

Кибербезопасность

[Кто такие дропы? Отвечает участковый Гомельского РОВД – Гомельский районный исполнительный комитет](#)

<https://gomelisp.gov.by/wp-content/uploads/2024/12/1.-Vishing.mp4>

<https://gomelisp.gov.by/wp-content/uploads/2024/12/2.-Bezopasnost-v-internete.mp4>

https://gomelisp.gov.by/wp-content/uploads/2024/12/3.-Profilaktika_kiberprestuplenij.mp4

<https://gomelisp.gov.by/wp-content/uploads/2024/12/4.-Bezopasnye-paroli.mp4>

https://gomelisp.gov.by/wp-content/uploads/2024/12/bezopasnyj_internet_dlya_detej.mp4

<https://gomelisp.gov.by/wp-content/uploads/2024/12/Beregite-svoi-dengi.mp4>

<https://gomelisp.gov.by/wp-content/uploads/2024/12/Vishing.-Ne-popadis-na-udochku-moshennikov.mp4>

<https://gomelisp.gov.by/wp-content/uploads/2024/12/dropy.mp4>

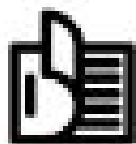
<https://gomelisp.gov.by/wp-content/uploads/2024/12/Miliciya-ne-zvonit-v-messendzherah.mp4>

https://gomelisp.gov.by/wp-content/uploads/2024/12/moshennichestvo_wildberries.mp4

https://gomelisp.gov.by/wp-content/uploads/2024/12/top-5_sovetov_kak_ne_stat_zhertvoj_moshennikov.mp4

<https://gomelisp.gov.by/wp-content/uploads/2024/12/Fishing.mp4>

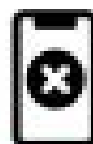
ОСТОРОЖНО! МОШЕННИКИ В ИНТЕРНЕТЕ



НЕ следуй инструкциям
незнакомцев, позвонившим
с неизвестного номера



НЕ сообщай неизвестным
лицам свои персональные
данные



НЕ совершай никаких
действий на смартфоне по
просьбе посторонних лиц



НЕ переводи деньги
незнакомым людям в
качестве предоплаты



Сохрани эту информацию и поделись с другими

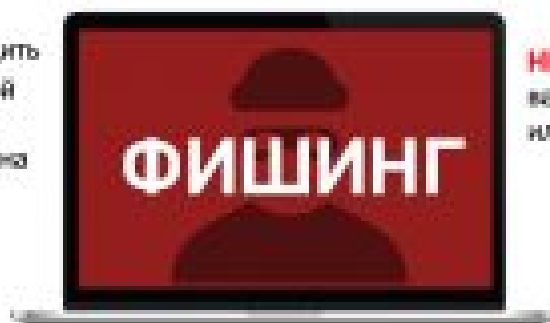
ОСТОРОЖНО! МОШЕННИКИ В ИНТЕРНЕТЕ



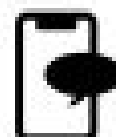
Не торопись переходить по ссылке, полученной от незнакомца: возможно, она ведет на фишинговый сайт



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



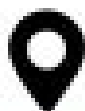
Сохрани эту информацию и поделись с другими

ВНИМАНИЕ!

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ СОЦСЕТЕЙ, МЕССЕНДЖЕРОВ И ЭЛЕКТРОННОЙ ПОЧТЫ!



Размещать персональную и контактную информацию о себе в открытом доступе



Использовать указание геолокации на фото в постах

НЕЛЬЗЯ



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



Хранить пинкод вместе с картой



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

НЕЛЬЗЯ



Сообщать CVV-код или отправлять его фото

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



НЕ верьте обещаниям внезапных выигрышей



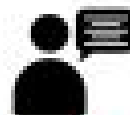
**УСТАНОВИТЕ АНТИВИРУС НА ВСЕ
ВАШИ УСТРОЙСТВА**



НЕ используйте одинаковые пароли для всех аккаунтов



НЕ сообщайте свои персональные данные и данные банковской карты



НЕ указывайте личную информацию в открытых источниках

Сохрани эту информацию и поделись с другими

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
-  оформить 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), логины и пароли доступа к системе "Интернет-банкинг"
-  сообщать данные, полученные в виде SMS-сообщений, скановые пароли***, код авторизации, пароли 3-D Secure

* Кодов 3-D Secure - для подтверждения онлайн-платежа держатель карточки вводит особый код (получается в смс-сообщении на телефон).

** Код CVV - последние 3 цифры номера на обратной стороне платежной карты справа от-белой линии, предназначенной для подписи. Код дает возможность распоряжаться средствами, находящимися на счету; физически не контактирует с картой.

*** Скановый пароль - предоставляется при входе в интернет-банкинг; действителен лишь в течение одного платежного сеанса.



Источник: МВД Беларуси

© Инфографика 

[Памятка для подростка. Осторожно – кибербуллинг!](#)

