AUFGEDECKT & ABGESICHERT

Entwickelt von Global Shapers Munich

SPIELREGELN I

Ziel des Memorys “Aufgedeckt & Abgesichert” ist es, spielerisch etwas über Betrugsmaschen und Sicherheit im digitalen Alltag zu lernen.

So läuft das Spiel ab:

1. Einteilung in Gruppen von 4 Personen.
2. Gespielt wird in 3 Runden à 20 Minuten mit je einem anderen Kartensatz:
   - Runde 1: *Begriffe & Erklärungen*
   - Runde 2: *Betrugsmaschen & Verhaltenstipps*
   - Runde 3: *Beispielbetrug & Warnzeichen*

SPIELREGELN II

3. Jede Karte hat ein bestimmtes Schwierigkeitslevel, das rechts oben erkennbar ist.
4. Memory-Spielregeln:
    - Es werden immer zwei Karten aufdeckt und geschaut, ob sie zusammenpassen.
    - Wenn sie zusammenpassen, darf der/die Spieler:in sie behalten.
    - Wenn nicht, kommen sie wieder verdeckt zurück und der/die nächste Spieler:in ist dran.
    - Ziel ist es, möglichst viele Paare zu finden.
5. Am Ende jeder Runde werfen wir einen gemeinsamen Blick auf die Karten: Was war neu? Gibt es offene Fragen?
6. Nach jeder Runde werden die Gruppen neu gemischt.

.

AUFGEDECKT & ABGESICHERT

TEIL 1

PASSWORD
(PASSWORT)

Ein geheimes Wort oder eine Zeichenfolge, mit der man sich in ein Konto einloggt

Du benutzt ein Passwort, um auf dein E-Mail-Konto oder Social Media zuzugreifen.

USERNAME
(BENUTZERNAME)

Der Name, den du wählst, um dich auf einer Website oder App zu identifizieren. Wird oft zusammen mit dem Passwort verwendet.

SCAM

Im Internet bezeichnet ein Scam betrügerische Aktivitäten, um an Geld, persönliche Daten oder Gefallen zu kommen.

PHISHING

Eine Methode durch die man über fiktive/ gefälschte Webseiten, über E-Mails oder über andere Nachrichten persönliche Daten einer Person erlangt. Diese werden anschließend meist für illegale Zwecke genutzt.

Eine gefälschte Nachricht (meist E-Mail oder Link), die dich dazu bringen will, persönliche Daten preiszugeben. Beispiel: Eine gefälschte E-Mail, die so tut, als käme sie von deiner Bank.

GEHACKT WORDEN SEIN

Bedeutet, dass jemand ohne Erlaubnis in deinen Computer, dein E-Mail-Konto oder ein anderes Online-Konto eingedrungen ist. Die Person kann dann deine Daten stehlen oder etwas in deinem Namen machen – zum Beispiel Nachrichten verschicken oder Geld überweisen.

TWO-FACTOR AUTHENTICATION (ZWEI-FAKTOR-AUTHENTIFIZIERUNG)

Ein zweiter Schritt zur Bestätigung deiner Identität (z. B. ein Code aufs Handy). Macht dein Konto sicherer.

PUBLIC WI-FI (ÖFFENTLICHES WLAN)

Kostenloses Internet z. B. in Cafés oder Flughäfen. Oft unsicher, deshalb keine Passwörter oder Bankdaten eingeben.

BROWSER

Das Programm, mit dem du ins Internet gehst.

Beispiele: Chrome, Safari, Firefox.

TAB
(TAB /REGISTERKARTE)

Eine offene Seite im Webbrowser. Man kann viele Tabs gleichzeitig öffnen.

POP-UP

Ein kleines Fenster oder Werbung, das sich über einer Seite öffnet.

LINK
(HYPERLINK)

Ein anklickbarer Text oder Bild, das dich zu einer anderen Seite führt. Oft unterstrichen oder in einer anderen Farbe.

HACKER

Jemand, der in Computer oder Netzwerke einbricht – oft um Daten zu stehlen oder Schaden zu verursachen.

SPAM

Unerwünschte oder nervige E-Mails, meist Werbung. Enthalten manchmal gefährliche Links.

CLOUD

Speicherplatz im Internet (nicht auf deinem Gerät).

Beispiele: Google Drive, iCloud.

ACCOUNT RECOVERY (KONTOWIEDERHER-STELLUNG)

Schritte, um dein Konto zurückzubekommen, wenn du z. B. dein Passwort vergisst. Oft über E-Mail, Handy oder Sicherheitsfrage.

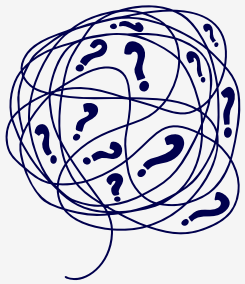
APP
(ANWENDUNG)

Ein Programm, das du auf deinem Handy oder Computer benutzt.

Beispiele: WhatsApp, YouTube, Zoom.

AUFGEDECKT & ABGESICHERT

TEIL 2



PHISHING
E-MAIL

BEDROHUNG

„Sie erhalten eine E-Mail, in der steht, dass Ihr Bankkonto geschlossen wird, wenn Sie nicht sofort auf einen Link klicken.“

TIPP!

Klicken Sie niemals auf Links in unerwarteten E-Mails – rufen Sie stattdessen direkt bei Ihrer Bank an.

ANHANG VON UNBEKANNTEM ABSENDER

BEDROHUNG

„Du erhälst eine E-Mail mit einem Anhang von jemandem, den du nicht kennst.“

TIPP!

Öffne keine unbekannten Anhänge – sie könnten Viren enthalten.

ENKELTRICK

BEDROHUNG

„Dein ‚Enkelkind' schreibt eine Nachricht und bittet um Geld, weil es in Schwierigkeiten steckt."

TIPP!

Rufe ihn oder ein anderes Familienmitglied an, um es zu bestätigen – schicke niemals Geld. Vereinbart ein Familienpasswort.

VERDÄCHTIGER LINK

BEDROHUNG

„Eine Nachricht fordert dich auf, auf einen Link zu klicken, der seltsam aussieht oder Rechtschreibfehler enthält.“

TIPP!

Prüfen den Link genau – wenn du dir nicht sicher bist, klicke nicht darauf.

SCHWACHES PASSWORT

BEDROHUNG

„Dein Passwort ist 123456 oder dein Geburtsdatum.“

TIPP!

Verwende einen langen Satz oder eine schwer zu erratende Kombination, z. B. ‚RotesPferdSonnenuntergang91!

FALSCHER GEWINN

BEDROHUNG

„Du hast einen Preis gewonnen – gib hier deine Kreditkarte ein, um ihn zu erhalten!“

TIPP!

Echte Gewinne fordern niemals eine Zahlung – das ist ein Betrug.

PAKETZUSTELLUNGS-BETRUG

BEDROHUNG

„Du erhälst eine SMS, dass dein Paket nicht zugestellt werden kann – klicke, um das Problem zu beheben.“

TIPP!

Wenn du nichts bestellt hast, handelt es sich wahrscheinlich um einen Betrug. Klicke nicht.

VERDÄCHTIGE FREUNDSCHAFTS-ANFRAGE

BEDROHUNG

„Jemand, den du nicht kennst, sendet dir eine Freundschaftsanfrage auf Facebook.“

TIPP!

Akzeptiere nur Leute, die du auch im wirklichen Leben kennst.

MERKWÜRDIGE KONTOAKTIVITÄT

BEDROHUNG

„Du erhälst eine Benachrichtigung, dass sich jemand in dein Konto eingeloggt hat.“

TIPP!

Ändern Sie Ihr Passwort sofort und aktivieren Sie die 2-Schritt-Verifizierung.

TÄUSCHEND ECHTE WEBSITE

BEDROHUNG

„Du besuchst eine Website, die aussieht wie dein Bank, aber eine seltsame Internetadresse hat.“

TIPP!

Prüfe die Adresse der Website sorgfältig - achte auf 'https' und Rechtschreibfehler.

TECH SUPPORT BETRUG

BEDROHUNG

„Du erhälst einen Anruf von einem Technikunternehmen wie Microsoft, das behauptet, dein Computer habe einen Virus.“

TIPP!

Lasse niemanden auf deinen Computer zugreifen. Beende das Telefonat und bitte jemanden, dem du vertraust, um Hilfe

SPENDENBETRUG

BEDROHUNG

„Du erhälst einen Anruf oder eine E-Mail mit der Bitte um Spenden für eine Wohltätigkeitsorganisation, von der du noch nie gehört hast.“

TIPP!

Überprüfe die offizielle Website der Wohltätigkeitsorganisation und spende kein Geld per Telefon oder über unbekannte Links.

ABOFALLE

BEDROHUNG

„Du klickst auf ein scheinbar kostenloses Angebot (z. B. ein Gewinnspiel oder Horoskop) – und merkst später, dass du ungewollt ein kostenpflichtiges Abo abgeschlossen hast.“

TIPP!

Lies das Kleingedruckte bei scheinbar kostenlosen Angeboten genau und klicke nicht unüberlegt auf „Jetzt anmelden“ oder „Weiter“.

QR-CODE-BETRUG

BEDROHUNG

"Du scannst einen QR-Code (z. B. auf einem Plakat oder Parkplatzautomaten), der zu einer gefälschten Website führt, um deine Daten oder Zahlungsinformationen zu stehlen."

TIPP!

Scanne QR-Codes nur von vertrauenswürdigen Quellen und überprüfe die URL, bevor du persönliche Daten eingibst.

AHHHH!

AUFGEDECKT & ABGESICHERT

TEIL 3

PHISHING
E-MAIL

Betreff: Wichtige Mitteilung zu Ihrem Konto

Von: sicherheit@onlinebanking-123.de

Hallo,
aus Sicherheitsgründen bitten wir Sie, Ihr Konto zu verifizieren. Klicken Sie dazu bitte auf Link:
👉 **https://onlinebanking-123-verifikation.com**
Ohne Verifizierung wird Konto innerhalb von 24 Stunden gesperrt.

Vielen Dank,
Ihre OnlineBanking 123

Die Absenderadresse wirkt offiziell, ist aber gefälscht.

Die E-Mail erzeugt künstlichen Zeitdruck ("innerhalb von 24 Stunden").

Es wird ein Link verwendet, der zu einer gefälschten Website führt.

Grammatik und Ausdruck können leicht unprofessionell wirken.

ANHANG VON UNBEKANNTEM ABSENDER

Betreff: Dringend - Offene Unterlagen zu Ihrem letzten Arztbesuch

---

Von: praxisverwaltung@gesund-check.de

Sehr geehrter Patient,
anbei finden Sie wichtige Dokumente zu Ihrem letzten Termin. Bitte öffnen Sie den Anhang umgehend zur weiteren Einsicht.
👉 Anhang: Befunde_April2025.zip
Bei Rückfragen wenden Sie sich bitte an unsere Praxis.

Mit freundlichen Grüßen
GesundCheck Praxisverwaltung

Der Absender klingt seriös, ist aber unbekannt.

Es wird ein allgemeiner, unpersönlicher Text verwendet.

Der Anhang ist eine ZIP-Datei – das ist ein häufiges Mittel zur Verbreitung von Schadsoftware.

Es wird indirekt Druck gemacht, aber ohne weitere konkrete Informationen.

ENKELTRICK

Sonntag, 5. Januar
+49/34780h2384234890234780234

Hallo Oma, mein Handy ist kaputt – ich schreibe dir von meiner neuen Nummer. Bitte speicher sie ab!

Ich bin gerade total im Stress... Ich muss heute noch dringend eine Rechnung bezahlen, aber mein Onlinebanking funktioniert nicht. 😞
Kannst du mir bitte aushelfen und das kurz für mich überweisen? Ich schick dir gleich die Daten. Ich zahl's dir natürlich sofort zurück! ❤️

Meld dich bitte kurz!

Der Absender meldet sich von einer unbekannten Nummer ohne Namen.

Es wird suggeriert, dass das bisherige Handy nicht funktioniert – so soll verhindert werden, dass man über die „alte“ Nummer gegencheckt. Es wird ein technisches Problem vorgeschoben ("Onlinebanking geht nicht").

Es wird eine Mischung aus emotionaler Dringlichkeit ("Oma", Herz-Emoji) erzeugt.

VERDÄCHTIGER LINK

Betreff: Bestellbestätigung – bitte Angaben sofort prüfen

Von: service@obiii-baumarkt.com

Sehr geehrter Kunde,

bitte überprüfen Sie sofort Ihre Bestellung, um den Versand zu bestätigen:

👉 https://obiii-baumarkt-bestellung-check.com

Vielen Dank
Ihr Obiii Baumarkt Online-Team

Die Absenderdomain sieht professionell aus, gehört aber nicht zu einem bekannten Anbieter.

Der Link wirkt vertrauenswürdig, ist aber gefälscht ("obiii").

Es wird Druck aufgebaut („bitte überprüfen Sie sofort“), obwohl keine echte Bestellung existiert.

SCHWACHES PASSWORT

Passwort:

"123456"

oder

“12/11/1951”

Zu kurz: weniger als 8–10 Zeichen sind schnell zu knacken.
Einfache Muster: Reihenfolgen wie 123456, abcdef, qwertz.
Keine Sonderzeichen oder Großbuchstaben: Passwörter nur aus Kleinbuchstaben oder nur Zahlen sind schwach.
Persönliche Daten: Name, Geburtsdatum, Wohnort – leicht zu erraten, wenn jemand etwas über Sie weiß.
Wiederverwendung: Dasselbe Passwort für mehrere Accounts genutzt – ein großes Risiko!

FALSCHER GEWINN

Betreff: Sie haben ein Samsung Galaxy S24 gewonnen!

Von: info-center@gewinn.com

Zur Bestätigung Ihres Gewinns zahlen Sie bitte 1,00 € Versandkosten.

Geben Sie dazu noch heute Ihre Kreditkartendaten auf folgender Seite ein:
👉 https://sicher-gewinn24.com/zahlung

Nur noch heute verfügbar – jetzt sichern! 📦✨

Kurze, reißerische Nachricht – keine Details zur Gewinnspiel Teilnahme oder Veranstalter.

Keine persönliche Ansprache.

Vortäuschung eines Minibetrags (1 €), um an die kompletten Kreditkartendaten zu kommen.

Dringlichkeit: Nur heute gültig → Druck wird aufgebaut.

Link auf eine unbekannte/gefälschte Website.

PAKETZUSTELLUNGS-BETRUG

Betreff: Paketzustellung (Dringend!)

Von: paketinfo@web.com

📦 Ihr Paket konnte heute nicht zugestellt werden!

Bitte bestätigen Sie Ihre Adresse und Zahlungsdaten unter folgendem Link, um eine neue Zustellung zu vereinbaren:
👉 https://dhll-paket-verfolgen-online.com

Achtung: Ohne Bestätigung wird Ihr Paket umgehend an den Absender zurückgeschickt!

Falscher Absender: Oft steht nur "DHL", "Paketinfo" oder eine unbekannte Nummer.
Keine Details: Keine Sendungsnummer, keine genauen Angaben zum Paket.
Verdächtiger Link: Der Link sieht auf den ersten Blick normal aus, gehört aber nicht zur echten DHL-Seite.
Dringlichkeit: "umgehend an den Absender zurück" → setzt unter Druck.

VERDÄCHTIGE FREUNDSCHAFTS-ANFRAGE

Absender: Profil einer fremden, oft sehr sympathisch oder attraktiv wirkenden Person ("Markus L.", "Sophie M.", oft mit perfekt wirkenden Fotos)

Hallo liebe/r [dein Name],
ich habe zufällig dein Profil entdeckt und konnte nicht widerstehen, dir zu schreiben. 😊
Bist du gerade auch auf der Suche nach echten Gefühlen? ❤️

Schreib mir doch direkt auf WhatsApp:
👉 +49 123 4567890

Perfekte Bilder: Die Fotos sind oft von Models oder gestohlen aus echten Profilen.

Unbekannte Person: Keine echte Verbindung oder gemeinsame Freunde.

Schnelle Kontaktaufnahme: Sofortige Nachricht nach Annahme der Anfrage.

Schnelle Emotionen: Nach ein paar Nachrichten sprechen sie von „Liebe“ oder „Seelenverwandtschaft“

Vorschlag, die Plattform zu wechseln: Meist auf WhatsApp, Telegram oder E-Mail, damit Facebook nicht dazwischenfunkt.

Bald kommt eine Notlage: Nach einigen Tagen oder Wochen wird plötzlich Geld gebraucht (z.B. für Krankenhauskosten)

MERKWÜRDIGE KONTOAKTIVITÄT

Betreff: Ungewöhnliche Anmeldung bei Ihrem Konto erkannt

Von: sicherheitsdienst@bank-support-online.com

Sehr geehrter Kunde,
wir haben eine Anmeldung von einem unbekannten Gerät festgestellt:
Standort: Lagos, Nigeria
Zeit: 26. April 2025, 14:35 Uhr
Wenn diese Anmeldung von Ihnen stammt, können Sie diese Nachricht ignorieren.
Wenn nicht, sichern Sie bitte sofort Ihr Konto:
👉 Konto jetzt schützen

Ihr Sicherheitsteam

Verdächtige Absenderadresse: z. B. nicht von der offiziellen Domain Ihrer Bank oder Ihres Dienstes ("sicherheitsdienst@bank-support-online.com")

Keine persönliche Ansprache: Oft nur "Sehr geehrter Kunde" statt deines echten Namens.

Druck: „Sichern Sie bitte sofort Ihr Konto“ → erzeugt Stress, damit man unüberlegt klickt.

Link führt auf eine gefälschte Website: Ziel ist es, Login-Daten zu klauen.

TÄUSCHEND ECHTE WEBSITE

https://www.meinebannk-login.de

So sieht die gefälschte Seite aus:

Logo und Farben der echten Bank perfekt kopiert.

Login-Felder für Benutzername und Passwort genau wie im Original.

Sicherheits-Icons (z. B. ein kleines Schloss-Symbol) täuschen Vertrauen vor.

Hinweis: „Diese Verbindung ist sicher“ – obwohl die Seite gefälscht ist.

Manchmal sogar ein gültiges SSL-Zertifikat (https://), damit es „vertrauenswürdig“ wirkt.

Tippfehler: Kleine Tippfehler in der Webadresse (z. B. „bannk“).

Komischer Aufbau: Manche Buttons oder Links funktionieren nicht oder leiten auf andere Seiten weiter.

Ungewöhnliche Aufforderungen: Nach vollständiger Kreditkartennummer oder PIN wird gefragt (echte Banken tun das nie!).

Druck: Meldungen wie „Ihr Konto wird gesperrt, wenn Sie sich nicht sofort anmelden.“

TECH SUPPORT BETRUG

Pop-up-Fenster auf dem Bildschirm:

⚠️ Achtung! Ihr Computer ist gesperrt!

Ihr System hat ungewöhnliche Aktivitäten festgestellt.
Virus erkannt! Ihre persönlichen Daten sind in Gefahr.

Bitte rufen Sie sofort Microsoft-Support, um Ihr Gerät zu entsperren:

📞 0800 123 4567

Ignorieren Sie Warnung nicht – Ihr Computer wird in 5 Minuten gesperrt!

Panikmache: Große Warnmeldungen und Countdown-Zeiten sollen Sie in Stress versetzen.

Angeblicher Support von großen Marken: Microsoft, Apple oder andere Anbieter werden missbraucht – echte Unternehmen rufen Sie nie ungefragt an oder schicken Pop-ups.

Telefonnummer führt zu Betrügern: Diese wollen dann Fernzugriff auf Ihren Computer oder fordern Geld für angebliche "Reparaturen".

Fehlerhafte oder sehr allgemeine Sprache: Oft sind Grammatik und Formulierungen etwas merkwürdig.

SPENDENBETRUG

Betreff: Hilfe dringend benötigt – retten Sie Leben noch heute!

Von: hilfjetzt@katastrophenhilfe-global.org

Lieber Unterstützer,

nach dem schrecklichen Erdbebensind tausende Familien obdachlos.

Bitte überweisen Sie Ihre Spende auf folgendes Konto:
IBAN: EE32 2200 2210 2014 5587

Achtung: Ohne Ihre sofortige Hilfe drohen schlimme Folgen für betroffene Kinder und Familien.

Unprofessionelle Gestaltung: Allgemeine Anrede („Lieber Unterstützer“), sonderbare Formulierungen („drohen schlimme Folgen“).

Ungewöhnliche IBAN: Ein estnisches Konto (EE…), obwohl es sich angeblich um eine deutsche Katastrophenhilfe handelt.

Keine Details zur Verwendung: Nur vage Angaben („für betroffene Kinder und Familien“), nichts Konkretes zu Hilfsprojekten oder Einsatzorten.

Fehlende Kontaktdaten: Keine Website, keine Adresse, keine Telefonnummer.

ABOFALLE

Betreff: Ihr kostenloser Zugang zu exklusiven Rezepten wartet! 🍝📖

Von: gourmetrezepte@deluxe-kochen.com

Holen Sie sich jetzt kostenfrei Zugang zu unserer exklusiven Rezepte-Sammlung!
✔️ Über 5.000 Rezepte
✔️ Täglich neue Ideen
✔️ Nur heute gratis testen!
👉 Jetzt kostenlos registrieren: https://rezepte-deluxe-kostenlos.com

Kleingedruckt (ganz unten, kaum sichtbar): Nach Ablauf der 3-tägigen Testphase wird automatisch ein Abo für 49,90 € pro Monat abgeschlossen.

Verlockendes Angebot: Ein wertvoller, aber angeblich kostenfreier Service wird angeboten.

Druck durch Zeitlimit: Nur heute, nur jetzt verfügbar.

Versteckte Kosten: Das Abo wird nur im schwer lesbaren Kleingedruckten erwähnt.

QR-CODE-BETRUG

Situation

In einer Stadt findest du einen Aufkleber auf einem Parkautomaten.
Darauf ist ein großer QR-Code mit dem Text:

"Jetzt schnell und einfach Parkgebühr bezahlen! 📱🚗
Scannen Sie hier:"

Ungewöhnliche Platzierung: QR-Codes auf Aufklebern, die nicht professionell aussehen (schief geklebt, etc.).

Keine klare Herkunft: Kein Logo oder Hinweis, dass der Code wirklich von der Stadt / dem Betreiber stammt.

Seltsame Webadresse: Die URL nach dem Scannen sieht komisch aus, z. B. www.stadtparkplatz-gebuehr-jetzt24.ru statt www.stadtname.de.

Direkte Zahlungsaufforderung: Ohne jede Verifikation oder Möglichkeit zur Prüfung.

RECHNUNGSBETRUG

Betreff: Zahlungserinnerung

Von: rechnungsstelle@business-service24.net

Sehr geehrte Kundin, sehr geehrter Kunde,

wir erinnern Sie an die noch offene Rechnung über 289,99 € für Ihre Bestellung. Bitte begleichen Sie den Betrag innerhalb von 5 Werktagen auf folgendes Konto:

IBAN: DE12 3456 7890 1234 5678 90
Die Rechnung finden Sie im Anhang als PDF.
Mit freundlichen Grüßen,
Ihr Kundenservice

Unbekannter Absender, der professionell klingt, aber nicht mit einem echten Geschäft in Verbindung steht.
Keine konkrete Angabe zur bestellten Ware oder Dienstleistung.
Druck durch Zahlungsfrist („innerhalb von 5 Werktagen“), um unüberlegtes Handeln zu provozieren
IBAN und Zahlungsempfänger wirken generisch oder unbekannt.
PDF-Anhang kann Schadsoftware enthalten