

ЩО РОБИТИ, ЯКЩО ЗАВАНТАЖИЛИ ПІДОЗРІЛИЙ ФАЙЛ У СМАРТФОН АБО НА КОМП'ЮТЕР

1

Не відкривайте завантаженого файлу

Перевірте антивірусними програмами файл, що викликає підозру, та весь пристрій. Переконайтеся, що база даних антивірусу оновлена до останньої версії та має модуль Антифішинг

Якщо відкрили файл, вимкніть передання даних через мережу

Не надавайте жодних дозволів, якщо запустився процес встановлення програми, чи скасуйте його взагалі



**Державна служба
спеціального зв'язку та захисту
інформації України**

ЩО РОБИТИ, ЯКЩО ЗАВАНТАЖИЛИ ПІДОЗРІЛИЙ ФАЙЛ У СМАРТФОН АБО НА КОМП'ЮТЕР

2

**Якщо виявилось, що файл
містить шкідливий код**

**Не вводьте жодних даних, яких
вимагає програма**

**Перевірте на сайті CERT-UA
<https://cert.gov.ua/>, чи немає
згаданого файлу в останніх
новинах про кібератаки**

**Надішліть файл з описом
ситуації на пошту CERT-UA
cert@cert.gov.ua**

**Повідомте Кіберполіцію
про користувача, від якого
отримали файл
callcenter@cyberpolice.gov.ua**



**Державна служба
спеціального зв'язку та захисту
інформації України**

ЩО РОБИТИ, ЯКЩО ЗАВАНТАЖИЛИ ПІДОЗРІЛИЙ ФАЙЛ У СМАРТФОН АБО НА КОМП'ЮТЕР

3

Якщо файл отриманий у месенджері, повідомте адміністрацію месенджера про шкідливий контент:

Telegram

Натисніть на повідомлення → оберіть Повідомити → опишіть причину (якщо фішинг → Інше → Фішинг)

WhatsApp

Натисніть на повідомлення і кілька секунд утримуйте → оберіть у правому верхньому кутку три крапки → натисніть Поскаржитись

Viber

Натисніть на повідомлення і кілька секунд утримуйте → натисніть Скарга → Інше → опишіть проблему



Державна служба
спеціального зв'язку та захисту
інформації України

ЩО РОБИТИ, ЯКЩО ЗАВАНТАЖИЛИ ПІДОЗРІЛИЙ ФАЙЛ У СМАРТФОН АБО НА КОМП'ЮТЕР

4

Порада. Для смартфона.

Збережіть у хмарі копії всіх важливих файлів і скиньте пристрій до заводських налаштувань, щоб виключити діяльність програм-Keylogger-ів, що слідкують за користувачем без запитування доступу до системи



Державна служба
спеціального зв'язку та захисту
інформації України

ЩО РОБИТИ, ЯКЩО ЗАВАНТАЖИЛИ ПІДОЗРІЛИЙ ФАЙЛ У СМАРТФОН АБО НА КОМП'ЮТЕР

5

Як обрати антивірус

Використовуйте платні версії всесвітньо відомих антивірусних програм. Деякі сервіси пропонують ліцензії для стаціонарних і мобільних пристроїв

ESET

Avast

Zillya

McAfee



Державна служба
спеціального зв'язку та захисту
інформації України

ЩО РОБИТИ, ЯКЩО ЗАВАНТАЖИЛИ ПІДОЗРІЛИЙ ФАЙЛ У СМАРТФОН АБО НА КОМП'ЮТЕР

6

Якщо немає ліцензійного антивірусу

Використовуйте безкоштовні
версії цих програм та
обов'язково регулярно
оновлюйте їхні вірусні бази
вручну

Перед використанням
безкоштовних антивірусних
програм обов'язково
перевіряйте в пошуковику
їхню репутацію

Проте навіть якщо файл не
детектується як шкідливий,
не варто втрачати пильності.
Шкідливе ПЗ або код може бути
новим, і про нього можуть
ще “не знати” антивіруси



Державна служба
спеціального зв'язку та захисту
інформації України

ЩО РОБИТИ, ЯКЩО ЗАВАНТАЖИЛИ ПІДОЗРІЛИЙ ФАЙЛ У СМАРТФОН АБО НА КОМП'ЮТЕР

7

Увага!

Завантажуйте антивірус винятково з офіційних сайтів або магазинів застосунків (AppStore, Google Play). Програмне забезпечення з невідомих джерел, швидше за все, містить шкідливий програмний код.

У жодному разі не використовуйте російських антивірусів (Kaspersky Antivirus, наприклад). Російське програмне забезпечення – небезпечне!



Державна служба
спеціального зв'язку та захисту
інформації України