PHISHING AWARENESS

WIE MAN PHISHING ERKENNT — UND WAS MAN DAGEGEN TUT

SPIELREGELN ⚠

> Alles hier ist **im Labor, mit Einwilligung, zur Verteidigung**.

Ihr habt das bei der Anmeldung bestätigt — deshalb kurz:
wir stellen Angriffe nach, damit ihr sie **erkennt**.

Wir greifen keine Menschen an.

WAS WIR DURCHGEHEN

1. Was Social Engineering ist + echte Fälle
2. 10 Anzeichen für Phishing
3. 🎮 Spiel „Phishing oder nicht?" (Google Quiz)
4. 🖥️ Live-Demo: GoPhish
5. 📱 Quishing (QR-Phishing)
6. 📞 Vishing + KI-Stimme / Deepfake
7. 🖼️ Versteckte und schädliche Dateien
8. 🆕 Moderne Angriffe: wenn selbst MFA nicht immer rettet
9. 🏆 Abschlussquiz

1. SOCIAL ENGINEERING

„Einen Menschen zu hacken ist leichter als ein System"

SOCIAL ENGINEERING ZIELT AUF EMOTIONEN, NICHT AUF CODE

Der Angreifer bricht nicht die Verschlüsselung — er bringt **euch** zum Klicken.

4 Hebel der Beeinflussung:

- ⏰ **Dringlichkeit** — „sofort machen, sonst…"
- 👔 **Autorität** — „hier ist der Chef / die IT / die Bank"
- 😱 **Angst** — „dein Konto wurde gehackt"
- 🎁 **Neugier/Gier** — „du hast gewonnen", „schau dir dieses Foto an"

> **Wenn eine Nachricht dich hetzen und fühlen lässt — das ist ein Warnsignal.**

ARTEN VON SOCIAL ENGINEERING

ART	KANAL	BEISPIEL
Phishing	E-Mail	„Ihr Microsoft-Konto ist gesperrt"
Smishing	SMS	„Ein DHL-Paket wartet, zahlen Sie 1 € nach"
Vishing	Anruf	„Hier ist die Bank, nennen Sie den Code aus der SMS"
Quishing	QR-Code	QR für „Parkgebühr" → Fake-Seite
BEC	E-Mail (Chef-Fälschung)	„Zahl dringend diese Rechnung, ich bin im Meeting"
Spear-Phishing	Gezielt	Eine Mail nur für dich, mit deinen Details

ECHTE FÄLLE (DAS IST KEINE THEORIE)

FALL	JAHR	WIE EINGEBROCHEN WURDE
Twitter (Musk, Obama)	2020	Vishing → interne Konsole
Uber	2022	MFA-Fatigue: 100 „Approve?"-Pushes
MGM / Caesars (Casinos)	2023	Anruf beim Helpdesk → MFA zurückgesetzt
Retool	2023	SMS + Anruf + AiTM kombiniert

Die Opfer waren nicht „dumm". Das waren Tech-Firmen mit MFA.

❌ KLASSISCHE KÖDER

> „Ihr Microsoft-Konto ist gesperrt. Melden Sie sich hier an."

> „Herzlichen Glückwunsch! Sie haben ein iPhone gewonnen 📱"

> „Prüfen Sie dringend die Rechnung (Anhang)."

> „Ungewöhnliche Anmeldung bei Ihrem Konto. Bestätigen Sie Ihre Identität."

Gemeinsam: Dringlichkeit + eine Handlung + ein Link/Anhang.

2. WIE MAN PHISHING ERKENNT

10 Anzeichen

🔍 10 ANZEICHEN FÜR PHISHING

1. 🌐 **Seltsame Domain** (microsft-login.com, paypa1.com)
2. ✍️ **Fehler** im Text / seltsame Sprache
3. ⏰ **Dringlichkeit** und Druck
4. 😱 **Drohungen** („Konto wird gelöscht")
5. 📎 **Ungewöhnlicher Anhang** (.zip, .html, .iso)
6. 📷 **QR-Code** statt eines normalen Links
7. 🔑 **Fragt nach dem Passwort** / MFA-Code
8. 💳 **Fordert dringend Zahlung**
9. 👤 **Ungewöhnlicher Absender** (Name ≠ Adresse)
10. 🔗 **Verdächtige Links** (drüberfahren, nicht klicken!)

ANZEICHEN NR. 1 — DOMAIN UND ABSENDER

Der Absendername lügt. Die **Adresse** sagt die Wahrheit.

```
Von: Microsoft Security <no-reply@microsft-secure-login.ru>
                         ^^^^^^^^ Tippfehler ^^^ seltsame Zone
```

- `microsft` statt `microsoft` (Typosquatting)
- `paypa1` (eine „1" statt einem „l")
- `.ru` / `.xyz` / `.top` dort, wo man `.com` erwartet
- Subdomain der Lüge: `microsoft.login-verify.com` → die echte Domain ist `login-verify.com`!

✅ **Lies die Domain von rechts nach links: der letzte Teil vor `/` ist der echte Eigentümer.**

ANZEICHEN NR. 10 — LINKS (DRÜBERFAHREN!)

Der Linktext ≠ wohin er führt.

🖱️ **Probier es live** — fahr (NICHT klicken) über diesen „sicheren" Link:

https://www.paypal.com/secure

↳ Unten im Browser / im Tooltip erscheint die echte Adresse: `evil-login-verify.xyz`

✅ **Am Computer: mit dem Cursor drüberfahren, die URL unten am Bildschirm ansehen.**
✅ **Am Handy: lange drücken → Link anzeigen.**
✅ **Nicht sicher — nicht klicken, die Seite manuell aufrufen.**

UND WENN DIE MAIL PERFEKT AUSSIEHT?

Modernes Phishing hat **keine** Fehler (KI schreibt fehlerfrei).
Dann hilft ein **Prozess**, kein „Bauchgefühl":

- 🛑 **Pause.** Drängt die Mail zur Eile? Das ist schon ein Signal.
- 📞 **Zweiter Kanal.** Ruf an / frag direkt — antworte nicht auf die Mail selbst.
- 🔐 **Niemals** Passwort/Code über einen Link aus einer Mail eingeben.
- 🚩 **Melden-Button** in Gmail/Outlook — nutz ihn.

> **Verify, don't trust.** Das ist Zero Trust für Menschen.

3. 🎮 SPIEL „PHISHING ODER NICHT?"

Wir stimmen gemeinsam ab

GOOGLE PHISHING QUIZ (JIGSAW)

📱 Vom Bildschirm scannen —
selbst durchgehen
🔗 **phishingquiz.withgoogle.com** ↗️

Regeln:

1. Wir sehen uns gemeinsam eine Beispiel-Mail an.
2. Wir stimmen ab: ✋ **Phishing** oder 🤚 **Legitim**?
3. Wir besprechen **warum** — worauf man achten muss.

4. 💻 GOPHISH — LIVE-DEMO

Wie ein Angriff von innen aussieht

WAS IST GOPHISH

Eine Open-Source-Plattform für **legale** Phishing-Simulationen.

Sie zeigt, was der Angreifer sieht:

- 📧 wer die Mail **erhalten** hat
- 👁️ wer sie **geöffnet** hat
- 🖱️ wer den Link **geklickt** hat
- ⌨️ wer **Daten eingegeben** hat auf der Fake-Seite

> ⚠️ **Nur eigene Testkonten / mit Einwilligung. Passwörter in der Demo sind Fake.**

GOPHISH: ANATOMIE EINER KAMPAGNE

```
Sending Profile   →  wer sendet (SMTP)
      +
Email Template    →  die Mail selbst (HTML, mit {{.FirstName}})
      +
Landing Page      →  gefälschte Login-Seite (+ Datenerfassung)
      +
Users & Groups    →  an wen wir senden (Testkonten)
      =
        Campaign  →  Start + Echtzeit-Dashboard
```

Der Schutz, den man hier sieht: technische Mail-Prüfungen erschweren die Zustellung der Fälschung.

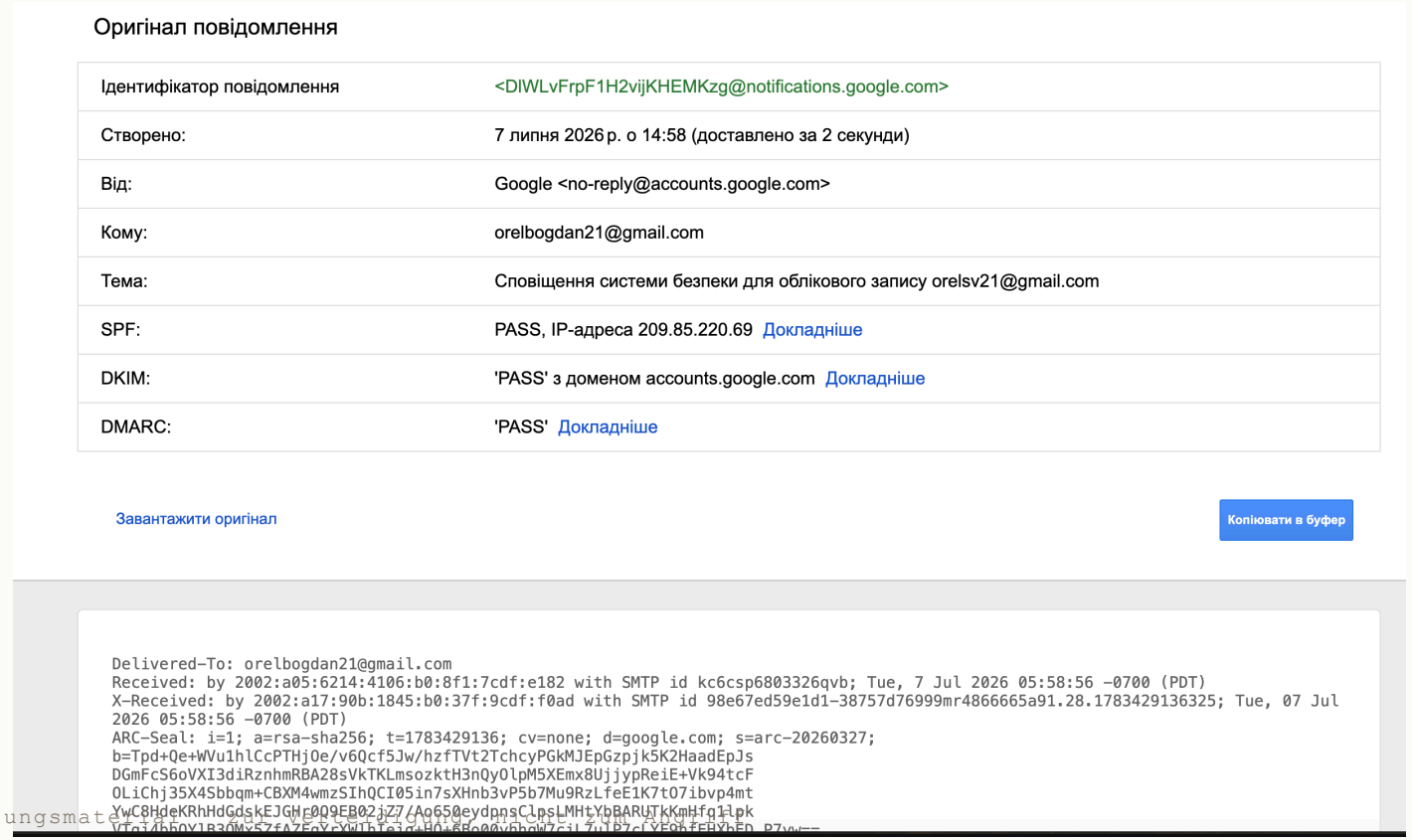
GOPHISH: WAS ES FÜR DIE VERTEIDIGUNG LEHRT

- 📊 Man sieht, **wie leicht** geklickt wird — ohne Vorwurf.
- 🏷️ Ein rotes „[EXTERNAL]"-Banner bei Mails von außen — einfach, aber wirksam.
- ✅ **Technische Mail-Prüfungen** — erschweren die Absender-Fälschung.
- 🚨 Der **Phishing-melden**-Button macht Opfer zu Sensoren.
- 🔁 Regelmäßige Simulationen senken die Klickrate mit der Zeit.

DER BLICK „UNTER DIE HAUBE" DER MAIL

Eine Mail hat **technische Prüfungen**, ob der Absender echt ist — die macht die Mail-Infrastruktur selbst.

In Gmail: ⋮ → **„Original anzeigen"**:



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
```

5. 📱 QUISHING (QR-PHISHING)

Wenn der Link in einem Bild versteckt ist

QUISHING — WARUM ES GEFÄHRLICH IST

Ein QR-Code = ein Link, den du **nicht mit den Augen siehst**.

- Umgeht E-Mail-Filter (es ist ja ein Bild!)
- Am Handy ist die URL schwerer zu prüfen
- Oft in PDF-„Rechnungen", an „Parkautomaten", auf „Speisekarten"

🔴 **Mit dem Handy scannen** → sieh, was passiert (unsere Seite)

✅ **Schutz: die Kamera zeigt die URL vor dem Öffnen — lies sie. Scann keine QR-Codes von zufälligen Aufklebern.**

6. 📞 VISHING + KI-STIMME

„Hallo, hier ist der Chef…"

AUCH STIMME UND VIDEO SIND KEIN BEWEIS

📞 Ein Anruf „vom Chef": Autorität + Dringlichkeit + vertraute Stimme.

Warum es funktioniert:

- 👔 Autorität („hier ist der Chef / die IT / die Bank")
- ⏰ Dringlichkeit („ich bin im Meeting, schnell")
- 🧠 wir sind gewohnt, einer vertrauten Stimme zu trauen

> **Ein KI-Stimmenklon entsteht aus wenigen Sekunden Aufnahme.**
> **Deepfake-Video ist ebenfalls schon Realität.**

KI-STIMME UND DEEPFAKE: WOZU DAS SCHON FÄHIG IST

📹 **Wir schauen 1–2 kurze Videos** — wie überzeugend Stimm- und Gesichtsfälschungen geworden sind.

- Stimmenklon aus wenigen Sekunden Aufnahme.
- Deepfake-Video in Echtzeit (Zoom-Anruf „von der Führungskraft").

💸 **2024: eine Firma in Hongkong verlor 25 Mio. $ — Überweisung nach einem Deepfake-Videoanruf „vom Finanzchef".**

✅ **Fazit: Stimme und Video sind kein Identitätsnachweis mehr.**

VISHING: DIE REGEL „ZERO TRUST FÜR DIE STIMME"

Selbst wenn die Stimme zu 100 % wie der Chef klingt:

- 🛑 **Stopp**, wenn nach Folgendem gefragt wird: Passwort, MFA-Code, Überweisung, Gutscheinkarten.
- 📞 **Ruf zurück** an eine Nummer, die du **kennst** (nicht die, die angerufen hat).
- 🔑 Ein **Codewort** für dringende Geldbitten.
- 🤝 Kein seriöser Dienst **fragt** per Stimme nach dem Passwort.

> **Die Stimme ist kein Identitätsnachweis mehr.**

7. 🖼️ VERSTECKTE UND SCHÄDLICHE DATEIEN

Wenn ein „Dokument" nicht das ist, was es scheint

DATEN LASSEN SICH IN EINER NORMALEN DATEI VERSTECKEN

🖼️ In einem normalen Foto kann **versteckter Text** stecken — das Auge sieht keinen Unterschied, die Größe bleibt fast gleich.

Das nennt man **Steganografie**. So versteckt man Daten (oder Befehle für Schadsoftware) „vor aller Augen".

> ⚠️ **Kernidee: eine Datei ist nicht immer „nur ein Bild" oder „nur ein Dokument".**

DEMO: WENN EIN „DOKUMENT" SOFORT ZUSCHLÄGT

🖱️ Ich öffne eine ganz normal aussehende Dokument-Datei im Browser…

→ 😱 sie zeigt „**Du wurdest gehackt!**" und **lädt selbst** eine Datei auf den Computer.

Kein „Enable" gedrückt — es genügte, sie zu **öffnen**.

✅ **Schutz: keine unerwarteten Anhänge öffnen, auch keine „Rechnungen" und „Dokumente". Im Zweifel den Absender über einen zweiten Kanal fragen.**

WELCHE DATEIEN GEFÄHRLICH SEIN KÖNNEN

Wir zeigen keine echte Schadsoftware — wichtig ist der **Reflex**:

- 📊 **Office mit „Enable Content"** — das heißt „ich erlaube Code-Ausführung". Ein legitimes Dokument verlangt das nicht.
- 📄 **PDF / HTML** — können Skripte enthalten und auf einen Fake-Login führen.
- 🗜️ **Archive (besonders mit Passwort)** — verstecken die Payload, umgehen den Virenscanner.

✅ **Schutz: keine Makros aktivieren; keine unerwarteten Anhänge öffnen; Dateiendungen einblenden (so erkennst du `rechnung.pdf.exe`).**

8. 🆕 MODERNE ANGRIFFE

Wenn selbst MFA nicht immer rettet

MFA: SCHÜTZT SEHR STARK — ABER NICHT ZU 100 %

MFA (Zwei-Faktor) ist einer der stärksten Schutzmechanismen. Aktiviere sie **überall**.

Aber auch sie wird umgangen:

- 🔁 Sie schicken „Approve?"-Pushes immer wieder, bis der müde Mensch „Yes" drückt (so wurde Uber gehackt).
- 🕵️ Sie stehlen die bereits **bestätigte Sitzung** — und kommen ohne Passwort und ohne Code rein.

✅ **Aktiviere MFA trotzdem — ohne sie ist es um ein Vielfaches schlimmer. Und die Regel: „ich habe den Login nicht ausgelöst → nicht bestätigen, Report drücken".**

BEDROHUNGSLAGE: ZUSAMMENFASSUNG

ANGRIFF	WORAUF ER ZIELT	EINFACHER SCHUTZ
Phishing	Aufmerksamkeit	Hover + Pause + Report
Mail-Fälschung	Vertrauen	Absender prüfen, zweiter Kanal
Vishing / Deepfake	Vertrauen in die Stimme	zweiter Kanal + Codewort
Quishing	dass du die URL nicht siehst	Adresse aus der Kamera lesen
MFA-Umgehung	deine Müdigkeit	nicht bestätigen, was du nicht angefragt hast

9. 🏆 ABSCHLUSSQUIZ

Testen wir den Reflex

KAHOOT — WIR MESSEN UNS!

🔗 (Spielcode auf dem Bildschirm)

10–15 Fragen: „Phishing oder nicht?" + „Was tun?"

Moderation: Kahoot starten, den Code geben, Spaß haben. Fragen — in 40_quiz/final-quiz.md.

🎯 MERK DIR 5 DINGE

1. 🛑 **Pause** vor dem Klick — Dringlichkeit ist das Signal.
2. 🔍 **Hover** über Links, lies die **Domain** (von rechts nach links).
3. 📞 **Zweiter Kanal** — prüf die Bitte, trau weder der Mail noch der Stimme.
4. 🔑 **Niemals** Passwort/Code durchgeben — niemandem, nirgends.
5. 🚨 **Melden** — dein Button macht alle sicherer.

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

DANKE! 🙏

Fragen?

📄 Das Merkblatt teile ich aus / schicke ich.

🔗 Google Phishing Quiz: phishingquiz.withgoogle.com

🔗 Prüf, ob deine E-Mail geleakt ist: haveibeenpwned.com

Bleibt in Maßen paranoid. 😉