ЩО РОБИТИ В РАЗІ ОТРИМАННЯ ФІШИНГОВОГО РОЗСИЛАННЯ

1

Перевірте відправника

Зверніть увагу на ім'я електронної пошти (текст до @) та перевірте, чи дійсно ця особа надсилала вам повідомлення із вкладенням (зателефонуйте, напишіть у месенджері тощо).

Державна служба спеціального зв'язку та захисту інформації України

ЩО РОБИТИ В РАЗІ ОТРИМАННЯ ФІШИНГОВОГО РОЗСИЛАННЯ

2

Перевірте відправника

Зверніть увагу на домен, з якого надіслано лист (текст після @). Державні установи можуть надсилати листи тільки з доменів GOV.UA. Робочі скриньки відправників листа зазвичай в тому ж самому домені, що й основні контактні адреси на сайтах організацій.

Державна служба спеціального зв'язку та захисту інформації України

ЩО РОБИТИ В РАЗІ ОТРИМАННЯ ФІШИНГОВОГО РОЗСИЛАННЯ

3

Перевірте відправника

Увага! Офіційні установи не запитують вашої конфіденційної інформації електронною поштою

Перевірте, чи дійсно існують організації та люди, від яких надійшов лист. Не використовуйте для перевірки каналів комунікації, передбачених у листі.

Перед тим як відкрити лист чи повідомлення, придивіться до теми, змісту та перевірте пошту адресанта.

Державна служба спеціального зв'язку та захисту інформації України

ЩО РОБИТИ В РАЗІ ОТРИМАННЯ ФІШИНГОВОГО РОЗСИЛАННЯ

4

Не відкривайте та не завантажуйте файлів, особливо тих, які є потенційно небезпечними

потенційно небезпечні розширення файлів: .exe, .bin, .ini, .iso, .dll, .com, .sys, .bat, .js тощо

потенційно безпечні розширення файлів: .docx, .zip, .rar, .pdf

Увага! Зловмисники можуть використовувати у своїх інтересах вразливості, макроси та інші загрози

Державна служба спеціального зв'язку та захисту інформації України

ЩО РОБИТИ В РАЗІ ОТРИМАННЯ ФІШИНГОВОГО РОЗСИЛАННЯ

5

**Знайдіть документ,
про який ідеться в листі,
за номером чи назвою
у відкритих джерелах:**

https://zakon.rada.gov.ua/

https://www.president.gov.ua/documents/all

Державна служба
спеціального зв'язку та захисту
інформації України

ЩО РОБИТИ В РАЗІ ОТРИМАННЯ ФІШИНГОВОГО РОЗСИЛАННЯ

6

Якщо випадково завантажили вкладений файл, не відкривайте та не запускайте його. Повідомте фахівця з інформаційної безпеки. Файл має бути переданий на перевірку

Державна служба спеціального зв'язку та захисту інформації України

ЩО РОБИТИ В РАЗІ ОТРИМАННЯ ФІШИНГОВОГО РОЗСИЛАННЯ

7

Не переходьте за посиланнями в листі

Увага! Особливо небезпечні посилання, які не містять протоколу безпеки:

https – захищене

http – не захищене

Якщо отримали рекламний лист, але не були підписані на розсилання, не натискайте одразу посилання для відписки від реклами. За цим посиланням може міститися шкідливий виконавчий код.

Не заповнюйте жодних форм і полів, не натискайте кнопок, не залишайте жодних даних.

Державна служба спеціального зв'язку та захисту інформації України

ЩО РОБИТИ В РАЗІ ОТРИМАННЯ ФІШИНГОВОГО РОЗСИЛАННЯ

8

Не пересилайте листа іншим користувачам.

Негайно повідомте про розсилання фахівця з ІБ вашої установи; перешліть листа йому чи CERT-UA на пошту cert@cert.gov.ua або у Facebook www.facebook.com/UACERT

Державна служба спеціального зв'язку та захисту інформації України

ЩО РОБИТИ В РАЗІ ОТРИМАННЯ ФІШИНГОВОГО РОЗСИЛАННЯ

9

Слідкуйте за новинами про кібератаки

Перегляньте новини у ЗМІ чи повідомлення CERT-UA про те, чи не було останнім часом фішингових атак і розсилань листів із ШПЗ.

Державна служба спеціального зв'язку та захисту інформації України