

ПРОФИЛАКТИКА КИБЕР



ВНИМАНИЕ! АТАКА НА ГОСОРГАНИЗАЦИИ!

**СПЕЦИАЛИСТЫ ОТМЕЧАЮТ УВЕЛИЧЕНИЕ
ЧИСЛА ФИШИНГОВЫХ АТАК НА ЭЛЕКТРОННЫЕ
ПОЧТОВЫЕ ЯЩИКИ ГОСОРГАНИЗАЦИЙ!**

ПРИ РАБОТЕ С ЭЛЕКТРОННОЙ ПОЧТОЙ

НЕ НАДО:

... ОТКРЫВАТЬ ВЛОЖЕНИЯ
ПОЧТОВЫХ СООБЩЕНИЙ
ОТ НЕИЗВЕСТНЫХ
ОТПРАВИТЕЛЕЙ

... ПЕРЕХОДИТЬ ПО
СЫЛКАМ, ПОЛУЧЕННЫМ
ОТ НЕИЗВЕСТНЫХ

... ХРАНИТЬ И
ПЕРЕДАВАТЬ В ОТКРЫТОМ
ВИДЕ ВАЖНЫЕ ДАННЫЕ
(ЗААРХИВИРУЙТЕ ИХ И
УСТАНОВИТЕ ПАРОЛЬ)

... ПРИ РЕГИСТРАЦИИ
ЯЩИКА УКАЗЫВАТЬ
БИОГРАФИЧЕСКИЕ
ДАННЫЕ, ИСПОЛЬЗОВАТЬ
ПРОСТЫЕ ПАРОЛИ И
ПОВТОРЯЮЩИЕСЯ
СИМВОЛЫ

НАДО:

... ПОДКЛЮЧИТЬ
2-ФАКТОРНУЮ
АУТЕНТИФИКАЦИЮ

... РЕГУЛЯРНО МЕНЯТЬ
ПАРОЛЬ ОТ ЭЛ. ПОЧТЫ

... ИСПОЛЬЗОВАТЬ
НЕСКОЛЬКО ПОЧТОВЫХ
ЯЩИКОВ ДЛЯ РАЗНЫХ
РЕСУРСОВ (ПЕРЕПИСКА,
РЕГИСТРАЦИЯ, ДЕЛОВАЯ
ПОЧТА)

... ИСПОЛЬЗОВАТЬ
УНИКАЛЬНЫЕ ПАРОЛИ
ДЛЯ РАЗНЫХ
ИНТЕРНЕТ-РЕСУРСОВ

... ВВОДИТЬ
ИНФОРМАЦИЮ ТОЛЬКО НА
ЗАЩИЩЕННЫХ САЙТАХ
(HTTPS)

ВНИМАНИЕ!

**ЕДИНСТВЕННЫЙ НАДЕЖНЫЙ СПОСОБ ЗАЩИТЫ
- ЭТО ВАША БДИТЕЛЬНОСТЬ!**

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД БЕЛАРУСИ

Безопасный интернет для детей

**СОХРАНИ
ИНФОРМАЦИЮ**

*Не сообщай незнакомцам
свой логин и пароль*

*Не открывай файлы из
непроверенных источников*

*Не заходи на сайты, которые
защита компьютера считает
подозрительными*


 **НЕ отправляй незнакомцам
свои фото и видео**

Злоумышленники могут узнать что-то
нужное им о твоей жизни

**ГЛАВНЫЕ
ПРАВИЛА
ЦИФРОВОЙ
ГИГИЕНЫ**

 **НЕ встречайся с людьми,
с которыми знакомишься
только в интернете**
За маской онлайн-собеседника
может скрываться злоумышленник

 **НЕ сообщай в интернете
свой реальный
адрес и телефон**
Злоумышленник может встретить
тебя с недобрыми намерениями

 **НЕ отправляй личные данные
для участия в конкурсах
на малоизвестных сайтах**
Информацией могут завладеть и
воспользоваться недоброжелатели

**РОДИТЕЛИ!
научите детей
пользоваться
интернетом
правильно!**



**Всегда важно помнить: неправильное поведение
в интернете может принести большой вред.**

не дай себя обмануть!



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ

круглосуточный
единый
номер **102**

**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
ЭЛЕКТРОННЫЕ
ПОЧТЫ**

**ПРЕЖДЕ, ЧЕМ
ОТПРАВИТЬ ПЕРЕВОД,
СВЯЗАЙТЕСЬ С
ПОЛУЧАТЕЛЕМ**

БЕЗОПАСНЫЙ WI-FI

Рекомендуется:

-  отключить общий доступ к своей точке Wi-Fi, даже если у вас безлимитный интернет;
-  использовать надежный пароль для доступа к своей точке Wi-Fi;
-  выключить автоматическое подключение своих устройств к точкам Wi-Fi.

ВАЖНО ПОНИМАТЬ,

что многие уязвимости в защите возникают из-за устаревшего ПО, поэтому обязательно установите все последние обновления для своего ноутбука или телефона.

Не рекомендуется:

доверять открытым точкам Wi-Fi: именно такие сети используют злоумышленники для воровства личных данных пользователей;



вводить свой логин и пароль доступа к учетной записи или системе банковского обслуживания при подключении к бесплатным точкам Wi-Fi.



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 платёжного сеанса.



Источник: МВД Беларуси.

© Инфографика 



БУДЬТЕ ОСТОРОЖНЫ

ПРИ ВВОДЕ «ЛОГИНА» И ПАРОЛЯ

И ВНИМАТЕЛЬНЫ

ПРИ ПЕРЕХОДЕ ПО ССЫЛКАМ

Отдел по раскрытию преступлений в сфере высоких технологий
криминальной милиции УВД Минского облисполкома



ГЛАВНЫЕ ПРАВИЛА **ЦИФРОВОЙ ГИГИЕНЫ** ДЛЯ ДЕТЕЙ

Не сообщай личную информацию незнакомцу. И, вообще, в интернете не размещай сведения о себе и семье

Советуйся с родителями, как правильно поступить, если столкнулся с чем-то непонятным или пугающим

Помни, что в интернете надо быть очень-очень внимательным. Старайся избегать общения с незнакомыми людьми в онлайн-играх и соцсетях, не выполняй бездумно то, что они попросят тебя сделать



ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ МВД



НАУЧИТЕ СВОИХ РОДИТЕЛЕЙ ФИНАНСОВОЙ ГРАМОТНОСТИ

ПО ПРОСЬБЕ ТРЕТЬИХ ЛИЦ

НЕ УСТАНОВЛИВАЙТЕ
ПРОГРАММЫ

НЕ ПЕРЕВОДИТЕ
ДЕНЬГИ



Главное управление по противодействию
киберпреступности МВД Республики Беларусь

ВНИМАНИЕ! ОПЕРАЦИЯ «ВИШИНГ»!

АФЕРИСТ МОЖЕТ
ПОВОНИТЬ 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



КАК ЗАЩИТИТЬ ПРЕДПРИЯТИЕ ОТ КИБЕРУГРОЗ

В 2018 году более 100 белорусских субъектов хозяйствования пострадали от киберпреступлений.

ОСНОВНЫЕ СХЕМЫ КИБЕРПРЕСТУПНИКОВ



Шифрование коммерческой информации

Хакеры получают доступ к данным организации, превращают их в бессмысленный набор символов и оставляют письмо с предложением расшифровать данные за деньги.



Подмена реквизитов для перевода средств

Эта криминальная схема используется в длительных и успешных деловых отношениях белорусской фирмы и зарубежного контрагента, которые активно контактируют по электронной почте. Злоумышленники получают доступ к одному из ящиков, участвующих в переписке. Когда у компаний намечается крупная сделка, со wspomанного email предприятия (или же другой электронной почты с максимально похожим адресом) хакеры высылают письмо, в котором от имени юриста уведомляют партнеров об изменении реквизитов для перевода средств.



Фишинговое письмо

На электронную почту учреждения приходит письмо с вложением-вредоносом, способным превращать ценную для компании информацию в бесполезный набор символов.

КАК ЗАЩИТИТЬСЯ ОТ КИБЕРУГРОЗ



воспользоваться
услугами профессионалов
по защите данных



регулярно выполнять
резервное
копирование данных



пользоваться
актуальными
антивирусами



настроить специальное
программное обеспечение,
блокирующее таргетированные
атаки на информационные
системы



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**.

ВНИМАНИЕ, ОПАСНОСТЬ! ВРЕДОНОСНЫЕ РАСШИРЕНИЯ ДЛЯ БРАУЗЕРОВ!

ЧТО УМЕЮТ ДЕЛАТЬ ВИРУСНЫЕ РАСШИРЕНИЯ?

- Размещать навязчивую рекламу в вашем браузере
- Совершать действия от имени пользователя в соцсетях (лайкать нужные материалы, делать рекламные посты)
- Перенаправлять на фишинговые или зараженные сайты
- Незаметно для пользователя кликать на вредоносные или рекламные ссылки, активировать скрипты
- Подсовывать пользователю для скачивания вирусное ПО, или веб-приложения
- Самовосстанавливаться после удаления
- Подменять контент, видоизменять кнопки, интерфейс страницы, оформление
- Следить за серфингом пользователя в интернете: куда он ходит, какие сайты посещает, чем интересуется



Внимание!

БАНКОВСКИЕ ТРОЯНЫ АТАКУЮТ ПРЕДПРИЯТИЯ

КАК ЗАЩИТИТЬСЯ



Не открывать вложения от неизвестных источников



Не оставлять в компьютере подключенным USB-ключ



Не использовать служебные e-mail в личных целях



Своевременно обновлять ПО, антивирус, браузеры и т.д.

Управление информации и общественных связей МВД Республики Беларусь