ВНИМАНИЕ!
ПОЯВИЛСЯ НОВЫЙ ВИД ВИШИНГА!

Password 123 456 789 1234

Не совершайте никаких действий на смартфоне по просьбе посторонних людей! Тем более, не сообщайте им коды, пароли, и др.информацию

Не сохраняйте в приложениях и браузерах пароли, коды, логины. Преступник может узнать код из присланного SMS-сообщения

128 293 154

Преступник по телефону просит вас установить программу на телефон для дистанционного доступа и сообщить ему пароль и код

УПРАВЛЕНИЕ «К» МВД БЕЛАРУСИ

ПОЗАБОТЬТЕСЬ О БЕЗОПАСНОСТИ ПАРОЛЕЙ

БРУТФОРС - ЭТО ТИП ХАКЕРСКОЙ АТАКИ НА АККАУНТЫ ПОЛЬЗОВАТЕЛЕЙ, ПРИ КОТОРОМ СПЕЦИАЛЬНЫЙ СОФТ ПОДБИРАЕТ ПАРОЛЬ

НЕОБХОДИМО:

- Создавать уникальные пароли (разный регистр, чередующиеся буквы, цифры и символы)
- Менять пароли каждые 3 месяца
- Создавать разные пароли для различных сервисов
- Доверять только проверенных менеджерам паролей

НЕ СЛЕДУЕТ:

- Автоматически сохранять пароли в браузерах
- Использовать один и тот же пароль для различных аккаунтов
- Сообщать кому-либо свой пароль или логин
- Использовать биографическую информацию при создании пароля

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД БЕЛАРУСИ

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

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

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД РЕСПУБЛИКИ БЕЛАРУСЬ

ВНИМАНИЕ!

БЕРЕГИТЕ СВОИ ДЕНЬГИ!

УЧАСТИЛИСЬ СЛУЧАИ ХИЩЕНИЯ ДЕНЕГ С БАНКОВСКИХ КАРТ-СЧЕТОВ!

Если вам пришло сообщение в мессенджере, социальных сетях или по электронной почте...

... в котором говорится, что банковская карта заблокирована, и предлагается разблокировать ее, пройдя по ссылке...

... ни в коем случае не переходите по ссылке! Незамедлительно обращайтесь в службу безопасности банка!

Если вы получили сообщение о блокировке банковской карты:

- не переходите по прикрепленной ссылке, никуда не пересылайте свои данные;
- проверьте баланс своей карты в банкомате, инфокиоске, мобильном или интернет-банкинге;
- обратитесь в службу безопасности банка.

Главное управление по противодействию киберпреступности криминальной милиции МВД Республики Беларусь

ВНИМАНИЕ! ОТКРЫТЫЙ WI-FI

УГРОЗА
ДЛЯ ВЛАДЕЛЬЦЕВ WI-FI:

- 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

УГРОЗА
ДЛЯ ПОЛЬЗОВАТЕЛЕЙ:

- ВВОДИМЫЕ ВАМИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ МОГУТ БЫТЬ ПЕРЕХВАЧЕНЫ ХАКЕРОМ (ПЛАТЕЖНАЯ ИНФОРМАЦИЯ, РЕВИЗИТЫ, 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 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.

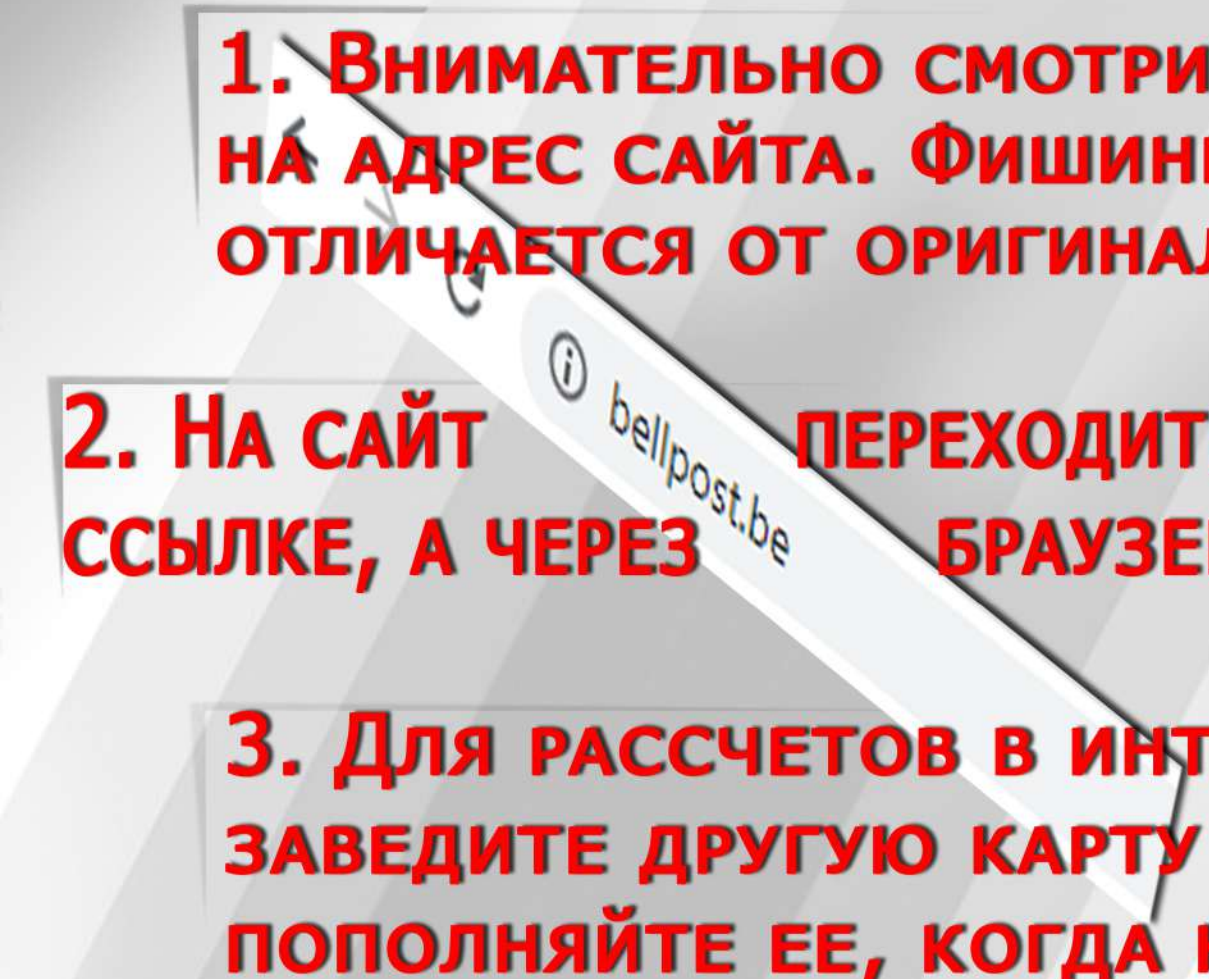
ПОДРОБНОСТИ - ПО QR-ССЫЛКЕ

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД РЕСПУБЛИКИ БЕЛАРУСЬ

МОШЕННИКИ СОЗДАЮТ ФИШИНГОВЫЕ КОПИИ САЙТА РУП «БЕЛПОЧТА»

СОБЛЮДАЙТЕ ОСНОВНЫЕ ПРАВИЛА «ЦИФРОВОЙ ГИГИЕНЫ»

1. ВНИМАТЕЛЬНО СМОТРИТЕ НА АДРЕС САЙТА. ФИШИНГОВЫЙ ОТЛИЧАЕТСЯ ОТ ОРИГИНАЛА!



2. НА САЙТ ПЕРЕХОДИТЕ НЕ ПО ССЫЛКЕ, А ЧЕРЕЗ БРАУЗЕР!

3. ДЛЯ РАССЧЕТОВ В ИНТЕРНЕТЕ ЗАВЕДИТЕ ДРУГУЮ КАРТУ И ПОПОЛНЯЙТЕ ЕЕ, КОГДА НАДО

Правильный адрес сайта РУП «Белпочта»:

belpost.by

Возможные фишинговые адреса:

bellpost.be
belpost.bj
belposta.bz
bellpochta.be

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ МВД БЕЛАРУСИ