТВО КРАЖ СОВЕРШЕНО ПО ПРИЧИНЕ БЕСПЕЧНОСТИ ПОТЕРПЕВШИХ

Если в отношении Вас совершено противоправное деяние или Вы стали свидетелем преступления,
Вы можете сообщить об этом в УВД Витебского облисполкома по телефону

102

ВНИМАНИЕ!

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ СОЦСЕТЕЙ, МЕССЕНДЖЕРОВ И ЭЛЕКТРОННОЙ ПОЧТЫ!

НЕЛЬЗЯ

Размещать персональную и контактную информацию о себе в открытом доступе

Реагировать на письма от неизвестного отправителя

Использовать указание геолокации на фото в постах

Открывать подозрительное вложение к письму

Отвечать на агрессию и обидные выражения

Сохрани эту информацию и поделись с другими

ВНИМАНИЕ!

ЗАЩИТИ СВОЮ БАНКОВСКУЮ КАРТУ

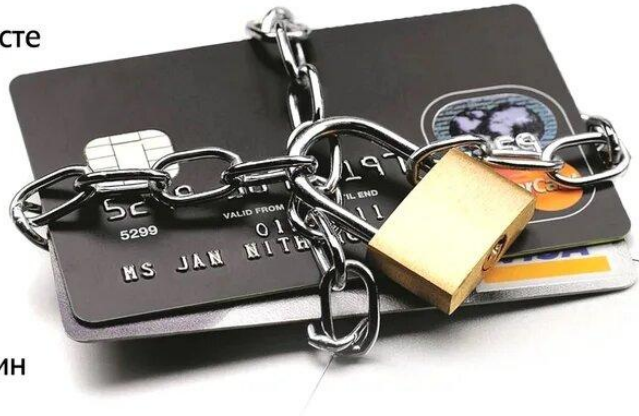
НЕЛЬЗЯ

123

Хранить пинкод вместе с картой

546

Сообщать CVV-код или отправлять его фото



Распространять личные данные, логин и пароль доступа к системе «Интернет-банкинг»

SMS

Сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации и т.д.

Сохрани эту информацию и поделись с другими

ВНИМАНИЕ!

ЦИФРОВАЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

НЕ переходите по ссылкам и письмам от незнакомцев, не нажимайте на картинки и кнопки

УСТАНОВИТЕ АНТИВИРУС НА ВСЕ ВАШИ УСТРОЙСТВА

НЕ сообщайте свои персональные данные и данные банковской карты

НЕ верьте обещаниям внезапных выигрышей

НЕ указывайте личную информацию в открытых источниках

НЕ используйте одинаковые пароли для всех аккаунтов

Сохрани эту информацию и поделись с другими

НЕ ДАЙ ОБМАНУТЬ СЕБЯ МОШЕННИКАМ!

1 МОШЕННИКИ ШЛЮТ «ПИСЬМА СЧАСТЬЯ» И ЖДУТ, КОГДА ВЫ ПОПОЛНИТЕ ИХ КОШЕЛЕК СВОИМИ ДЕНЬГАМИ!

НЕ ОТВЕЧАЙТЕ НА ТАКИЕ СМС!!!

- КАРТА ЗАБЛОКИРОВАНА. ИНФОРМАЦИЯ ПО ТЕЛ. ХХХХХ
- ВЫ ВЫИГРАЛИ АВТОМОБИЛЬ! ИНФОРМАЦИЯ ПО ТЕЛ. ХХХХХ
- ПОПОЛНЕНИЕ СЧЕТА НА 20 000 РУБЛЕЙ. ИНФОРМАЦИЯ ПО ТЕЛ. ХХХХХ
- НАПОМИНАЕМ ПОГАСИТЬ ЗАДОЛЖЕННОСТЬ ПО КРЕДИТУ. ИНФОРМАЦИЯ ПО ТЕЛ. ХХХХХ
- МАМА, У МЕНЯ ПРОБЛЕМЫ. ПОТОМ ВСЕ ОБЪЯСНЮ. ПЕРЕВЕДИ 300 РУБЛЕЙ НА ТЕЛ. ХХХХХ.

2 У МЕНЯ ЗАЗВОНИЛ ТЕЛЕФОН

МОШЕННИКИ ПРЕДЛАГАЮТ ПО АКЦИИ УДВОИТЬ ПЕНСИЮ. ПОМОЧЬ ПОПАВШЕМУ В ДТП ВНУКУ, ВНЕ ОЧЕРЕДИ ПРОЙТИ МЕДИЦИНСКОЕ ОБСЛЕДОВАНИЕ.

НЕ ПЕРЕДАВАЙТЕ И НЕ ПЕРЕЧИСЛЯЙТЕ ДЕНЬГИ НЕЗНАКОМЦАМ.
ПРОВЕРЬТЕ ПОСТУПИВШУЮ ИНФОРМАЦИЮ, ПОЗВОНИТЕ РОДСТВЕННИКАМ ИЛИ 02.

3 МОДНЫМ И НАИВНЫМ ИНТЕРНЕТ-ПОЛЬЗОВАТЕЛЯМ ПОСВЯЩАЕТСЯ!

В СОЦИАЛЬНЫХ СЕТЯХ, НА САЙТАХ «АВИТО», «ДРОМ.РУ» ДОВЕРЧИВЫМ ПОКУПАТЕЛЯМ ПРЕДЛАГАЮТ ВНЕСТИ ПРЕДОПЛАТУ ЗА ТОВАР, ОДНАКО В ДАЛЬНЕЙШЕМ СВЯЗЬ С ЛЖЕПРОДАВЦАМИ ПРЕКРАЩАЕТСЯ. У ГРАЖДАН, ПОДАВШИХ ОБЪЯВЛЕНИЯ

МОШЕННИКИ ПОД РАЗЛИЧНЫМИ ПРЕДЛОГАМИ ПЫТАЮТСЯ УЗНАТЬ CVV-код (3 цифры на оборотной стороне карты) ИЛИ ПОДКЛЮЧИТЬ К КАРТЕ УСЛУГУ "МОБИЛЬНЫЙ БАНК".
НЕ В КОЕМ СЛУЧАЕ НЕ СОВЕРШАЙТЕ ЭТИХ ДЕЙСТВИЙ!!!

4 РУЧКУ ПОЗОЛОТИ, ВСЮ ПРАВДУ РАССКАЖУ —

МОШЕННИКИ ПРЕДЛАГАЮТ ЧУДОДЕЙСТВЕННОЕ ИСЦЕЛЕНИЕ ОТ ПОРЧИ ИЛИ СГЛАЗА. ОДНАКО, ГЛАВНАЯ ИХ ЦЕЛЬ - ЗАВЛАДЕТЬ ВАШИМИ ДЕНЕЖНЫМИ СРЕДСТВАМИ, ЦЕННЫМИ ВЕЩАМИ И СКРЫТЬСЯ . **НЕ ВЕРЬТЕ «ЛЖЕЦЕЛИТЕЛЯМ» И ГАДАЛКАМ!!!**

МИЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

Как обезопасить себя от действий мошенников

- не пускайте в дом посторонних;
- требуйте предъявления документов у лиц, представляющихся работниками социальных, жилищно-эксплуатационных и иных служб. При отказе предъявить документы сообщите в милицию по телефону 102;
- не вступайте в разговор с лицами, которые предлагают снять порчу;
- не покупайте у незнакомых людей с рук электробытовые и иные товары;
- не разменивайте денежные купюры посторонним;
- ни под каким предлогом не передавайте свои вещи и деньги незнакомым лицам, особенно, для оказания ими услуг в приобретении квартиры, автомашины, строительных материалов, топлива, продуктов питания и других вещей, производства каких-либо работ, в целях благоприятного решения вопроса с должностными лицами о непривлечении к ответственности, сдаче экзаменов, решении жилищного вопроса и т.д.;
- не давайте в долг крупные суммы денег без должного юридического оформления и свидетелей.

Если же вы пострадали от действий злоумышленников немедленно сообщите об этом в милицию (102).

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ 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

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

ФИШИНГ: КАК ЗАЩИЩИТЬ 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: SB.BY БЕЛАРУСЬ СЕГОДНЯ

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД РЕСПУБЛИКИ БЕЛАРУСЬ

ОСТОРОЖНО!
МОШЕННИКИ В ИНТЕРНЕТЕ

Не торопись переходить по ссылке, полученной от незнакомца: возможно, она ведет на фишинговый сайт

НЕ пользуйся открытыми вай-фай-сетями в кафе или на улице

Не спеши переходить по ссылке: введи адрес вручную

Фишинговая ссылка может прийти в мессенджере, по электронной почте, в смс-сообщении

Сохрани эту информацию и поделись с другими


КАК SVPENG ПОХИЩАЛ ДЕНЬГИ ЧЕРЕЗ МОБИЛЬНЫЕ УСТРОЙСТВА
ЗАРАЖЕНИЕ МОБИЛЬНОГО УСТРОЙСТВА ВРЕДОНОСНОЙ ПРОГРАММОЙ SVPENG
ИСПОЛЬЗОВАНИЕ СМС-БАНКИНГА
Троянская программа перехватывает все СМС
Преступник переводит деньги себе на счет через СМС-банкинг
Троян перехватывает СМС-код от банка и подтверждает перевод
Жертва теряет деньги
ИСПОЛЬЗОВАНИЕ ФИШИНГОВЫХ САЙТОВ
Троян показывает поддельную страницу банка
Клиент вводит свой логин и пароль
Преступник переводит деньги на свой счет, используя эти данные
Троян перехватывает СМС-код от банка и подтверждает перевод
СБОР ДАННЫХ ВЛАДЕЛЬЦА КАРТЫ
Хакер дает команду показывать фишинговое окно при доступе в Google Play
Клиент банка указывает данные своей карты
На сервере проверяются достоверность данных карты по специальным алгоритмам
Жертва теряет деньги
GROUP IB
www.group-ib.ru

Памятка

«Чему научить ребенка в социальных сетях, чтобы защитить»

1. Критически оценивать все полученное в личных сообщениях и прочитанное в соцсетях.

2. Подозрительные сообщения и комментарии удалять, по ссылкам не переходить, на их авторов сразу жаловаться.

3. Не делиться личной информацией (ни в профиле, ни в личке, не ставить геометки).

4. Не пересылать спам друзьям.

5. Троллей и хейтеров игнорировать, их комментарии удалять, их самих отправлять в бан.

6. Уважительно относиться к собеседникам в онлайн пространстве.

7. Не отвечать на кибербуллинг, при этом сохранять доказательства, жаловаться на обидчиков в соцсети и сообщать взрослым.

8. Не вступать в группы смерти даже из любопытства.

9. Реагировать на фразы-маркеры типа «*только не говори родителям*».

10. Регулярно проверять настройки безопасности в телефоне и настройки конфиденциальности в соцсетях.

11. Думать о последствиях, когда выкладываешь свое или чужое видео/фото.

12. Помнить о рекламных технологиях и не доверять рекламе.

13. Не общаться с теми, кого не знаешь в реале, даже если это друг твоего друга.

14. Рассказывать о проблемных ситуациях родителям.

ВНИМАНИЕ! ЗАЩИТИТЕ СЕБЯ ОТ КИБЕРМОШЕННИЧЕСТВА!

МОШЕННИК МОЖЕТ ПРЕДСТАВИТЬСЯ:

сотрудником банка

сотрудником правоохранительных органов

родственником или другом из социальных сетей

И НАЗВАТЬ ПРИЧИНУ ЗВОНКА:

вам одобрен кредит

по вашему счету обнаружены мошеннические операции

подтверждение оформления доверенности на операции по вкладу

МОШЕННИК МОЖЕТ ПОПРОСИТЬ:

назвать номер, срок действия и трехзначный код на обороте карты, коды из смс-сообщений

войти в ваш интернет-банкинг и проверить не изменился ли баланс счета

назвать или напечатать цифры из смс-сообщения

установить программу или мобильное приложение для отмены операции по счету или защиты своего счета от мошенников

помочь разоблачить недобросовестного сотрудника банка

оформить кредит в банке

перевести деньги на «защищенный» счет

НЕ СООБЩАЙТЕ ДАННЫЕ КАРТЫ И КОДЫ ИЗ СМС

НЕ УСТАНАВЛИВАЙТЕ ПРОГРАММЫ по просьбе третьих лиц

НЕ ОФОРМЛЯЙТЕ КРЕДИТЫ

НЕ ПЕРЕВОДИТЕ ДЕНЬГИ НА «ЗАЩИЩЕННЫЙ» СЧЕТ

Больше информации на канале Цифровая грамотность в Telegram t.me/cifgram