# Учреждение образования «Гомельский государственный медицинский университет»

## Профилактика и противодействие киберпреступности


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

# 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


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!

# 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.

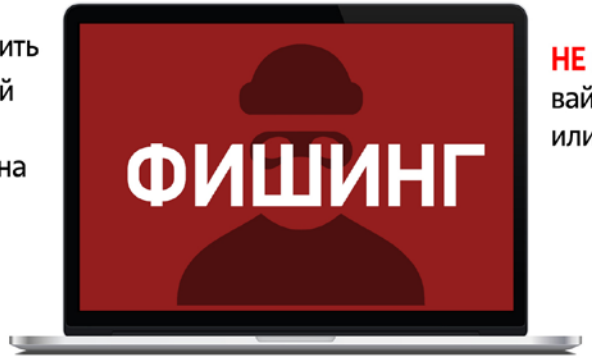
Источник: Следственный комитет Республики Беларусь.

# 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

# 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

**Использовать** указание геолокации на фото в постах

**Отвечать** на агрессию и обидные выражения

**Реагировать** на письма от неизвестного отправителя

**Открывать** подозрительное вложение к письму

**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

**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

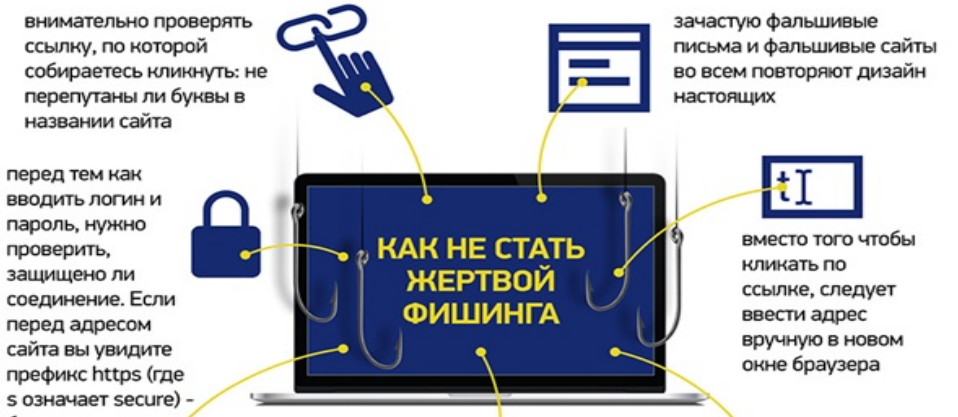
**НЕ указывайте** личную информацию в открытых источниках

**НЕ используйте** одинаковые пароли для всех аккаунтов

**Сохрани эту информацию и поделись с другими**

# 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.

# 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.