# Фішинг та захист від нього

# Фішинг – це

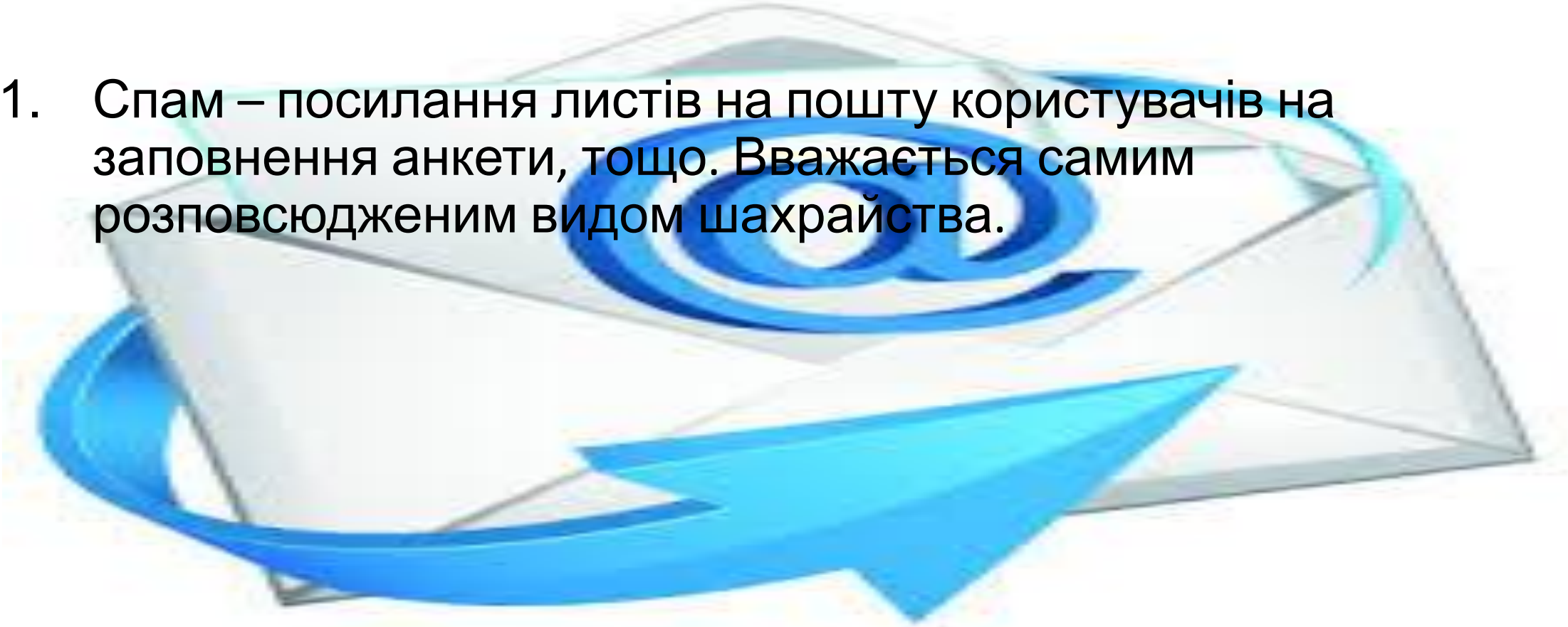
- вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказування або обміну валюти, інтернет-магазинів. Шахраї використовують усілякі виверти, які найчастіше змушують користувачів самостійно розкрити конфіденційні дані — наприклад, посилаючи електронні листи із пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на веб-сайт в Інтернеті, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів.

# Запобіжні засоби «справжніх» сайтів

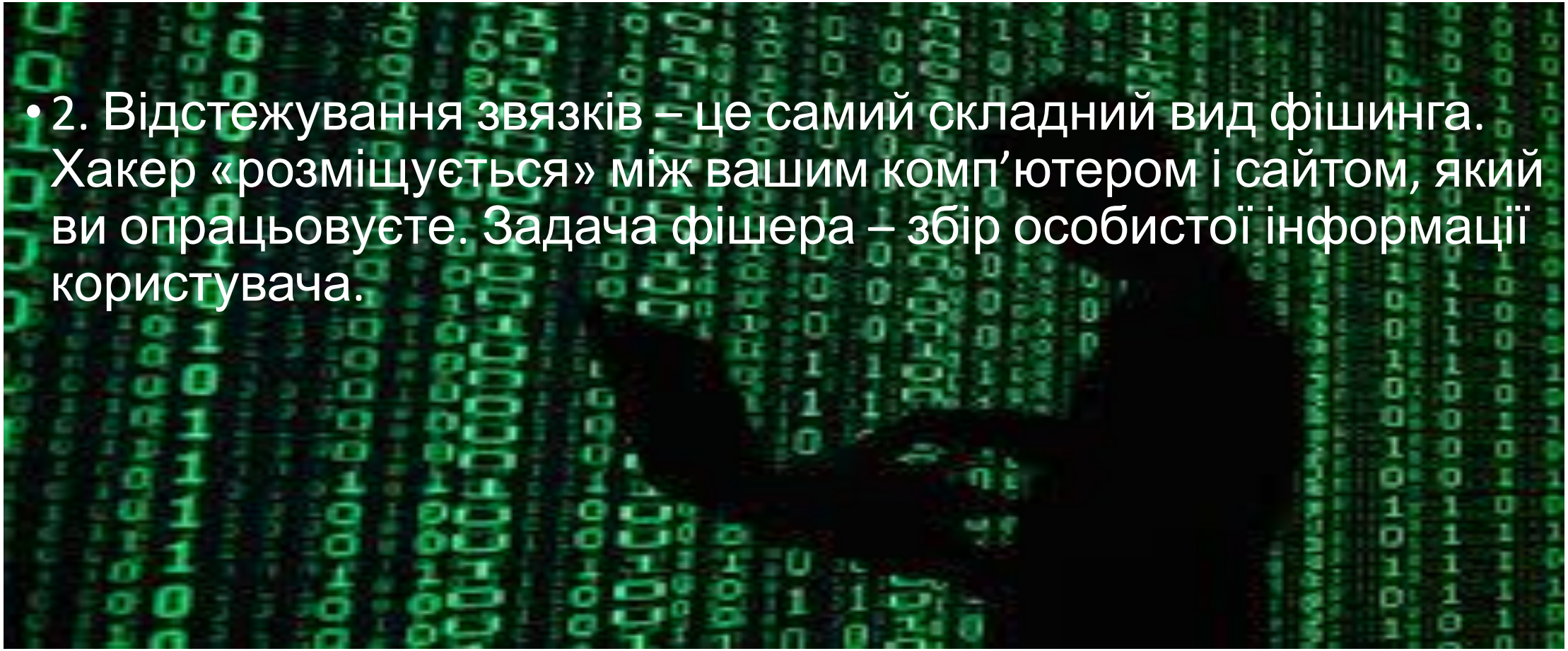
- Фішинг - один з різновидів соціальної інженерії, заснований на незнанні користувачами основ мережевої безпеки. Зокрема, багато хто не знає простого факту: сервіси не розсилають листів з проханнями повідомити свої облікові дані, пароль та інше.
- Для захисту від фішингу виробники основних інтернет-браузерів домовилися про застосування однакових способів інформування користувачів про те, що вони відкрили підозрілий сайт, який може належати шахраям. Нові версії браузерів вже володіють такою можливістю, яка відповідно іменується «антифішинг».

# Різновиди фішингу:

1. Спам – посилання листів на пошту користувачів на заповнення анкети, тощо. Вважається самим розповсюдженим видом шахрайства.



# Різновиди фішингу



- 2. Відстежування звязків – це самий складний вид фішинга. Хакер «розміщується» між вашим комп’ютером і сайтом, який ви опрацьовуєте. Задача фішера – збір особистої інформації користувача.

# Різновиди фішингу

- 3. Троянські программи – невидимі хакери, котрі намагаються проникнути в
облiковий запис користувача для збору особистої інформації і

користування нею.

# Тому:

- Ніколи не переходьте по невідомим посиланням.
- Не довіряйте проханням в листах невідомих користувачів.
- Не вказуйте особисту інформацію на сайтах.


Дякую за
увагу☺