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

КАК ОНИ ПОПАДАЮТ В ВАШ КОМПЬЮТЕР?

- В комплекте с другими программами (“в нагрузку” с какими-то нужным файлом или программой)
- Выдает себя за полезное ПО (наряду с полезными функциями программа может иметь и несколько “неполезных”)
- Обманом и шантажом (мошенники не дают пользователю уйти с их сайта, пока тот не установит программу или приложение)

В КАКИХ БРАУЗЕРАХ ОНИ УСТАНАВЛИВАЮТСЯ?

Дополнительные расширения поддерживают такие браузеры:

GOOGLE CHROME	OPERA
MOZILLA FIREFOX	EDGE
SAFARI	ЯНДЕКС.БРАУЗЕР
INTERNET EXPLORER	AMIGO, и др.

КАК ЗАЩИТИТЬСЯ ОТ "ВРЕДОНОСА"?

- Внимательно следить за ПО, которое устанавливаете
- Устанавливайте расширения ТОЛЬКО из официальных источников!
- Проверяйте права доступа, которые запрашивает приложение
- Используйте браузер со встроенной защитой
- Быть бдительным при открытии файлов *.exe, .vbs, .scr
- Удалите все подозрительные файлы и расширения, затем просканируйте компьютер
- Если расширение появляется и после удаления - удалите приложение и создайте новый ярлык браузера
- Обновите антивирус и просканируйте компьютер. Если антивирус не помог - восстановите систему до более ранней версии
- В крайнем случае, напишите разработчику браузера

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД РЕСПУБЛИКИ БЕЛАРУСЬ

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**.

Управление информации и общественных связей МВД Республики Беларусь

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

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!
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 «замяты» дело
5. затем звонит «милиционер»/ «следователь» и подтверждает легенду
6. за деньгами приезжает курьер

Мама, папа, я в беде!

Нужны деньги! Срочно!

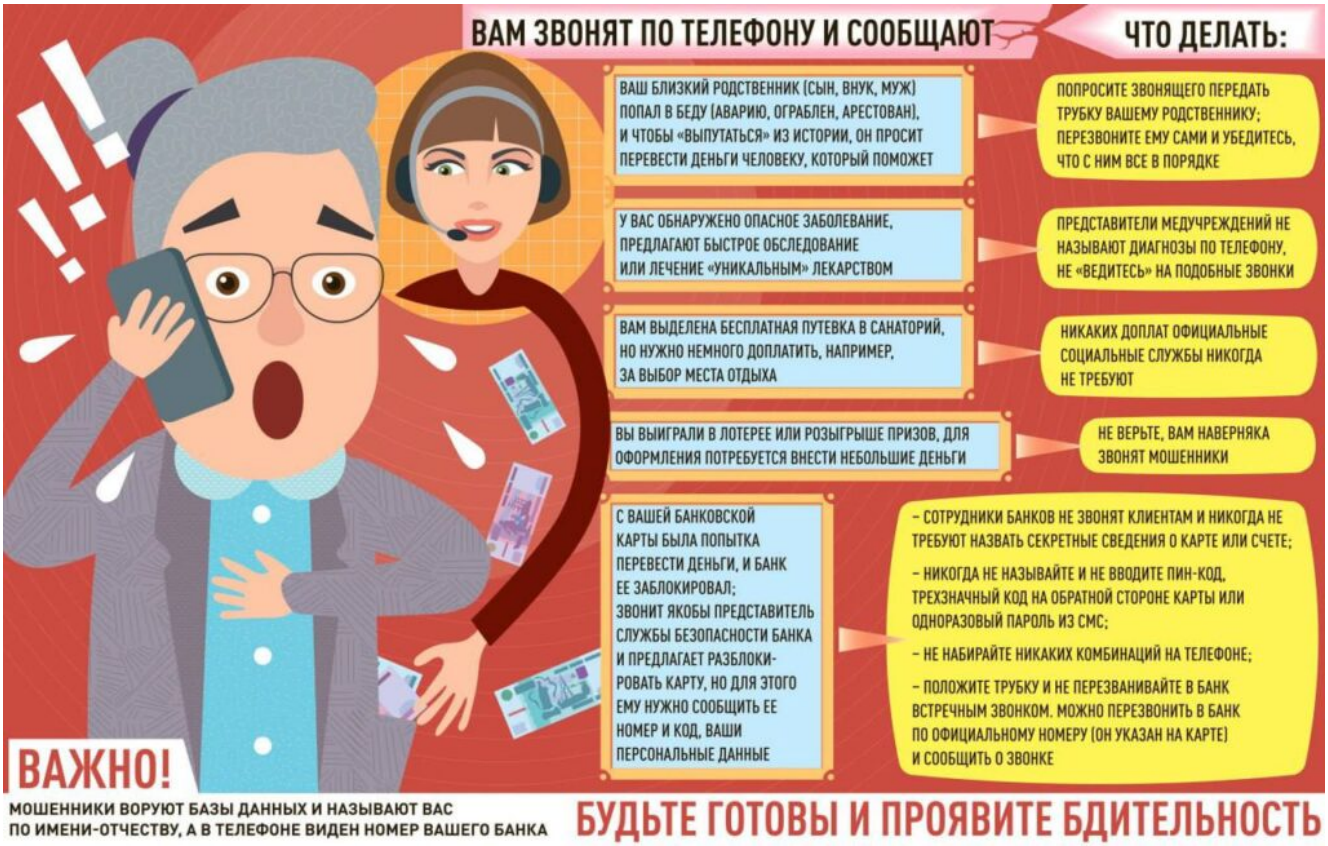
Что делать?

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


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