PHISHING AWARENESS

ЯК РОЗПІЗНАТИ, ЩО ЦЕ ФІШИНГ — І ЩО З ЦИМ РОБИТИ

ПРАВИЛА ГРИ ⚠️

> **Усе тут — у лабі, зі згодою, для захисту.**

Ви це підтвердили при реєстрації — тому коротко:
ми відтворюємо атаки, щоб ви їх **упізнавали**.

Ми не атакуємо людей.

ЩО МИ ПРОЙДЕМО

1. Що таке соціальна інженерія + реальні кейси
2. 10 ознак фішингу
3. 🎮 Гра «Фішинг чи ні?» (Google Quiz)
4. 🖥️ Live demo: GoPhish
5. 📱 Quishing (QR-фішинг)
6. 📞 Vishing + AI-голос / deepfake
7. 🖼️ Приховані та шкідливі файли
8. 🆕 Сучасні атаки: коли навіть MFA не завжди рятує
9. 🏆 Фінальний квіз

1. СОЦІАЛЬНА ІНЖЕНЕРІЯ

«Зламати людину простіше, ніж систему»

СОЦ. ІНЖЕНЕРІЯ ТИСНЕ НА ЕМОЦІЇ, НЕ НА КОД

Атакуючий не ламає шифрування — він змушує **вас** натиснути.

4 важелі впливу:

- ⏰ **Терміновість** — «зробіть зараз, інакше…»
- 👔 **Авторитет** — «це директор / IT / банк»
- 😱 **Страх** — «ваш акаунт зламано»
- 🎁 **Цікавість/жадібність** — «ви виграли», «подивіться фото»

> **Якщо лист змушує поспішати і відчувати — це червоний прапор.**

ВИДИ СОЦ. ІНЖЕНЕРІЇ

ВИД	КАНАЛ	ПРИКЛАД
Phishing	Email	«Ваш акаунт Microsoft заблоковано»
Smishing	SMS	«Посилка DHL чекає, доплатіть 1€»
Vishing	Дзвінок	«Це банк, назвіть код із SMS»
Quishing	QR-код	QR на «оплату паркінгу» → фейк-сайт
BEC	Email (підробка боса)	«Терміново оплати інвойс, я на зустрічі»
Spear phishing	Цільовий	Лист особисто вам, з вашими деталями

РЕАЛЬНІ КЕЙСИ (ЦЕ НЕ ТЕОРІЯ)

КЕЙС	РІК	ЯК ЗЛАМАЛИ
Twitter (Маск, Обама)	2020	Vishing → внутрішня панель
Uber	2022	MFA fatigue: 100 push «Approve?»
MGM / Caesars (казино)	2023	Дзвінок у helpdesk → скинули MFA
Retool	2023	SMS + дзвінок + AiTM разом

> **Жертви — не «дурні». Це були техкомпанії з MFA.**

❌ КЛАСИЧНІ ПРИМАНКИ

> «Ваш акаунт Microsoft заблоковано. Увійдіть тут.»

> «Вітаємо! Ви виграли iPhone 📱»

> «Терміново перевірте рахунок-фактуру (вкладення).»

> «Незвичний вхід у ваш акаунт. Підтвердіть особу.»

Спільне: терміновість + дія + посилання/вкладення.

2. ЯК РОЗПІЗНАТИ ФІШИНГ

10 ознак

🔍 10 ОЗНАК ФІШИНГУ

1. 🌐 **Дивний домен** (microsft-login.com, paypa1.com)
2. ✍️ **Помилки** в тексті / дивна мова
3. ⏰ **Терміновість** і тиск
4. 😱 **Погрози** («акаунт видалять»)
5. 📎 **Незвичне вкладення** (.zip, .html, .iso)
6. 📷 **QR-код** замість звичайного посилання
7. 🔑 **Просять ввести пароль** / код MFA
8. 💳 **Просять оплатити** терміново
9. 👤 **Незвичний відправник** (ім'я ≠ адреса)
10. 🔗 **Підозрілі посилання** (наведи, не клікай!)

ОЗНАКА №1 — ДОМЕН І ВІДПРАВНИК

Ім'я відправника бреше. **Адреса** — правда.

```
Від: Microsoft Security <no-reply@microsft-secure-login.ru>
                        ^^^^^^^^ помилка    ^^^ дивна зона
```

- `microsft` замість `microsoft` (typosquatting)
- `paypa1` (одиниця замість «l»)
- `.ru` / `.xyz` / `.top` там, де чекаєш `.com`
- піддомен брехні: `microsoft.login-verify.com` → справжній домен це `login-verify.com`!

✅ **Читай домен справа наліво: останнє перед `/` — справжній власник.**

ОЗНАКА №10 — ПОСИЛАННЯ (HOVER!)

Текст посилання ≠ куди воно веде.

🖱️ **Спробуй наживо** — наведи (НЕ клікай) на це «безпечне» посилання:

https://www.paypal.com/secure

↳ Унизу браузера / у підказці з'явиться справжня адреса: `evil-login-verify.xyz`

✅ **На комп’ютері: наведи курсор, глянь URL внизу екрана.**
✅ **На телефоні: довге натискання → показати посилання.**
✅ **Не впевнений — не клікай, зайди на сайт вручну.**

А ЯКЩО ЛИСТ ВИГЛЯДАЄ ІДЕАЛЬНО?

Сучасний фішинг **без** помилок (AI пише грамотно).
Тоді працює **процес**, а не «відчуття»:

- 🛑 **Пауза.** Лист тисне поспішити? Це вже сигнал.
- 📞 **Другий канал.** Подзвони/спитай напряму — не відповідай на сам лист.
- 🔐 **Ніколи** не вводь пароль/код за посиланням із листа.
- 🚩 **Кнопка Report** у Gmail/Outlook — користуйся.

> **Verify, don't trust.** Це і є Zero Trust для людей.

3. 🎮 ГРА «ФІШИНГ ЧИ НІ?»

Голосуємо разом

GOOGLE PHISHING QUIZ (JIGSAW)

📱 Скануй з екрана —
проходь сам
🔗 **phishingquiz.withgoogle.com** ↗️

Правила:

1. Дивимось приклад листа разом.
2. Голосуємо: ✋ **Phishing** чи 🤚 **Legit**?
3. Розбираємо **чому** — на що дивитись.

4. 💻 GOPHISH — LIVE DEMO

Як виглядає атака зсередини

ЩО ТАКЕ GOPHISH

Open-source платформа для **легальних** фішинг-симуляцій.

Показує те, що бачить атакуючий:

- 📧 хто **отримав** лист
- 👁️ хто **відкрив**
- 🖱️ хто **клікнув** посилання
- ⌨️ хто **ввів дані** на фейк-сторінці

> ⚠️ **Тільки власні тестові акаунти / зі згодою. Паролі в демо — фейкові.**

GOPHISH: АНАТОМІЯ КАМПАНІЇ

```
Sending Profile   →  хто шле (SMTP)
      +
Email Template    →  сам лист (HTML, з {{.FirstName}})
      +
Landing Page      →  фейкова сторінка входу (+ захоплення даних)
      +
Users & Groups    →  кому шлемо (тестові акаунти)
      =
        Campaign  →  старт + дашборд у реальному часі
```

Захист, що видно тут: технічні фільтри пошти ускладнюють доставку підробки.

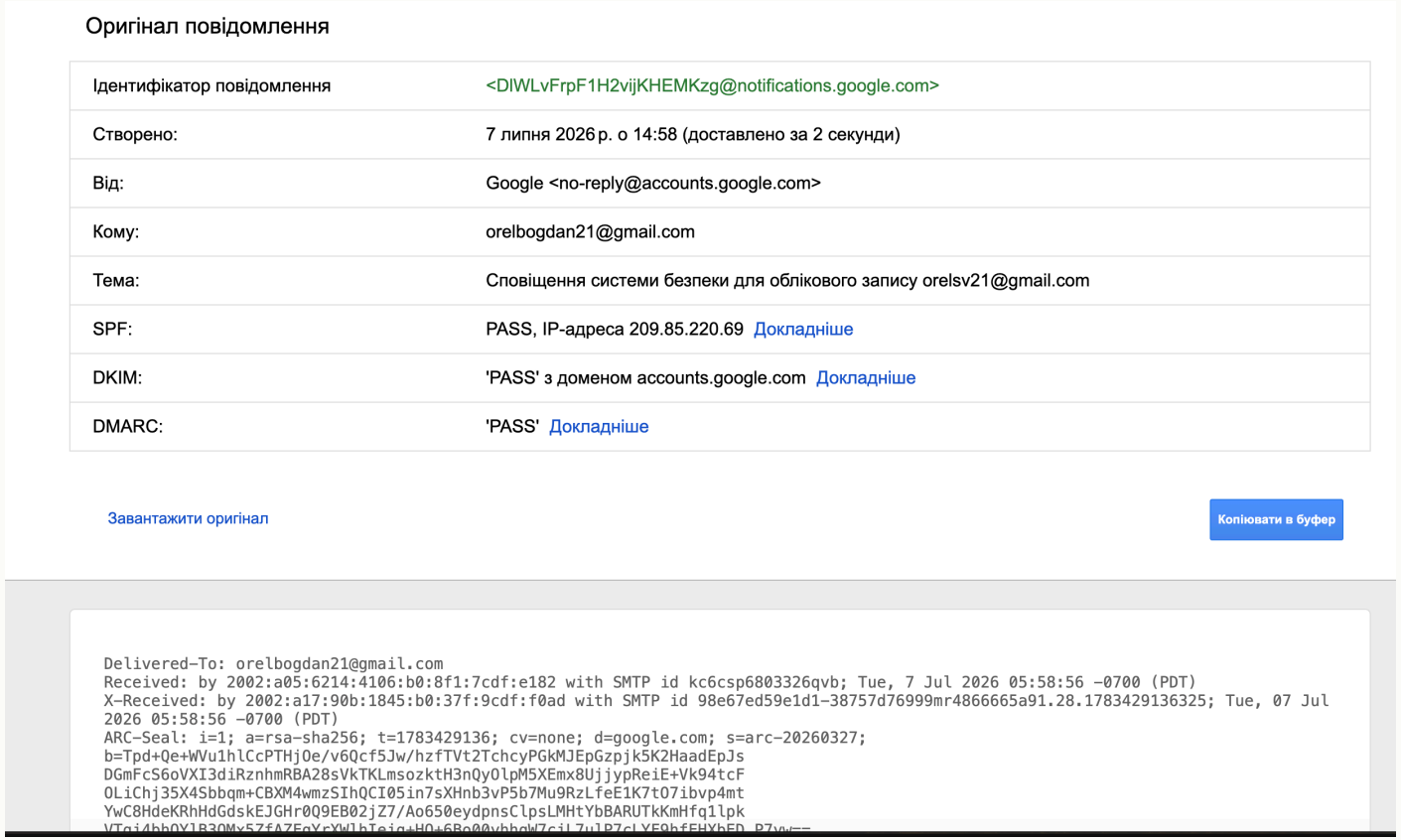
GOPHISH: ЩО ЦЕ ВЧИТЬ ЗАХИСТУ

- 📊 Видно, **наскільки легко** клікають — без осуду.
- 🏷️ Червоний банер «[EXTERNAL]» на листах ззовні — простий, але дієвий.
- ✅ **Технічні фільтри пошти** — ускладнюють підробку відправника.
- 🚨 Кнопка **Report Phishing** перетворює жертв на сенсор.
- 🔁 Регулярні симуляції ↓ клік-рейт із часом.

ЗАГЛЯНУТИ «ПІД КАПОТ» ЛИСТА

У листа є **технічні перевірки**, чи відправник справжній — їх робить сама пошта.

У Gmail: ⋮ → **«Показати оригінал»**:



Оригінал повідомлення

Ідентифікатор повідомлення	<DlWLvFrpF1H2vijKHEMKzg@notifications.google.com>
Створено:	7 липня 2026 р. о 14:58 (доставлено за 2 секунди)
Від:	Google <no-reply@accounts.google.com>
Кому:	orelbogdan21@gmail.com
Тема:	Сповіщення системи безпеки для облікового запису orelsv21@gmail.com
SPF:	PASS, IP-адреса 209.85.220.69 Докладніше
DKIM:	'PASS' з доменом accounts.google.com Докладніше
DMARC:	'PASS' Докладніше

Завантажити оригінал

Копіювати в буфер

```
Delivered-To: orelbogdan21@gmail.com
Received: by 2002:a05:6214:4106:b0:8f1:7cdf:e182 with SMTP id kc6csp6803326qvb; Tue, 7 Jul 2026 05:58:56 -0700 (PDT)
X-Received: by 2002:a17:90b:1845:b0:37f:9cdf:f0ad with SMTP id 98e67ed59e1d1-38757d76999mr4866665a91.28.1783429136325; Tue, 07 Jul
2026 05:58:56 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1783429136; cv=none; d=google.com; s=arc-20260327;
b=Tpd+Qe+WVu1hlCcPTHjOe/v6Qcf5Jw/hzfTVt2TchcyPGkMJEpGzpjk5K2HaadEpJs
DGmFcS6oVXI3diRznhmRBA28sVkTKLmsozktH3nQyOlpM5XEmx8UjjypReiE+Vk94tcF
OLiChj35X4Sbbqm+CBXM4wmzSIhQCI05in7sXHnb3vP5b7Mu9RzLfeE1K7tO7ibvp4mt
YwC8HdeKRhHdGdskEJGHr0Q9EB02jZ7/Ao650eydpnsClpsLMHtYbBARUTkKmHfq1lpk
```


✅ **Бачиш `PASS` — добре. Бачиш `FAIL` — привід не довіряти листу.**

5. 📱 QUISHING (QR-ФІШИНГ)

Коли посилання сховане в картинці

QUISHING — ЧОМУ НЕБЕЗПЕЧНО

QR-код = посилання, яке **ти не бачиш очима**.

- Обходить email-фільтри (це ж картинка!)
- На телефоні складніше перевірити URL
- Часто в PDF «рахунках», на «паркоматах», «меню»

🔴 **Скануй телефоном** → побачиш, що буває (наша сторінка)

✅ **Захист: камера показує URL перед відкриттям — читай його. Не скануй QR із випадкових наліпок.**

6. 📞 VISHING + AI-ГОЛОС

«Привіт, це директор…»

ГОЛОСУ І ВІДЕО ТЕЖ НЕ МОЖНА ВІРИТИ

📞 Дзвінок «від боса»: авторитет + терміновість + знайомий голос.

Чому спрацьовує:

- 👔 авторитет («це директор / IT / банк»)
- ⏰ терміновість («я на зустрічі, швидко»)
- 🧠 ми звикли довіряти знайомому голосу

> **AI-клон голосу робиться з кількох секунд запису.**
> **Deepfake-відео — уже теж реальність.**

AI-ГОЛОС І DEEPFAKE: НА ЩО ЦЕ ВЖЕ ЗДАТНЕ

🎥 **Дивимось 1–2 короткі відео** — наскільки переконливими стали підробки голосу й обличчя.

- Клон голосу з кількох секунд запису.
- Deepfake-відео в реальному часі (Zoom-дзвінок «від керівника»).

💸 **2024: компанія в Гонконзі втратила $25 млн — переказ після deepfake-відеодзвінка «від фіндиректора».**

✅ **Висновок: голос і відео — більше не доказ особи.**

VISHING: ПРАВИЛО «ZERO TRUST ДЛЯ ГОЛОСУ»

Навіть якщо голос звучить на 100% як шеф:

- 🛑 **Стоп**, якщо просять: пароль, код MFA, переказ, gift-карти.
- 📞 **Передзвони** на номер, який ти **знаєш** (не той, що дзвонив).
- 🔑 **Кодове слово** для термінових фінансових прохань.
- 🤝 Жодна легітимна служба **не просить** пароль голосом.

> **Голос — більше не доказ особи.**

7. 🖼️ ПРИХОВАНІ ТА ШКІДЛИВІ ФАЙЛИ

Коли «документ» — не те, чим здається

ДАНІ МОЖНА СХОВАТИ В ЗВИЧАЙНОМУ ФАЙЛІ

🖼️ У звичайному фото може бути **захований текст** — око не бачить різниці, розмір майже той самий.

Це називають **стеганографія**. Так ховають дані (або команди для малваря) «на видноті».

> ⚠️ **Головна ідея: файл не завжди «просто картинка» чи «просто документ».**

ДЕМО: КОЛИ «ДОКУМЕНТ» Б'Є ОДРАЗУ

🖱️ Відкриваю звичайний на вигляд файл-документ у браузері…

→ 😱 він показує «**Тебе зламано!**» і **сам завантажує** файл на комп'ютер.

Жодного «Enable» я не тиснув — досить було **відкрити**.

✅ **Захист: не відкривай несподівані вкладення, навіть «рахунки» й «документи». Сумнів — спитай відправника другим каналом.**

ЯКІ ФАЙЛИ БУВАЮТЬ НЕБЕЗПЕЧНИМИ

Не показуємо робочий малвар — важливий **рефлекс**:

- 📊 **Office із «Enable Content»** — це «дозволяю запустити код». Легітимний документ цього не просить.
- 📄 **PDF / HTML** — можуть містити скрипти й вести на фейк-логін.
- 🗜️ **Архіви (особливо з паролем)** — ховають payload, обходять антивірус.

✅ **Захист: не вмикай макроси; не відкривай несподівані вкладення; увімкни показ розширень файлів (ловиш `рахунок.pdf.exe`).**

8. 🆕 СУЧАСНІ АТАКИ

Коли навіть MFA не завжди рятує

MFA: ДУЖЕ ЗАХИЩАЄ — АЛЕ НЕ НА 100%

MFA (двофакторка) — один із найсильніших захистів. Вмикай її **скрізь**.

Але і її обходять:

- 🔁 шлють push «Approve?» знову і знову, поки втомлений не натиснеш «Yes» (так зламали Uber).
- 🥷 крадуть уже **підтверджену сесію** — заходять без пароля й без коду.

✅ **Все одно вмикай MFA — без неї в рази гірше. І правило: «я не ініціював вхід → не підтверджуй, тисни Report».**

КАРТИНА ЗАГРОЗ: ПІДСУМОК

АТАКА	НА ЩО ТИСНЕ	ПРОСТИЙ ЗАХИСТ
Phishing	увагу	hover + пауза + Report
Підробка листа	довіру	перевір відправника, другий канал
Vishing / deepfake	довіру до голосу	другий канал + кодове слово
Quishing	що не бачиш URL	читай адресу з камери
Обхід MFA	твою втому	не підтверджуй, чого не просив

9. 🏆 ФІНАЛЬНИЙ КВІЗ

Перевіримо рефлекс

KAHOOT — ЗМАГАЄМОСЬ!

🔗 (код гри на екрані)

10–15 питань: «Фішинг чи ні?» + «Що робити?»

Ведучий: запусти Kahoot, дай код, веселощі. Питання — у 40_quiz/final-quiz.md.

🎯 ЗАПАМ’ЯТАЙ 5 РЕЧЕЙ

1. 🛑 **Пауза** перед кліком — терміновість це сигнал.
2. 🔍 **Hover** на посилання, читай **домен** (справа наліво).
3. 📞 **Другий канал** — перевір прохання, не довіряй листу/голосу.
4. 🔑 **Ніколи** не диктуй пароль/код — нікому, ніде.
5. 🚨 **Report** — твоя кнопка робить усіх безпечнішими.

> **Verify, don't trust.**

ДЯКУЮ! 🙏

Запитання?

📄 Хендаут-шпаргалку роздам / надішлю.

🔗 Google Phishing Quiz: phishingquiz.withgoogle.com

🔗 Перевір, чи витік твій email: haveibeenpwned.com

Залишайтесь параноїками в міру. 😉