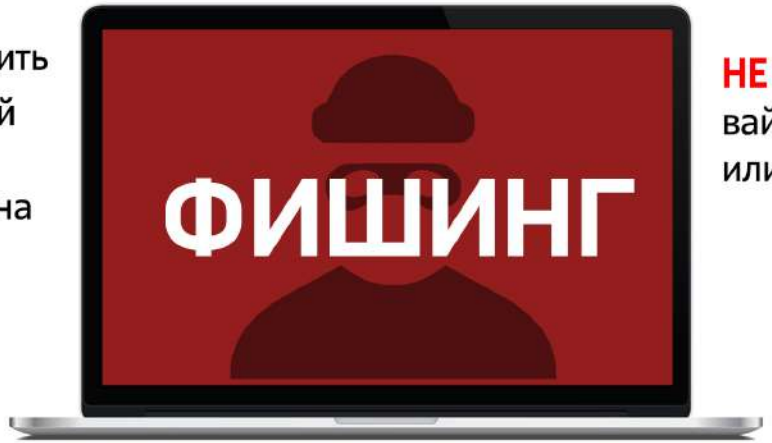
ОСТОРОЖНО!
МОШЕННИКИ В ИНТЕРНЕТЕ

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

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

Хранить пинкод вместе с картой

Сообщать CVV-код или отправлять его фото

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

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

УСТАНОВИТЕ АНТИВИРУС НА ВСЕ ВАШИ УСТРОЙСТВА

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

НЕ сообщайте свои персональные данные и данные банковской карты

НЕ верьте обещаниям внезапных выигрышей

НЕ используйте одинаковые пароли для всех аккаунтов

НЕ указывайте личную информацию в открытых источниках

Сохрани эту информацию и поделись с другими

10 ПРАВИЛ безопасного использования карты

1. ХРАНИТЕ ПИН-КОД ОТДЕЛЬНО ОТ КАРТЫ
2. НИКОГДА И НИКОМУ НЕ СООБЩАЙТЕ СВОЙ ПИН-КОД ИЛИ CVV
3. В СЛУЧАЕ ПОТЕРИ КАРТЫ ИЛИ ПИН-КОДА НЕМЕДЛЕННО ОБРАТИТЕСЬ В БАНК ДЛЯ БЛОКИРОВКИ КАРТЫ
4. ПОДКЛЮЧИТЕ СМС-УВЕДОМЛЕНИЯ ОБ ОПЕРАЦИЯХ ПО КАРТЕ
5. НИКОГДА И НИКОМУ НЕ СООБЩАЙТЕ ПАРОЛЬ ДЛЯ ДОСТУПА В МОБИЛЬНЫЙ ИЛИ ИНТЕРНЕТ-БАНК
6. ХРАНИТЕ ПОД РУКОЙ КОНТАКТНЫЙ НОМЕР СЛУЖБЫ ПОДДЕРЖКИ ВАШЕГО БАНКА
7. РЕГУЛЯРНО ОБНОВЛЯЙТЕ АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
8. НЕ ОСТАВЛЯЙТЕ КАРТУ БЕЗ ПРИСМОТРА. ПРИКРЫВАЙТЕ РУКОЙ КЛАВИАТУРУ ПРИ ВВОДЕ ПИН-КОДА КАК В БАНКОМАТЕ, ТАК И ПРИ ОПЛАТЕ КАРТОЙ В МАГАЗИНЕ
9. УСТАНОВИТЕ ДОСТУПНЫЙ ЛИМИТ СПИСАНИЙ ПО КАРТЕ В ДЕНЬ
10. ОБРАЩАЙТЕ ВНИМАНИЕ НА ВНЕШНИЙ ВИД БАНКОМАТА. ЕСЛИ У ВАС ВОЗНИКЛИ СОМНЕНИЯ, СООБЩИТЕ ОБ ЭТОМ СОТРУДНИКАМ БАНКА И ВОСПОЛЬЗУЙТЕСЬ ДРУГИМ БАНКОМАТОМ. ЗВОНИТЕ В БАНК ТОЛЬКО ПО ОФИЦИАЛЬНОМУ НОМЕРУ БАНКА, УКАЗАННОМУ НА ОБОРОТНОЙ СТОРОНЕ КАРТЫ

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

ВАМ ЗВОНЯТ ПО ТЕЛЕФОНУ И СООБЩАЮТ

ЧТО ДЕЛАТЬ:

ВАШ БЛИЗКИЙ РОДСТВЕННИК (СЫН, ВНУК, МУЖ) ПОПАЛ В БЕДУ (АВАРИЮ, ОГРАБЛЕН, АРЕСТОВАН), И ЧТОБЫ «ВЫПУТАТЬСЯ» ИЗ ИСТОРИИ, ОН ПРОСИТ ПЕРЕВЕСТИ ДЕНЬГИ ЧЕЛОВЕКУ, КОТОРЫЙ ПОМОЖЕТ	ПОПРОСИТЕ ЗВОНЯЩЕГО ПЕРЕДАТЬ ТРУБКУ ВАШЕМУ РОДСТВЕННИКУ; ПЕРЕЗВОНИТЕ ЕМУ САМИ И УБЕДИТЕСЬ, ЧТО С НИМ ВСЕ В ПОРЯДКЕ
У ВАС ОБНАРУЖЕНО ОПАСНОЕ ЗАБОЛЕВАНИЕ, ПРЕДЛАГАЮТ БЫСТРОЕ ОБСЛЕДОВАНИЕ ИЛИ ЛЕЧЕНИЕ «УНИКАЛЬНЫМ» ЛЕКАРСТВОМ	ПРЕДСТАВИТЕЛИ МЕДУЧРЕЖДЕНИЙ НЕ НАЗЫВАЮТ ДИАГНОЗЫ ПО ТЕЛЕФОНУ, НЕ «ВЕДИТЕСЬ» НА ПОДОБНЫЕ ЗВОНКИ
ВАМ ВЫДЕЛЕНА БЕСПЛАТНАЯ ПУТЕВКА В САНАТОРИЙ, НО НУЖНО НЕМНОГО ДОПЛАТИТЬ, НАПРИМЕР, ЗА ВЫБОР МЕСТА ОТДЫХА	НИКАКИХ ДОПЛАТ ОФИЦИАЛЬНЫЕ СОЦИАЛЬНЫЕ СЛУЖБЫ НИКОГДА НЕ ТРЕБУЮТ
ВЫ ВЫИГРАЛИ В ЛОТЕРЕЕ ИЛИ РОЗЫГРЫШЕ ПРИЗОВ, ДЛЯ ОФОРМЛЕНИЯ ПОТРЕБУЕТСЯ ВНЕСТИ НЕБОЛЬШИЕ ДЕНЬГИ	НЕ ВЕРЬТЕ, ВАМ НАВЕРНЯКА ЗВОНЯТ МОШЕННИКИ
С ВАШЕЙ БАНКОВСКОЙ КАРТЫ БЫЛА ПОПЫТКА ПЕРЕВЕСТИ ДЕНЬГИ, И БАНК ЕЕ ЗАБЛОКИРОВАЛ; ЗВОНИТ ЯКОБЫ ПРЕДСТАВИТЕЛЬ СЛУЖБЫ БЕЗОПАСНОСТИ БАНКА И ПРЕДЛАГАЕТ РАЗБЛОКИРОВАТЬ КАРТУ, НО ДЛЯ ЭТОГО ЕМУ НУЖНО СООБЩИТЬ ЕЕ НОМЕР И КОД, ВАШИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ	– СОТРУДНИКИ БАНКОВ НЕ ЗВОНЯТ КЛИЕНТАМ И НИКОГДА НЕ ТРЕБУЮТ НАЗВАТЬ СЕКРЕТНЫЕ СВЕДЕНИЯ О КАРТЕ ИЛИ СЧЕТЕ; – НИКОГДА НЕ НАЗЫВАЙТЕ И НЕ ВВОДИТЕ ПИН-КОД, ТРЕХЗНАЧНЫЙ КОД НА ОБРАТНОЙ СТОРОНЕ КАРТЫ ИЛИ ОДНОРАЗОВЫЙ ПАРОЛЬ ИЗ СМС; – НЕ НАБИРАЙТЕ НИКАКИХ КОМБИНАЦИЙ НА ТЕЛЕФОНЕ; – ПОЛОЖИТЕ ТРУБКУ И НЕ ПЕРЕЗВАНИВАЙТЕ В БАНК ВСТРЕЧНЫМ ЗВОНКОМ. МОЖНО ПЕРЕЗВОНИТЬ В БАНК ПО ОФИЦИАЛЬНОМУ НОМЕРУ (ОН УКАЗАН НА КАРТЕ) И СООБЩИТЬ О ЗВОНКЕ

ВАЖНО!

МОШЕННИКИ ВОРУЮТ БАЗЫ ДАННЫХ И НАЗЫВАЮТ ВАС ПО ИМЕНИ-ОТЧЕСТВУ, А В ТЕЛЕФОНЕ ВИДЕН НОМЕР ВАШЕГО БАНКА

БУДЬТЕ ГОТОВЫ И ПРОЯВИТЕ БДИТЕЛЬНОСТЬ

КАК НЕ СТАТЬ ЖЕРТВОЙ ВИШИНГА

Вишинг (голосовой фишинг - voice fishing) - один из методов мошенничества с использованием социальной инженерии. Злоумышленники, используя телефонную коммуникацию и играя определенную роль (сотрудника банка, покупателя и т. д.), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию (ее реквизиты, номер паспорта, личный идентификационный номер, логины, пароли, СМС-коды) или стимулируют к совершению определенных действий со своим карточным счетом/платежной картой.

Вам позвонили/прислали СМС "из банка" с неизвестного номера:

- не торопитесь следовать инструкциям;
- не сообщайте персональные данные неизвестным лицам, даже если они представляются сотрудниками банка;
- проверьте информацию, позвонив в контактный центр банка;
- незамедлительно обратитесь в правоохранительные органы.

Вам позвонили/прислали СМС с неизвестного номера с просьбой о помощи близкому человеку:

- не впадайте в панику, не торопитесь предпринимать действия по инструкциям неизвестных людей;
- задайте звонящему вопросы личного характера, помогающие отличить близкого вам человека от мошенника;
- под любым предлогом постарайтесь прервать контакт с собеседником, позвоните родным и узнайте, все ли у них в порядке.

Вы заподозрили интернет-продавца в недобросовестности:

необходимо оставаться бдительным, не принимать поспешных решений и при первых же подозрениях отказаться от покупки;

никогда не переводите деньги незнакомым людям в качестве предоплаты.

Источник: Следственный комитет Республики Беларусь.

© Инфографика БЕЛТА

Внимание! Мошенники!

Ваш внук попал в беду!
Срочно нужны деньги...
Вы выиграли автомобиль...
С вашей карты похищают деньги...
Ваша карта заблокирована...

Не переводите деньги на счет, который вам укажут
Не сообщайте номер карты, ее CVC-код, код из СМС, свои паспортные данные!

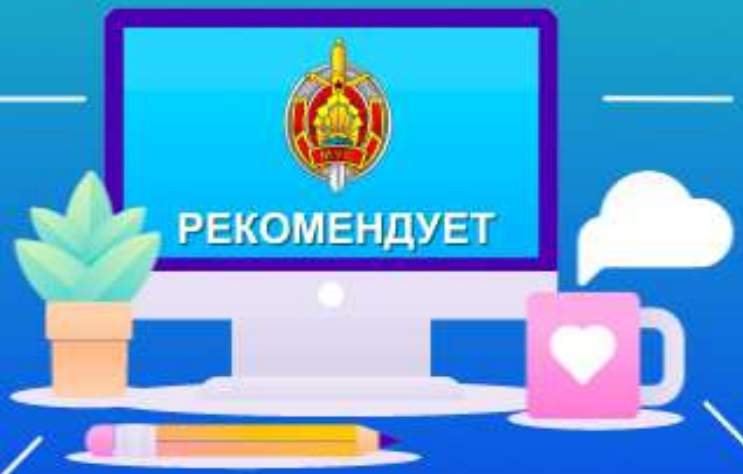
Помните: это кибермошенники!
Не дайте себя обмануть!

БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ

Всегда проверяй ссылки на ресурсы

Остерегайся назойливой рекламы

Используй сложные пароли



Не переходи по незнакомым ссылкам

Используй только безопасные платежи

Подключайся к безопасным сетям

Используй проверенные программы

КАК НЕ СТАТЬ ЖЕРТВОЙ ИНТЕРНЕТ-МОШЕННИКОВ

ПРИ ОПЛАТЕ ТОВАРОВ В ИНТЕРНЕТЕ:

используйте для платежей отдельную карту

после завершения сеанса оплаты рекомендуется выйти из браузера

переводите на указанную карту точную сумму денежных средств, которая необходима вам для оплаты

при работе на устройстве, с которого производится оплата, ни в коем случае не переходите по сомнительным ссылкам

производите оплату только с устройств (ноутбуков, планшетов, компьютеров, мобильных телефонов), защищенных антивирусным программным обеспечением*

не используйте для расчетов устройство, к которому имеют доступ более одного человека

в настройках используемого браузера нужно запретить сохранение логинов, паролей и другой конфиденциальной информации

**Антивирус должен быть включен, антивирусные базы и программа - обновляться, следует регулярно проводить антивирусное сканирование.*

Источник: Следственный комитет Республики Беларусь.

© Инфографика БЕЛТА

FinGramota

МОШЕННИКИ «НА КАРАНТИНЕ»: ВИШИНГ

ЛУЧШЕ НЕВЕЖЛИВО ПРЕРВАТЬ РАЗГОВОР, ЧЕМ ВЕЖЛИВО СООБЩИТЬ PIN-КОД КАРТЫ.

Сотрудники банка никогда не попросят у вас данные по карте. А чтобы убедиться, что звонок был от мошенников, нужно звонить на официальный номер вашего банка.

НЕ СПЕШИТЕ РАСКРЫВАТЬ ПЕРВОМУ ЗВОНЯЩЕМУ СВОИ ДАННЫЕ, В БАНКЕ ИХ ИТАК ЗНАЮТ.

Банки никогда не звонят сами, чтобы спросить по телефону: полный номер карточки; срок ее действия; CVC/CVV; логин и пароль к интернет-банкингу; кодовое слово, код из SMS-сообщения.

НЕ ПОДДАВАЙТЕСЬ ПАНИКЕ, ЕСЛИ ВАС ПОПЫТАЮТСЯ НАПУГАТЬ ТЕЛЕФОННЫЕ МОШЕННИКИ.

На паническое заявление о том, что с вашей картой серьезная проблема лучший ответ: «Сейчас позвоню или схожу в банк, чтобы проверить это лично». Будьте уверены – звонящий тут же отключится. Это очень распространенная уловка – напугать владельца карты.

НАИБОЛЕЕ РАСПРОСТРАНЁННЫЕ СХЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

«ВАША КАРТА ЗАБЛОКИРОВАНА»

SMS-сообщение о якобы заблокированной банковской карты, для разблокировки которой требуется сообщить ПИН-код вашей карты, либо провести определенные действия с помощью банкомата

«РОДСТВЕННИК В БЕДЕ»

Требование крупной суммы денег для решения проблемы с якобы попавшему в беду родственником

«ВЫ ВЫИГРАЛИ»

SMS-сообщение о том, что вы стали победителем и вам положен приз

«ВИРУСНАЯ АТАКА»

SMS-сообщение, содержащее ссылку на какой-либо интернет ресурс, содержащая вредоносную программу, дающую доступ мошенникам к вашей банковской карте

«ВАМ ПОЛОЖЕНА КОМПЕНСАЦИЯ»

Вам якобы положена компенсация за приобретаемые ранее некачественные БАДы либо иные медицинские препараты, для получения которой вам необходимо оплатить какие-либо пошлины или проценты

«ОШИБОЧНЫЙ ПЕРЕВОД СРЕДСТВ»

просят вернуть деньги за ошибочный перевод средств, дополнительно снимая средства со счета по чеку

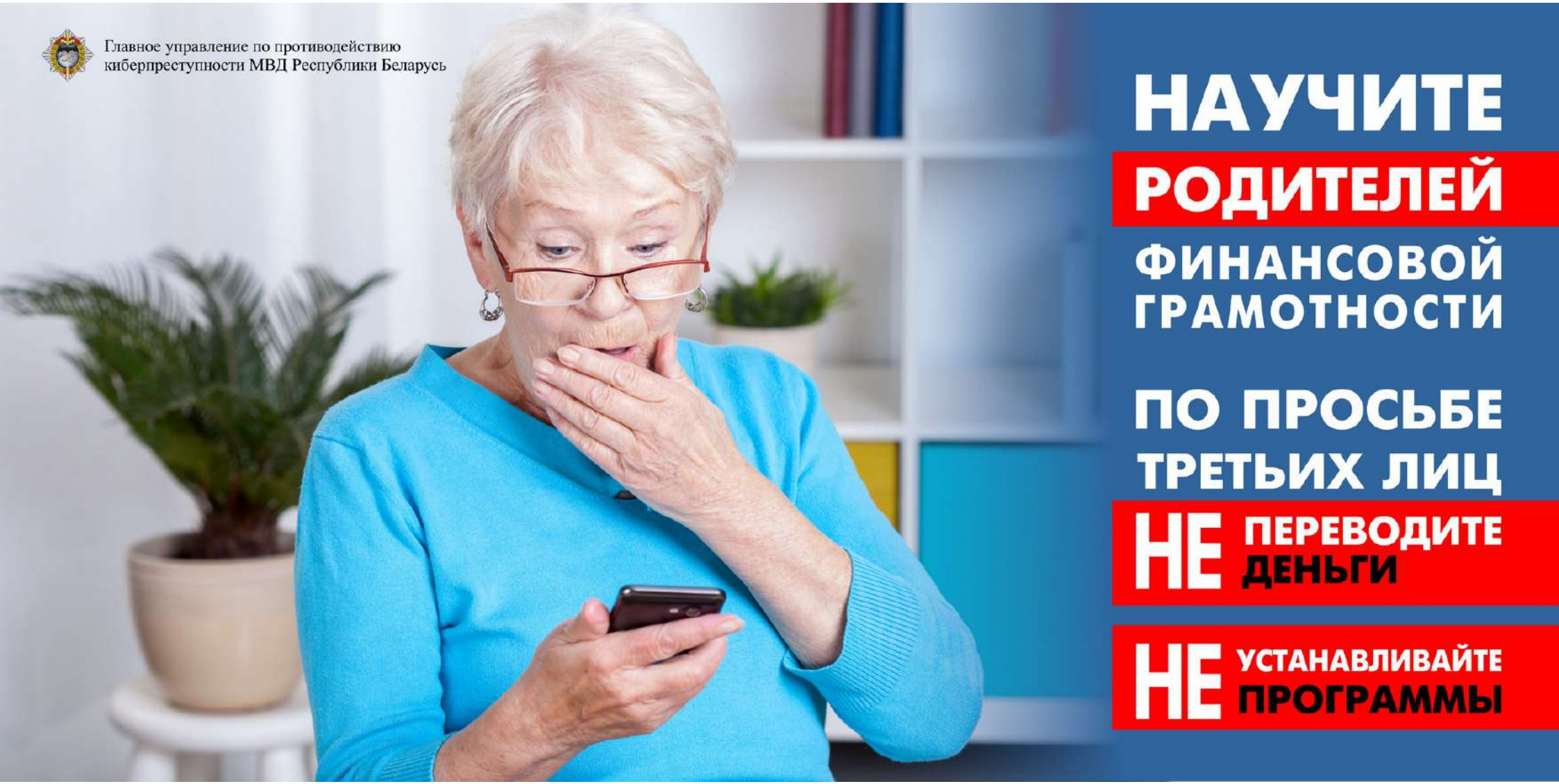
НАУЧИТЕ СВОИХ РОДИТЕЛЕЙ ФИНАНСОВОЙ ГРАМОТНОСТИ

ПО ПРОСЬБЕ ТРЕТЬИХ ЛИЦ

НЕ УСТАНАВЛИВАЙТЕ ПРОГРАММЫ

НЕ ПЕРЕВОДИТЕ ДЕНЬГИ

Главное управление по противодействию киберпреступности МВД Республики Беларусь


Главное управление по противодействию
киберпреступности МВД Республики Беларусь
НАУЧИТЕ
РОДИТЕЛЕЙ
ФИНАНСОВОЙ
ГРАМОТНОСТИ
ПО ПРОСЬБЕ
ТРЕТЬИХ ЛИЦ
НЕ ПЕРЕВОДИТЕ ДЕНЬГИ
НЕ УСТАНАВЛИВАЙТЕ ПРОГРАММЫ

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


ОСТОРОЖНО! ТЕЛЕФОННЫЕ МОШЕННИКИ!
НЕ ДАЙ СЕБЯ ОБМАНУТЬ!
Звонок службы безопасности банка
- Родственник в беде!
- Банковская карта заблокирована!
- С вашей банковской карты пытались снять деньги!
- НЕ РАЗГЛАШАЙТЕ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ И РЕКВИЗИТЫ БАНКОВСКИХ КАРТ И СЧЕТОВ
- НЕ ПЕРЕВОДИТЕ ДЕНЬГИ НЕЗНАКОМЫМ ЛЮДЯМ
ПРЕДУПРЕДИТЕ СВОИХ ДРУЗЕЙ И РОДСТВЕННИКОВ!

Памятка

Не передавать любой конфиденциальной информации о себе другим лицам, в том числе по телефону (номера банковских карт и коды доступа к ним, пароли, PIN-коды и т. п.). При возникновении каких-либо проблем **обращайтесь в службу поддержки** Вашего банка или оператора связи по телефону, указанному в договоре или на самой карте.

Не переводите денежные средства по звонкам и SMS-сообщениям, где Вам сообщают, что Ваш родственник попал в беду, в этом случае обязательно **перезвоните ему** и выясните обстоятельства произошедшего и только после этого предпринимайте какие-либо действия.

Игнорируйте поступающие звонки или SMS-сообщения о причитающемся Вам выигрыше, либо компенсации за лекарства и необходимости перевода денежных средств.

При получении SMS-сообщения или звонке лица, представившегося сотрудником Вашего оператора связи, о необходимости устранения каких-либо технических проблем и перечисления денежных средств, отправки SMS-сообщений с Вашими персональными данными, приобретения карт оплаты услуг, предложении перейти на более выгодный тариф, а также оплаты каких-либо услуг, штрафов и т. п. не предпринимайте указанных действий и **лично обратитесь в сервисный центр** Вашего оператора связи, или же справочную службу за разъяснениями, либо сообщайте по номеру «02», для любых операторов мобильной связи — «112».

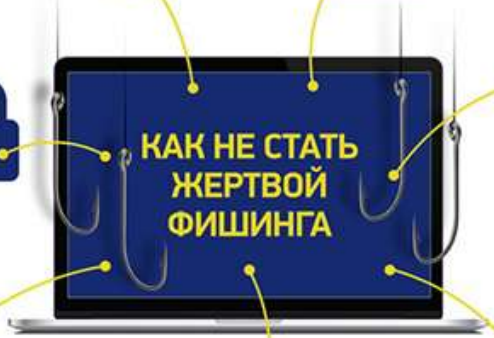
КАК НЕ СТАТЬ ЖЕРТВОЙ ФИШИНГА

Фишинг (англ. phishing от fishing "рыбная ловля, выуживание") - вид интернет-мошенничества для получения доступа к конфиденциальным данным пользователей - логинам и паролям. Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например от имени банков или внутри социальных сетей.

внимательно проверять ссылку, по которой собираетесь кликнуть: не перепутаны ли буквы в названии сайта

зачастую фальшивые письма и фальшивые сайты во всем повторяют дизайн настоящих

перед тем как вводить логин и пароль, нужно проверить, защищено ли соединение. Если перед адресом сайта вы увидите префикс https (где s означает secure) - безопасное



вместо того чтобы кликать по ссылке, следует ввести адрес вручную в новом окне браузера

даже если письмо или сообщение со ссылкой пришло от лучшего друга, все равно нужно помнить, что его тоже могли обмануть или взломать. Поэтому ведите себя не менее осторожно, чем при обращении со ссылками, пришедшими из неизвестного источника

обнаружив фишинговую операцию, необходимо сообщить о ней в банк (если письмо пришло от имени финансового учреждения) или в службу поддержки соцсети (если такие ссылки рассылает кто-то из пользователей) и т.д.

не заходите в онлайн-банки и тому подобные сервисы через открытые Wi-Fi-сети в кафе или на улице. Лучше воспользоваться мобильным интернетом или потерпеть, чем потерять все деньги на карте

Источник: Следственный комитет Республики Беларусь.

© Инфографика БЕЛТА