БЕЗОПАСНО СКАЧАТЬ ФАЙЛЫ ИЗ ИНТЕРНЕТА

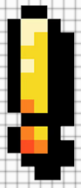
ФАЙЛЫ С РАСШИРЕНИЕМ .EXE МОГУТ СОДЕРЖАТЬ ВРЕДОНОСНЫЙ КОД. НИКОГДА НЕ ЗАПУСКАЙТЕ ТАКИЕ ФАЙЛЫ, ПОЛУЧЕННЫЕ ИЗ НЕНАДЁЖНЫХ ИСТОЧНИКОВ — ПО ПОЧТЕ, МЕССЕНДЖЕРАМ ИЛИ С ПОДОЗРИТЕЛЬНЫХ САЙТОВ.

СКАЧИВАЙТЕ ПРОГРАММЫ ТОЛЬКО С ОФИЦИАЛЬНЫХ САЙТОВ

ДАЖЕ БЕСПЛАТНЫЕ ПРОГРАММЫ СТОИТ ЗАГРУЖАТЬ ИСКЛЮЧИТЕЛЬНО С ПРОВЕРЕННЫХ РЕСУРСОВ. ПИРАТСКИЕ ВЕРСИИ КОММЕРЧЕСКОГО ПО ЧАСТО ИСПОЛЬЗУЮТСЯ ДЛЯ РАСПРОСТРАНЕНИЯ ТРОЯНОВ, ШПИОНСКИХ ПРОГРАММ И ВЫМОГАТЕЛЕЙ.

NEXT

КАК БЕЗОПАСНО СКАЧАТЬ ФАЙЛЫ ИЗ ИНТЕРНЕТА



Файлы с расширением .exe могут содержать вредоносный код. Никогда не запускайте такие файлы, полученные из ненадёжных источников.

Скачивайте программы только с официальных сайтов

Даже бесплатные программы стоит загружать исключительно с проверенных ресурсов. Пиратские версии коммерческого ПО часто используются для распространения троянов, шпионских программ и вымогателей.

NEXT

ИСПОЛЬЗУЙТЕ И ОБНОВЛЯЙТЕ АНТИВИРУС

Надёжное антивирусное решение с регулярными обновлениями поможет обнаружить и заблокировать угрозы.

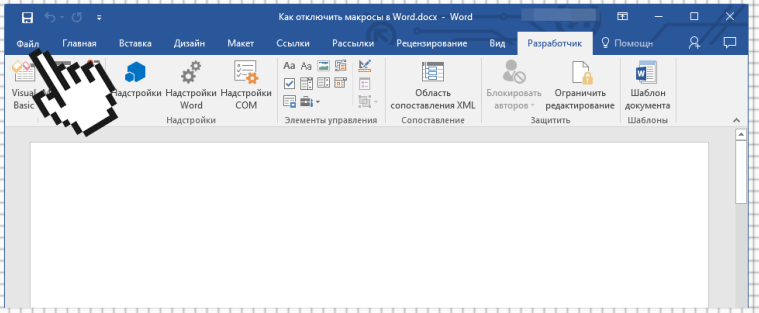
Последствия заражения:

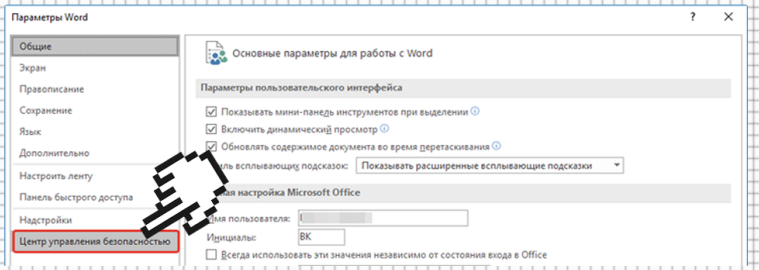
— Кража личных данных
— Шифрование или удаление файлов
— Включение устройства в бот-сеть (для DDoS, майнинга и т.п.)
— Скрытая слежка через трояны

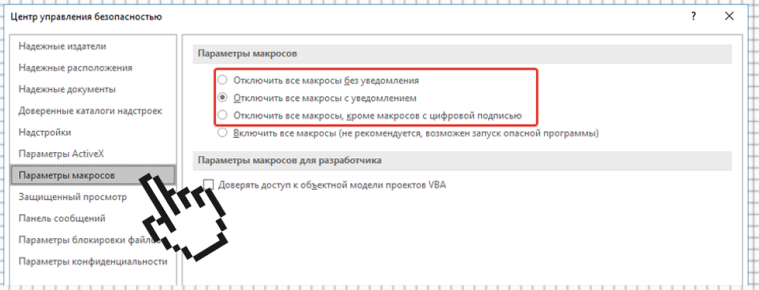
NEXT

ДОКУМЕНТЫ .DOCX И .XLSX

Даже безобидные на вид документы Word (.docx) или Excel (.xlsx), полученные по почте, могут содержать вредоносные макросы.
При открытии они запускают скрытый код — например, для кражи данных или заражения системы.







Запустите Word и перейдите в меню «Файл» --> «Параметры» --> «Центр управления безопасностью» --> «Параметры центра управления безопасностью» --> «Параметры макросов»

установите маркер напротив одного из пунктов:
--> «Отключить все без уведомления»

NEXT

ФАЙЛЫ PDF

Файлы PDF могут содержать фишинговые ссылки или вредоносный код.
При открытии такого документа может запуститься вредоносная программа для кражи данных, установки шпионского ПО или выполнения произвольного кода.

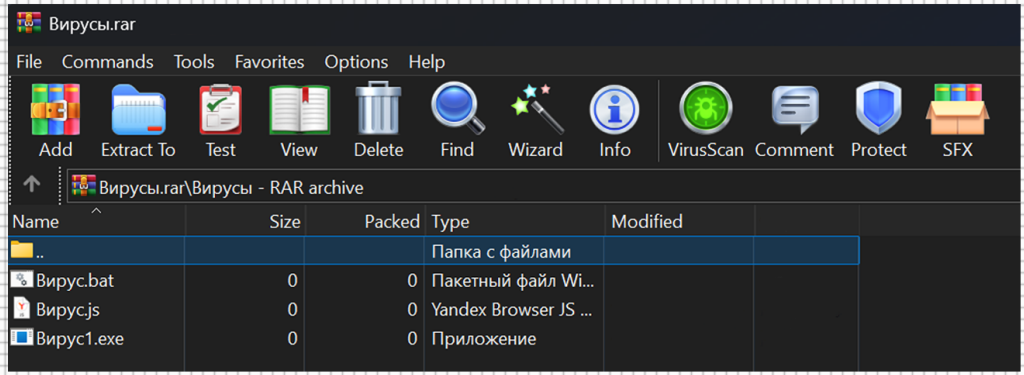
— Не переходите по ссылкам из PDF, полученных из ненадёжных источников.
Даже если сайт кажется легитимным — введите его адрес вручную.
— Используйте актуальные версии PDF-ридеров: разработчики регулярно выпускают обновления, устраняющие критические уязвимости.
— По возможности отключите поддержку JavaScript в настройках программы для просмотра PDF.

NEXT

Архивы

Вредоносные файлы можно спрятать и внутри архивов (.zip, .rar и др.).

При распаковке пользователь может случайно запустить троян, вымогателя или шпионскую программу — особенно если внутри скрывается исполняемый файл (.exe, .scr и т.п.).



— Не распаковывайте архивы из писем неизвестных отправителей.
— Перед открытием проверьте список файлов внутри архива: следует быть осторожнее, если среди них есть форматы .exe, .js, .bat и других исполняемых форматов.
— Никогда не запускайте программы, если вы не уверены в источнике или разработчике.
— Используйте антивирус с функцией сканирования архивов.

ПОДВЕДЕМ ИТОГИ

— Устанавливайте приложения только из официальных магазинов.
— Перед установкой проверяйте: рейтинг, отзывы, количество скачиваний, разработчика.
— Ограничьте разрешения приложений: не давайте доступ к контактам, SMS, геолокации без необходимости.
— Проверяйте скаченные файлы с помощью антивируса и не игнорируйте предупреждения.

ЗАГРУЗКА

ИСПОЛЬЗУЙТЕ И ОБНОВЛЯЙТЕ АНТИВИРУС

НАДЁЖНОЕ АНТИВИРУСНОЕ РЕШЕНИЕ С РЕГУЛЯРНЫМИ ОБНОВЛЕНИЯМИ ПОМОЖЕТ ОБНАРУЖИТЬ И ЗАБЛОКИРОВАТЬ УГРОЗЫ ДО ИХ АКТИВАЦИИ.

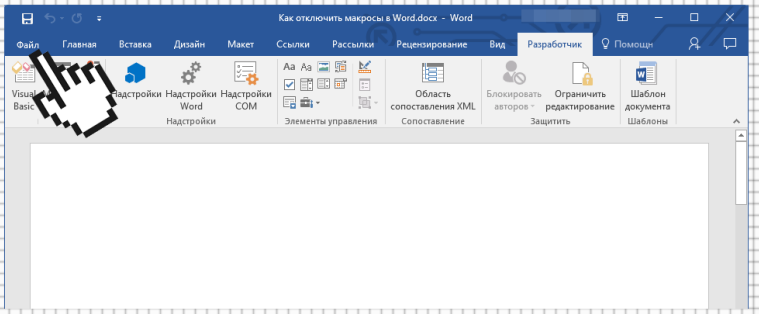
ПОСЛЕДСТВИЯ ЗАРАЖЕНИЯ:

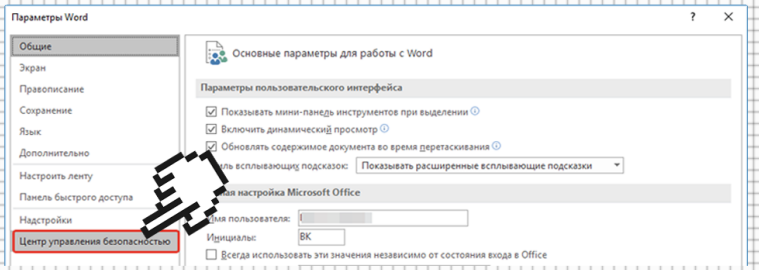
- КРАЖА ЛИЧНЫХ ДАННЫХ
- ШИФРОВАНИЕ ИЛИ УДАЛЕНИЕ ФАЙЛОВ
- ВКЛЮЧЕНИЕ УСТРОЙСТВА В БОТ-СЕТЬ (ДЛЯ DDOS, МАЙНИНГА И Т.П.)
- СКРЫТАЯ СЛЕЖКА ЧЕРЕЗ ТРОЯНЫ

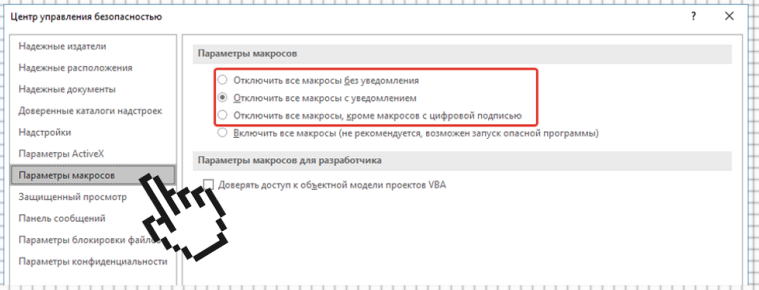
NEXT

ДОКУМЕНТЫ .DOCX И .XLSX

ДАЖЕ БЕЗОБИДНЫЕ НА ВИД ДОКУМЕНТЫ WORD (.DOCX) ИЛИ EXCEL (.XLSX), ПОЛУЧЕННЫЕ ПО ПОЧТЕ, МОГУТ СОДЕРЖАТЬ ВРЕДОНОСНЫЕ МАКРОСЫ.
ПРИ ОТКРЫТИИ ОНИ ЗАПУСКАЮТ СКРЫТЫЙ КОД — НАПРИМЕР, ДЛЯ КРАЖИ ДАННЫХ ИЛИ ЗАРАЖЕНИЯ СИСТЕМЫ.







ЗАПУСТИТЕ ВОРД И ПЕРЕЙДИТЕ В МЕНЮ «ФАЙЛ» --> «ПАРАМЕТРЫ» --> «ЦЕНТР УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ» --> «ПАРАМЕТРЫ ЦЕНТРА УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ» --> «ПАРАМЕТРЫ МАКРОСОВ»

УСТАНОВИТЕ МАРКЕР НАПРОТИВ ОДНОГО ИЗ ПУНКТОВ:
--> «ОТКЛЮЧИТЬ ВСЕ БЕЗ УВЕДОМЛЕНИЯ»

NEXT

ФАЙЛЫ PDF

Файлы PDF могут содержать фишинговые ссылки или исполняемый JavaScript-код.
При открытии такого документа может запуститься вредоносная программа для кражи данных, установки шпионского ПО или выполнения произвольного кода.

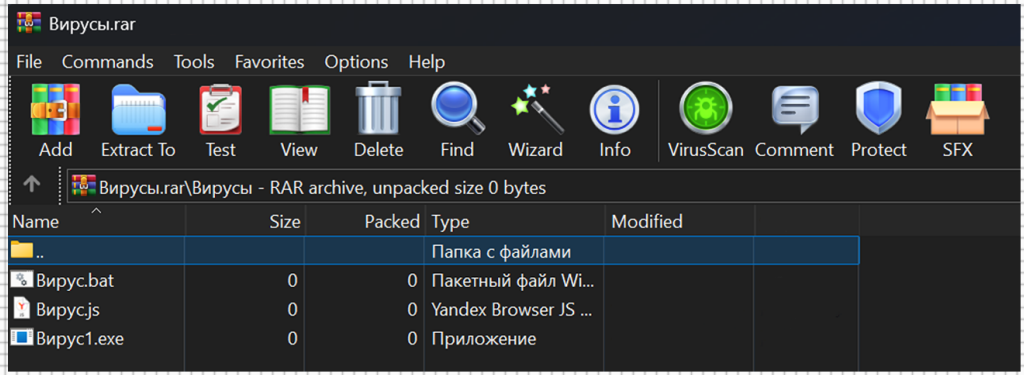
Не переходите по ссылкам из PDF, полученных из ненадёжных источников.
Даже если сайт кажется легитимным — введите его адрес вручную.
— Используйте актуальные версии PDF-ридеров: разработчики регулярно выпускают обновления, устраняющие критические уязвимости.
— По возможности отключите поддержку JavaScript в настройках программы для просмотра PDF.

NEXT

Архивы

Вредоносные файлы можно спрятать и внутри архивов (.zip, .rar и др.).

При распаковке пользователь может случайно запустить троян, вымогателя или шпионскую программу — особенно если внутри скрывается исполняемый файл (.exe, .scr и т.п.).



- Не распаковывайте архивы из писем неизвестных отправителей.
- Перед открытием проверьте список файлов внутри архива: насторожитесь при наличии .exe, .js, .bat и других исполняемых форматов.
- Никогда не запускайте программы, если вы не уверены в источнике или разработчике.
- Используйте антивирус с функцией сканирования архивов.

- Устанавливайте приложения только из официальных магазинов.
- Перед установкой проверяйте: рейтинг, отзывы, количество скачиваний, разработчика.
- Ограничьте разрешения приложений: не давайте доступ к контактам, SMS, геолокации без необходимости.
- Проверяйте скаченные файлы с помощью антивируса и не игнорируйте предупреждения.

ЗАГРУЗКА