



ВНИМАНИЕ: СВАТТИНГ



Сваттинг - новый для Беларуси вид преступления. Хулиганы-геймеры отправляют в экстренные службы ложное сообщение об опасности от имени другого игрока.

Во-первых, ложные сообщения отвлекают экстренные службы от оказания помощи тем, кто в ней действительно нуждается

Во-вторых, такими «разводами» геймеры могут доставить большие неприятности с законом своим визави

По всему миру полиция успешно устанавливает личности этих геймеров. В Беларуси за "сваттинг" предусмотрена ответственность по статье 340 Уголовного кодекса: вплоть до 7 лет лишения свободы!

А если геймер не достиг возраста привлечения к уголовной ответственности, то отвечать за него придется **родителям!**

... ПО ВСЕЙ СТРОГОСТИ ЗАКОНА!



ГУПК КМ МВД Республики Беларусь



научись пользоваться интернетом правильно!

СОХРАНИ
ИНФОРМАЦИЮ

БЕЗОПАСНЫЙ
INTERNET
ДЕТЯМ

1
2
3

**не сообщай незнакомцам
свой логин и пароль**

**не открывай файлы из
непроверенных источников**

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

не дай себя обмануть!



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ

круглосуточный
единый
номер

102

ВНИМАНИЕ! МОШЕННИЧЕСТВО!

1 

поступает звонок
с **неизвестного**
номера

2 

звонящий
представляется
вашим
родственником

3 

он говорит,
что **сбил человека**
или из-за него
человек
попал в **ДТП**

4 

он просит **денег**,
как **компенсацию**
вреда или
чтобы **«замять»** дело

5 

затем звонит
«милиционер»/
«следователь»
и подтверждает
легенду

6 

за деньгами
приезжает
курьер

Мама, папа, я
в беде!

Нужны деньги!
Срочно!

Что делать?

1. немедленно положить трубку
2. самому перезвонить родственнику
3. не передавать курьерам никаких денег
4. сообщить в милицию

не дай себя обмануть!



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ

круглосуточный
единый
номер

102



КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПНИКА

НАДЕЖНЫЕ ПАРОЛИ

01

НЕОБХОДИМО:

- + Создавать персональные (уникальные) пароли к разным сервисам
- + Использовать сложные пароли: минимум 10 символов, одновременно цифры, строчные и прописные символы, знаки пунктуации и другие символы
- + Доверять только проверенным менеджерам паролей

НЕ РЕКОМЕНДУЕТСЯ:

- ✗ Использовать повторения символов
- ✗ Хранить пароли на бумажных носителях
- ✗ Использовать в качестве пароля свой логин (имя пользователя, учетная запись, никнейм)
- ✗ Сохранять пароль автоматически в браузере
- ✗ Использовать биографическую информацию в пароле

БЕЗОПАСНЫЙ WI-FI

02


- + Отключить общий доступ к своей Wi-Fi точке, даже если у вас безлимитный Интернет
- + Использовать надежный (см. выше) пароль для доступа к вашей Wi-Fi точке
- + Деактивировать автоматическое подключение своих устройств к открытым Wi-Fi точкам

- ✗ Вводить свой логин и пароль доступа к учетной записи (странице) или системе банковского обслуживания при подключении к бесплатным (открытым) точкам Wi-Fi в кафе, транспорте, торговых центрах и т.д.

ПРОВЕРЕННЫЕ БРАУЗЕРЫ И САЙТЫ

03

- + Использовать специальное программное обеспечение (антивирус, расширение для браузера), чтобы избежать посещения сомнительных сайтов

- ✗ Переходить по непроверенным ссылкам
- ✗ Вводить информацию на сайтах, если соединение не защищено (нет https и )

**БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ**

04

НЕОБХОДИМО:

- + Подключить двухфакторную аутентификацию
- + Использовать минимум 2 типа e-mail адресов: закрытый (только для привязки устройств и средств их защиты) и открытый (для переписки, подписок и т.д.)
- + Использовать СПАМ-фильтры

НЕ РЕКОМЕНДУЕТСЯ:

- ✗ Реагировать на письма от неизвестного отправителя: скорее всего это спам или мошенники
- ✗ Открывать подозрительное вложение к письму: сначала позвоните отправителю и узнайте, что это за файл

ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ, СОЦСЕТЕЙ И МЕССЕНДЖЕРОВ

05

- + Устанавливать приложения только из PlayMarket, AppStore или из проверенных источников
- + Обращать внимание, к каким функциям гаджета приложение запрашивает доступ
- + Обмениваться сообщениями в соцсетях и мессенджерах, только полностью удостоверившись в личности собеседника, не реагируя на сомнительные просьбы и предложения
- ✗ Размещать персональную и контактную информацию о себе в открытом доступе
- ✗ Использовать указание геолокации на фото в постах
- ✗ Отвечать на обидные выражения и агрессию в соцсетях – лучше напишите об этом администратору ресурса
- ✗ Употреблять ненормативную лексику при общении
- ✗ Устанавливать приложения с низким рейтингом и отрицательными отзывами

ЗАЩИТА ДАННЫХ БАНКОВСКОЙ КАРТОЧКИ

06

- + Хранить в тайне пин-код карты
- + Прикрывать ладонью клавиатуру при вводе пин-кода
- + Оформить отдельную карту для онлайн-покупок и не держать на ней большие суммы
- + 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
- ✗ Хранить пин-код вместе с карточкой / на карточке
- ✗ Сообщать CVV-код или отправлять его фото
- ✗ Распространять свои паспортные данные (информацию личного характера, номер мобильного телефона), логин и пароль доступа к системе «Интернет-банкинг»
- ✗ Сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации, пароль 3-D Secure и т.д.



КАК ЗАЩИТИТЬ ПРЕДПРИЯТИЕ ОТ КИБЕРУГРОЗ

В 2018-2020 ГГ ПРЕДПРИЯТИЯМ ПРИЧИНЕН УЩЕРБ НА СУММУ БОЛЕЕ 2 МЛН. РУБЛЕЙ

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 взломанного 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

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.



ФИШИНГ: КАК ЗАЩИТИТЬ 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

© СОВМЕСТНАЯ ИНФОГРАФИКА:



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;

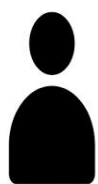


- обратитесь в службу безопасности банка.

**Главное управление по противодействию киберпреступности
криминальной милиции МВД Республики Беларусь**

ВНИМАНИЕ!

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ СОЦСЕТЕЙ, МЕССЕНДЖЕРОВ И ЭЛЕКТРОННОЙ ПОЧТЫ!



НЕЛЬЗЯ



Размещать персональную
и контактную
информацию о себе в
открытом доступе



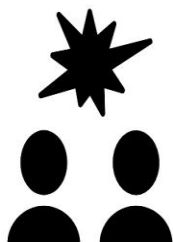
Реагировать на
письма от
неизвестного
отправителя



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