PHISHING AWARENESS

HOW TO SPOT THAT IT'S PHISHING — AND WHAT TO DO ABOUT IT

RULES OF THE GAME ⚠️

> Everything here is **in a lab, with consent, for defense**.

You confirmed this at registration — so, briefly:
we recreate attacks so that you can **recognize** them.

We do not attack people.

WHAT WE'LL COVER

1. What social engineering is + real cases
2. 10 signs of phishing
3. 🎮 Game "Phishing or not?" (Google Quiz)
4. 🖥️ Live demo: GoPhish
5. 📱 Quishing (QR phishing)
6. 📞 Vishing + AI voice / deepfake
7. 🖼️ Hidden and malicious files
8. 🆕 Modern attacks: when even MFA doesn't always save you
9. 🏆 Final quiz

1. SOCIAL ENGINEERING

"Hacking a human is easier than hacking a system"

SOCIAL ENGINEERING TARGETS EMOTIONS, NOT CODE

The attacker doesn't break the encryption — they make **you** click.

4 levers of influence:

- ⏰ **Urgency** — "do it now, or else…"
- 👔 **Authority** — "it's the director / IT / the bank"
- 😱 **Fear** — "your account has been hacked"
- 🎁 **Curiosity/greed** — "you've won", "look at this photo"

> **If a message makes you rush and feel — that's a red flag.**

TYPES OF SOCIAL ENGINEERING

TYPE	CHANNEL	EXAMPLE
Phishing	Email	"Your Microsoft account is locked"
Smishing	SMS	"A DHL parcel is waiting, pay €1 extra"
Vishing	Call	"This is the bank, read out the code from the SMS"
Quishing	QR code	QR for "parking payment" → fake site
BEC	Email (boss spoof)	"Urgently pay this invoice, I'm in a meeting"
Spear phishing	Targeted	An email just for you, with your details

REAL CASES (THIS ISN'T THEORY)

CASE	YEAR	HOW THEY BROKE IN
Twitter (Musk, Obama)	2020	Vishing → internal panel
Uber	2022	MFA fatigue: 100 "Approve?" pushes
MGM / Caesars (casinos)	2023	Call to the helpdesk → MFA reset
Retool	2023	SMS + call + AiTM combined

> **The victims weren't "stupid". These were tech companies with MFA.**

❌ CLASSIC BAIT

> "Your Microsoft account is locked. Sign in here."

> "Congratulations! You've won an iPhone 📱"

> "Urgently check the invoice (attachment)."

> "Unusual sign-in to your account. Confirm your identity."

The common thread: urgency + an action + a link/attachment.

2. HOW TO SPOT PHISHING

10 signs

🔍 10 SIGNS OF PHISHING

1. 🌐 **Odd domain** (microsft-login.com, paypa1.com)
2. ✍️ **Errors** in the text / strange language
3. ⏰ **Urgency** and pressure
4. 😱 **Threats** ("your account will be deleted")
5. 📎 **Unusual attachment** (.zip, .html, .iso)
6. 📷 **QR code** instead of a normal link
7. 🔑 **Asks for your password** / MFA code
8. 💳 **Asks you to pay** urgently
9. 👤 **Unusual sender** (name ≠ address)
10. 🔗 **Suspicious links** (hover, don't click!)

SIGN #1 — DOMAIN AND SENDER

The sender's name lies. The **address** tells the truth.

```
From: Microsoft Security <no-reply@microsft-secure-login.ru>
                          ^^^^^^^^ typo        ^^^ odd zone
```

- `microsft` instead of `microsoft` (typosquatting)
- `paypa1` (a "1" instead of an "l")
- `.ru` / `.xyz` / `.top` where you'd expect `.com`
- a subdomain of lies: `microsoft.login-verify.com` → the real domain is `login-verify.com`!

✅ **Read the domain right to left: the last part before `/` is the real owner.**

SIGN #10 — LINKS (HOVER!)

The link text ≠ where it leads.

🖱️ **Try it live** — hover (do NOT click) over this "safe" link:

https://www.paypal.com/secure

↳ At the bottom of the browser / in the tooltip the real address appears: `evil-login-verify.xyz`

✅ **On a computer: hover the cursor, look at the URL at the bottom of the screen.**
✅ **On a phone: long-press → show link.**
✅ **Not sure — don't click, go to the site manually.**

WHAT IF THE EMAIL LOOKS PERFECT?

Modern phishing has **no** typos (AI writes flawlessly).
Then a **process** works, not a "gut feeling":

- 🛑 **Pause.** Is the email pushing you to hurry? That's already a signal.
- 📞 **Second channel.** Call/ask directly — don't reply to the email itself.
- 🔐 **Never** enter a password/code via a link from an email.
- 🚩 **Report button** in Gmail/Outlook — use it.

> **Verify, don't trust.** This is Zero Trust for people.

3. 🎮 GAME "PHISHING OR NOT?"

We vote together

GOOGLE PHISHING QUIZ (JIGSAW)

📱 Scan from the screen —
take it yourself
🔗 **phishingquiz.withgoogle.com** ↗️

Rules:

1. We look at an example email together.
2. We vote: ✋ **Phishing** or 🤚 **Legit**?
3. We discuss **why** — what to look at.

4. 💻 GOPHISH — LIVE DEMO

What an attack looks like from the inside

WHAT IS GOPHISH

An open-source platform for **legal** phishing simulations.

It shows what the attacker sees:

- 📧 who **received** the email
- 👁️ who **opened** it
- 🖱️ who **clicked** the link
- ⌨️ who **entered data** on the fake page

> ⚠️ **Only your own test accounts / with consent. Passwords in the demo are fake.**

GOPHISH: ANATOMY OF A CAMPAIGN

```
Sending Profile   →  who sends (SMTP)
      +
Email Template    →  the email itself (HTML, with {{.FirstName}})
      +
Landing Page      →  fake login page (+ data capture)
      +
Users & Groups    →  who we send to (test accounts)
      =
        Campaign  →  launch + real-time dashboard
```

The defense visible here: technical mail checks make delivery of the forgery harder.

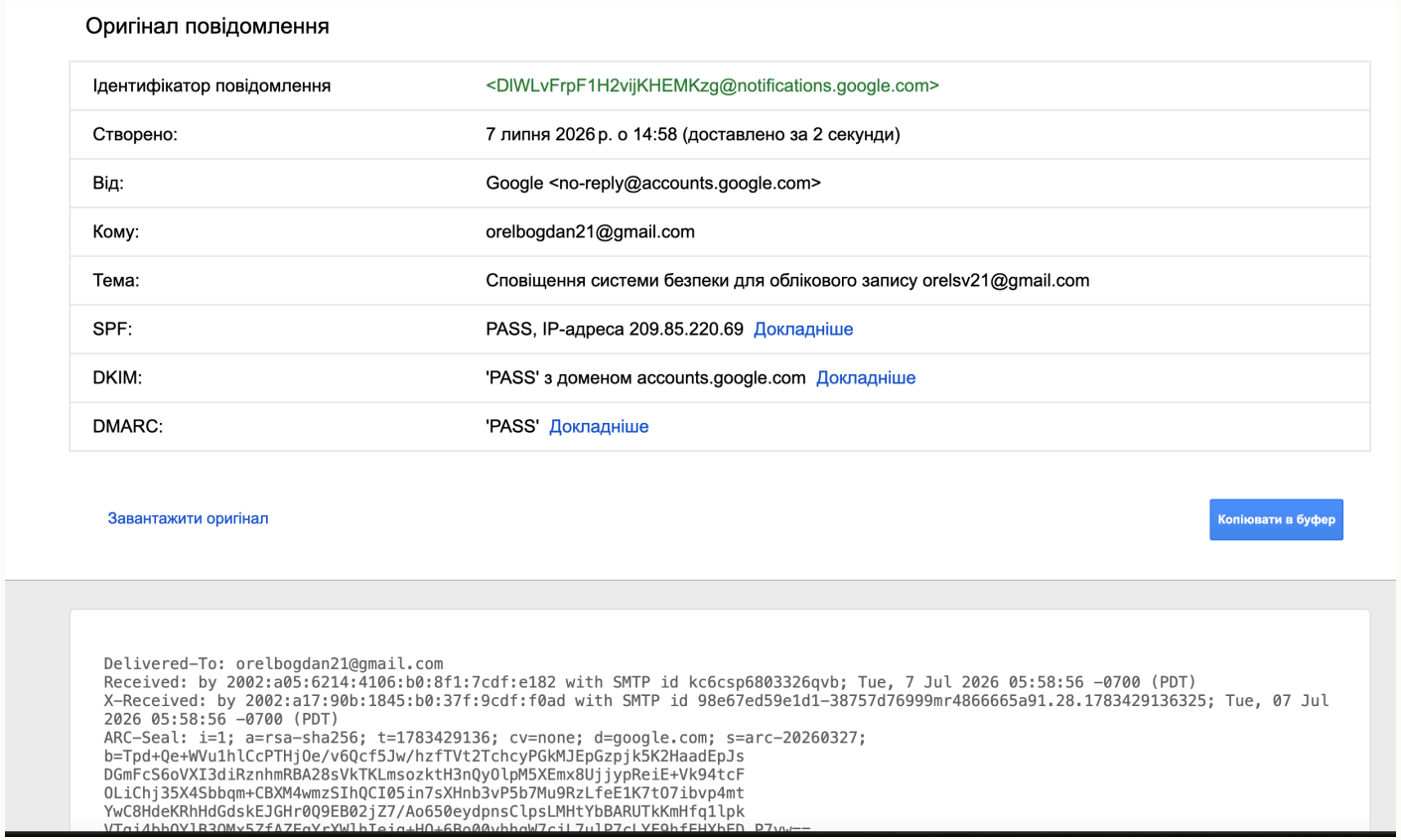
GOPHISH: WHAT IT TEACHES DEFENSE

- 📊 You see **how easily** people click — without blame.
- 🏷️ A red "[EXTERNAL]" banner on mail from outside — simple but effective.
- ✅ **Technical mail checks** — make sender forgery harder.
- 🚨 The **Report Phishing** button turns victims into a sensor.
- 🔁 Regular simulations ↓ the click rate over time.

A LOOK "UNDER THE HOOD" OF THE EMAIL

An email has **technical checks** of whether the sender is real — the mail system does them itself.

In Gmail: ⋮ → **"Show original"**:



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
VTgi4bhOYlB3QMx5ZfAZEqYrYWlbIeig+HQ+6Bo00vbbqW7ciL7ulP7cLYE9bfEHXbED P7vw==
```

✅ You see `PASS` — good. You see `FAIL` — a reason not to trust the email.

5. 📱 QUISHING (QR PHISHING)

When the link is hidden in an image

QUISHING — WHY IT'S DANGEROUS

A QR code = a link you **don't see with your eyes**.

- Bypasses email filters (it's just an image!)
- On a phone it's harder to check the URL
- Often in PDF "invoices", on "parking meters", "menus"

🔴 **Scan it with your phone** → see what happens (our page)

✅ **Defense: the camera shows the URL before opening — read it. Don't scan QR codes from random stickers.**

6. 📞 VISHING + AI VOICE

"Hi, it's the director…"

VOICE AND VIDEO AREN'T PROOF EITHER

📞 A call "from the boss": authority + urgency + a familiar voice.

Why it works:

- 👔 authority ("it's the director / IT / the bank")
- ⏰ urgency ("I'm in a meeting, quick")
- 🧠 we're used to trusting a familiar voice

> **An AI voice clone is made from a few seconds of recording.**
> **Deepfake video is already a reality too.**

AI VOICE AND DEEPFAKE: WHAT IT'S ALREADY CAPABLE OF

🎥 **We watch 1–2 short videos** — how convincing voice and face fakes have become.

- A voice clone from a few seconds of recording.
- Real-time deepfake video (a Zoom call "from the manager").

💸 **2024: a company in Hong Kong lost $25M — a transfer after a deepfake video call "from the CFO".**

✅ **Conclusion: voice and video are no longer proof of identity.**

VISHING: THE "ZERO TRUST FOR VOICE" RULE

Even if the voice sounds 100% like the boss:

- 🛑 **Stop** if they ask for: a password, an MFA code, a transfer, gift cards.
- 📞 **Call back** a number you **know** (not the one that called).
- 🔑 A **code word** for urgent financial requests.
- 🤝 No legitimate service **asks** for a password by voice.

> **A voice is no longer proof of identity.**

7. 🖼️ HIDDEN AND MALICIOUS FILES

When a "document" isn't what it seems

DATA CAN BE HIDDEN IN AN ORDINARY FILE

🖼️ An ordinary photo can contain **hidden text** — the eye sees no difference, the size is almost the same.

This is called **steganography**. It hides data (or commands for malware) "in plain sight".

> ⚠️ **Key idea: a file isn't always "just a picture" or "just a document".**

DEMO: WHEN A "DOCUMENT" STRIKES INSTANTLY

🖱️ I open an ordinary-looking document file in the browser…

→ 😱 it shows "**You've been hacked!**" and **downloads** a file to the computer by itself.

I didn't press any "Enable" — just **opening** it was enough.

✅ **Defense: don't open unexpected attachments, not even "invoices" and "documents". In doubt, ask the sender through a second channel.**

WHICH FILES CAN BE DANGEROUS

We don't show working malware — the **reflex** is what matters:

- 📊 **Office with "Enable Content"** — that means "I allow code to run". A legitimate document doesn't ask for this.
- 📄 **PDF / HTML** — can contain scripts and lead to a fake login.
- 🗜️ **Archives (especially password-protected)** — hide the payload, bypass antivirus.

✅ **Defense: don't enable macros; don't open unexpected attachments; turn on file extensions (so you catch `invoice.pdf.exe`).**

8. 🆕 MODERN ATTACKS

When even MFA doesn't always save you

MFA: PROTECTS VERY WELL — BUT NOT 100%

MFA (two-factor) is one of the strongest defenses. Turn it on **everywhere**.

But it gets bypassed too:

- 🔁 they send "Approve?" pushes again and again until the tired person taps "Yes" (that's how Uber was hacked).
- 🕵️ they steal an already **approved session** — getting in without a password and without a code.

✅ **Turn MFA on anyway — without it it's far worse. And the rule: "I didn't start a login → don't approve, press Report".**

THREAT LANDSCAPE: SUMMARY

ATTACK	WHAT IT TARGETS	SIMPLE DEFENSE
Phishing	attention	hover + pause + Report
Email forgery	trust	check the sender, second channel
Vishing / deepfake	trust in a voice	second channel + code word
Quishing	that you don't see the URL	read the address from the camera
MFA bypass	your fatigue	don't approve what you didn't ask for

9. 🏆 FINAL QUIZ

Let's test the reflex

KAHOOT — LET'S COMPETE!

🔗 (game code on the screen)

10–15 questions: "Phishing or not?" + "What to do?"

Host: launch Kahoot, give the code, have fun. Questions — in 40_quiz/final-quiz.md.

🎯 REMEMBER 5 THINGS

1. 🛑 **Pause** before you click — urgency is the signal.
2. 🔍 **Hover** over links, read the **domain** (right to left).
3. 📞 **Second channel** — verify the request, don't trust the email/voice.
4. 🔑 **Never** dictate a password/code — to anyone, anywhere.
5. 🚨 **Report** — your button makes everyone safer.

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

THANK YOU! 🙏

Questions?

📄 I'll hand out / send the cheat-sheet.

🔗 Google Phishing Quiz: phishingquiz.withgoogle.com

🔗 Check if your email has leaked: haveibeenpwned.com

Stay paranoid in moderation. 😉