Name: _____ **Datum:** _____ **Punkte:** _____

Online-Betrug und Social Engineering Schutzleitfaden

E-Mail-Phishing, gefälschte Domains, Vishing, Support-Betrug, Überprüfung über einen separaten Kanal, BEC

LERNÜBERSICHT ONLINE-BETRUG

GESICHERT
DATENVERSCHLÜSSELUNG
256-Bit-AES-Standard

KONFORM
GLOBALE STANDARDS
Rahmenwerke DSGVO (GDPR) und CCPA

ZERO-TRUST
ZUGRIFFSRICHTLINIE
Mehr-Faktor-Authentifizierung

Willkommen! Dieses Aktivitätspaket führt Sie durch die Abwehr von Online-Betrug. Sie lernen gefälschte Phishing-Websites, Social-Engineering-Taktiken, Betrug mit angeblichem Support, Wege für Überweisungsbetrug und Methoden zur Zahlungsprüfung kennen.

KONTROLLPUNKTE DES ARBEITSBLATTS

- [ ] **Teil 1-4: Cybersicherheit und Bedrohungsabwehr beherrschen.**
- [ ] **Teil 5-7: Kreuzworträtsel und Suchsel lösen.**
- [ ] **Teil 8-9: Fallstudien und Chiffre-Aufgabe lösen.**
- [ ] **Teil 10: Seiten mit grundlegenden und fortgeschrittenen häufigen Fragen durchgehen.**
- [ ] **Teil 11: 10 interessante Fakten aus der Praxis entdecken.**
- [ ] **Bonus: Herausforderung Schnell denken.**

Cybersicherheits-Leitfaden von VPN.com öffnen

URL: https://www.vpn.com/de/cybersicherheit/online-betrug/

Ihr Lernfahrplan: Schutz vor Online-Betrug

- Typische Anzeichen von Support-Betrug und Typosquatting-Domains erkennen.
- E-Mail-Verifizierungsprotokolle (SPF, DKIM, DMARC) gegen Spoofing einsetzen.
- Führen Sie eine Überprüfung von Transaktionen über einen separaten Kanal ein, um Überweisungsbetrug in Unternehmen zu verhindern.

ANLEITUNG ZUM LEITFADEN ONLINE-BETRUG

Beantworten Sie die Auswahlaufgaben und Richtig/Falsch-Fragen, vervollständigen Sie die Lückensätze mithilfe der Wortliste, ordnen Sie die Definitionen zu und lösen Sie das Kreuzworträtsel und das Suchsel. Wenden Sie Ihr Wissen in folgenden Bereichen an: Schutz vor Online-Betrug. Zum Schluss folgt die Bonusaufgabe Schnell denken.

SCHUTZ VOR ONLINE-BETRUG UND SOCIAL ENGINEERING (EINFÜHRUNG)

Online-Betrug nutzt menschliches Verhalten durch Phishing, Support-Pop-ups, Vishing und Überweisungsbetrug aus. Die Durchsetzung einer Transaktionsprüfung über einen separaten Kanal sowie von SPF/DKIM/DMARC-Domainregeln hilft, Social-Engineering-Angriffswege schon am Gateway zu blockieren.

LESEN SIE JEDEN KONTROLLPUNKT SORGFÄLTIG UND WÄHLEN ODER SCHREIBEN SIE DIE RICHTIGE ANTWORT.

Kontrollpunkt 1: Auswahlaufgaben

1. Was ist das wichtigste Anzeichen für einen Support-Betrug?

- A. Ein Pop-up, das behauptet, Ihr System sei infiziert, und Sie auffordert, eine Telefonnummer anzurufen
- B. Ein automatisches Sicherheitsupdate, das aus einer offiziellen Registry heruntergeladen wird
- C. Ein Passwort-Manager, der Zugangsdaten auf einer Unternehmensdomain nicht ausfüllt
- D. Eine Hintergrund-Dateisicherung auf einem externen Laufwerk

2. Welche Technik nutzt gefälschte Absenderdomains, um Bankdaten zu stehlen?

- A. E-Mail-Phishing
- B. Portscan
- C. Speicherinjektion
- D. Crypto-Shredding

3. Was beschreibt Überweisungsbetrug?

- A. Opfer mithilfe von Social Engineering dazu bringen, Geld auf gefälschte Firmenkonten zu überweisen
- B. Verschlüsseln von Systemdatenbanken mit Ransomware-Nutzlasten
- C. Abfragen von Datenbanken mittels SQL-Injection-Befehlen
- D. Sichern von Systemdateien auf Offline-Speicherdatenträgern

4. Warum erstellen Betrüger gefälschte Online-Shops?

- A. Um Kreditkartendaten und Zahlungsinformationen von Käufern zu stehlen
- B. Um Datenbanktabellen für die Malware-Analyse in Sandboxes zu hosten
- C. Um die Lieferung von Online-Bestellungen zu beschleunigen
- D. Um neue Website-Designs kostenlos zu testen

5. Was bedeutet Vishing?

- A. Telefonbetrug (Voice-Phishing) über Telefonnetze, um Zugangsdaten zu stehlen
- B. Durchsuchen lokaler Netzwerke nach ungesicherten Systemgeräten
- C. Wiederherstellen von Systemdatenbanken nach einem unbefugten Eindringen
- D. Ausführen nicht vertrauenswürdigen Codes in sicheren virtuellen Containern

Kontrollpunkt 2: Richtig oder falsch

6 Frage 6

6. Phishing-Betrug richtet sich nur gegen Endnutzer, nie gegen Führungskräfte als Whaling-Ziele.

○ Richtig ○ Falsch

7 Frage 7

7. Gefälschte Domains verwenden oft kleine Tippfehler (wie amaz0n.com), um vertrauenswürdige Marken nachzuahmen.

○ Richtig ○ Falsch

8 Frage 8

8. Support-Betrug lässt sich lösen, indem man dem Anrufer Fernzugriff gewährt.

○ Richtig ○ Falsch

9 Frage 9

9. Social Engineering nutzt menschliche Psychologie wie Angst und Zeitdruck aus, um Sicherheitsregeln zu umgehen.

○ Richtig ○ Falsch

10 Frage 10

10. Überweisungsanfragen sollten immer über einen separaten, unabhängigen Kommunikationsweg (Out-of-Band) überprüft werden.

○ Richtig ○ Falsch

Kontrollpunkt 3: Schlüsselbegriffe einsetzen

Lesen Sie jeden der folgenden Sätze und füllen Sie die Lücke mit dem richtigen Begriff aus der Wortliste.

1. Betrügerische E-Mails, die Nutzer täuschen, nennt man _____ .

2. Webadressen, die vertrauenswürdige Marken nachahmen, sind _____ .

3. Telefonbetrug, der auf Bankdaten abzielt, nennt man _____ .

4. Ein Pop-up, das Geld für die Entfernung eines Virus verlangt, ist ein _____ mit vorgetäuschtem Support.

5. Um eine Zahlungsanforderung zu bestätigen, ist eine _____ über einen separaten Kanal erforderlich.

6. Die Umleitung von Geschäftstransaktionen auf Konten von Dieben erfolgt per manipulierter _____ .

WORTSCHATZ-WORTBANK

BETRUG GEFÄLSCHT PHISHING SMISHING ÜBERWEISUNG VERIFIZIERUNG VISHING WHALING

Schreiben Sie Ihre Antworten hier:

1. **2.**

3. **4.**

5. **6.**

Kontrollpunkt 4: Zuordnung von Sicherheits-Begriffen

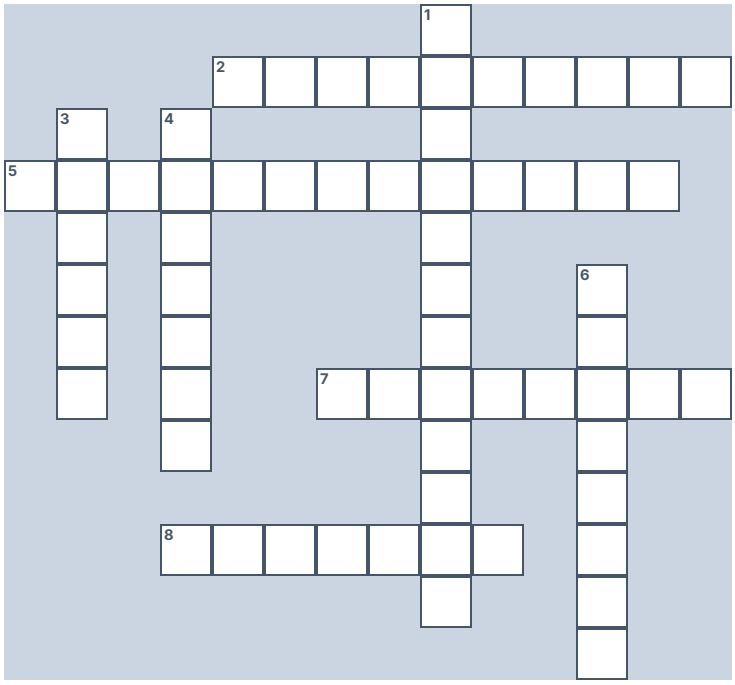
DEFINITIONEN ZUORDNEN

Ordnen Sie jeden Fachbegriff links der richtigen Definition rechts zu, indem Sie den passenden Buchstaben (A–H) in das ausfüllbare Eingabefeld schreiben.

☐	1. PHISHING	A	Betrügerische Umleitung von Banktransaktionen auf Konten von Kriminellen.
☐	2. GEFÄLSCHT	B	Betrugsmasche, mit der Opfern Geld oder Zugangsdaten gestohlen werden sollen.
☐	3. VISHING	C	Versenden betrügerischer SMS, um Zugangsdaten für Mobilfunkkonten zu stehlen.
☐	4. BETRUG	D	Betrügerische Anrufe, mit denen Anmeldedaten und Kontodaten gestohlen werden sollen.
☐	5. ÜBERPRÜFUNG	E	Gezielte Phishing-Angriffe, die darauf abzielen, Zugangsdaten von Führungskräften der obersten Ebene zu stehlen.
☐	6. KABEL	F	Nachgeahmte E-Mail-Absender- oder Website-Adresse, die echt aussehen soll.
☐	7. WHALING	G	Betrügerische E-Mail-Kampagnen, die Anmeldedaten und Passwörter stehlen sollen.
☐	8. SMISHING	H	Bestätigen von Zahlungsdetails über einen vertrauenswürdigen zweiten Kontaktweg.

Kontrollpunkt 5: Kreuzworträtsel

Lösen Sie das Kreuzworträtsel, indem Sie Buchstaben in die aktiven weißen Felder eingeben. Die Zahlen entsprechen den Hinweisen unten.



WAAGERECHT

2. So ist eine nachgeahmte Absender- oder Website-Adresse, die seriös wirken soll. (10)

5. Bestätigung von Zahlungsdetails über einen vertrauenswürdigen zweiten Kontaktweg. (13)

7. Betrügerische E-Mail-Kampagnen, mit denen Anmeldedaten und Passwörter gestohlen werden sollen. (8)

8. Gezielte Phishing-Angriffe, die Zugangsdaten von Führungskräften der C-Ebene stehlen sollen. (7)

SENKRECHT

1. Bei diesem Betrug werden Banktransaktionen auf Konten von Kriminellen umgeleitet. (12)

3. Masche, mit der Opfern Geld oder Zugangsdaten gestohlen werden sollen. (6)

4. Betrügerische Sprachanrufe, mit denen Zugangsdaten und Kontodetails gestohlen werden sollen. (7)

6. Versand betrügerischer SMS, um Zugangsdaten für Mobilfunkkonten zu stehlen. (8)

Kontrollpunkt 5, Alternative: Barrierefreie Kreuzworträtsel-Hinweise

Nutzer von Screenreadern und Tastatur können die Kreuzworträtsel-Antworten direkt in die Textfelder unten eingeben.

WAAGERECHT

2 waagerecht: So ist eine nachgeahmte Absender- oder Website-Adresse, die seriös wirken soll. (10 Buchstaben):

5 waagerecht: Bestätigung von Zahlungsdetails über einen vertrauenswürdigen zweiten Kontaktweg. (13 Buchstaben):

7 waagerecht: Betrügerische E-Mail-Kampagnen, mit denen Anmeldedaten und Passwörter gestohlen werden sollen. (8 Buchstaben):

8 waagerecht: Gezielte Phishing-Angriffe, die Zugangsdaten von Führungskräften der C-Ebene stehlen sollen. (7 Buchstaben):

SENKRECHT

1 senkrecht: Bei diesem Betrug werden Banktransaktionen auf Konten von Kriminellen umgeleitet. (12 Buchstaben):

3 senkrecht: Masche, mit der Opfern Geld oder Zugangsdaten gestohlen werden sollen. (6 Buchstaben):

4 senkrecht: Betrügerische Sprachanrufe, mit denen Zugangsdaten und Kontodetails gestohlen werden sollen. (7 Buchstaben):

6 senkrecht: Versand betrügerischer SMS, um Zugangsdaten für Mobilfunkkonten zu stehlen. (8 Buchstaben):

Kontrollpunkt 6: Suchsel

Finden Sie die 8 wichtigen Fachbegriffe, die im Gitter unten versteckt sind. Die Wörter können waagerecht, senkrecht oder diagonal verlaufen.

G I R Z S F Q G V F A A Q O N
N G P T X Q K E R U P S D N Y
U N G B F S X F W J H A R Z Y
S I U Y W L G A I M I R J M L
I H R T H O H E Q Q S H Z A O
E S T V A G U L B Y H R Y B H
W I E L L Z G S J O I P N W C
R M B M I Z Y C G Y N O W U K
E S V P N B N H V T G M G V D
B Y U K G R B T X Z Y M R Q X
E V E R I F I Z I E R U N G I
U P D A D J Q V W W L J H T H
G B V I S H I N G E I K T S V
R Z E H E S C A L Q C Z M K V
R U A S W J M M H H N H R F K

WORTSCHATZ-WORTLISTE

PHISHING GEFAELSCHT VISHING BETRUG VERIFIZIERUNG UEBERWEISUNG WHALING SMISHING

Kontrollpunkt 6, Alternative: Barrierefreie Begriffszuordnung

Ordnen Sie jeden der 8 Fachbegriffe aus dem Suchrätsel der richtigen Definition zu, indem Sie den Buchstaben (A–H) in die Lücke schreiben.

FACHBEGRIFFE

- **A. PHISHING**
- **B. GEFAELSCHT**
- **C. VISHING**
- **D. BETRUG**
- **E. VERIFIZIERUNG**
- **F. UEBERWEISUNG**
- **G. WHALING**
- **H. SMISHING**

DEFINITIONEN UND ZUORDNUNGSFELDER

1. So ist eine nachgeahmte Absender- oder Website-Adresse, die seriös wirken soll.
2. Bestätigung von Zahlungsdetails über einen vertrauenswürdigen zweiten Kontaktweg.
3. Bei diesem Betrug werden Banktransaktionen auf Konten von Kriminellen umgeleitet.
4. Versand betrügerischer SMS, um Zugangsdaten für Mobilfunkkonten zu stehlen.
5. Gezielte Phishing-Angriffe, die Zugangsdaten von Führungskräften der C-Ebene stehlen sollen.
6. Betrügerische Sprachanrufe, mit denen Zugangsdaten und Kontodetails gestohlen werden sollen.
7. Betrügerische E-Mail-Kampagnen, mit denen Anmeldedaten und Passwörter gestohlen werden sollen.
8. Masche, mit der Opfern Geld oder Zugangsdaten gestohlen werden sollen.

Kontrollpunkt 7: Buchstabensalat

Bringen Sie die Buchstaben unten in die richtige Reihenfolge, um zentrale Begriffe der Cybersicherheit aufzudecken. Schreiben Sie Ihre Antworten in die vorgesehenen Eingabefelder.

1. NSHPIHGI
2. VSGNIHI
3. EVIRENGRZFI UI
4. GHILNWA
5. CLTEASEGHF
6. URBTGE
7. ISRUEEGUNB WE
8. SMHGSNII

Bonusaufgabe: Schnell denken

3 ANTWORTEN PRO KATEGORIE. WER DIE LISTE ZUERST VOLLSTÄNDIG AUSFÜLLT, GEWINNT.

1	Geräte, die gehackt werden können			
2	Sätze, die Betrüger häufig verwenden			
3	Zahlungsmethoden, die Betrüger verlangen			
4	Arten von Online-Betrug			
5	Angebote, die zu gut sind, um wahr zu sein			
6	Stellen, bei denen Sie einen Betrug melden können			
7	Wörter rund um Cybersicherheit			
8	Personen, die Sie vor Betrug warnen können			
9	Dinge, von denen Sie ein Backup machen			
10	Warnzeichen in einer E-Mail			
11	Anzeichen, dass ein Computer infiziert ist			
12	Möglichkeiten, einen Onlineshop zu überprüfen			
13	Möglichkeiten, Ihre Konten zu schützen			
14	Dinge, die zu tun sind, wenn Sie betrogen wurden			
15	Dinge, die nach einem Datenleck zu tun sind			

Kontrollpunkt 8: Fallstudien zur Cybersicherheit

Wenden Sie die erlernten Konzepte an, um die folgenden praxisnahen Szenarien zu lösen.

FALLSTUDIE 1: VERHINDERUNG VON BETRUG MIT FIRMENÜBERWEISUNGEN



Szenario: Eine Finanzabteilung erhält eine dringende E-Mail von einer gefälschten Lieferantenadresse mit der Aufforderung, künftige Rechnungsüberweisungen an eine neue Bankverbindung zu senden.

Diskussionsfrage: Beschreiben Sie eine Richtlinie zur Überprüfung von Überweisungen und nennen Sie Sperren durch E-Mail-Authentifizierung.

FALLSTUDIE 2: WHALING-PHISHING-VORFALL AUF FÜHRUNGSEBENE



Szenario: Eine Führungskraft hat auf einen Phishing-Link geklickt, der angeblich zu einem vertraulichen Dokument für eine Vorstandssitzung führte, und ihre wichtigsten Firmenzugangsdaten auf einem gefälschten Portal eingegeben.

Diskussionsfrage: Beschreiben Sie die Schritte der Vorfallsreaktion und erklären Sie, wie sich die Anmeldungen der Führungskraft prüfen lassen.

Kontrollpunkt 9: Entschlüsselung der Chiffre

Eine Fachkraft für Cybersicherheit schützt Netzwerkressourcen vor Bedrohungsakteuren im Internet. Entschlüsseln Sie mithilfe des Buchstaben-Zahlen-Schlüssels unten die Nachricht, indem Sie die passenden Buchstaben in die Lücken schreiben.

SCHLÜSSEL FÜR DIE BUCHSTABEN-ZAHLEN-VERSCHLÜSSELUNG

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

5	18	11	5	14	14	5	14		19	9	5		16	8	9	19	8	9	14	7

4	21	18	3	8		22	5	18	9	6	9	26	9	5	18	21	14	7

Entschlüsselte Nachricht:

TIPP: JEDE ZAHL STEHT FÜR DIE POSITION DIESES BUCHSTABENS IM ALPHABET (Z. B. 1 = A, 2 = B, 26 = Z).

Kontrollpunkt 10: Grundlegende häufige Fragen zur Cybersicherheit (Teil A)

Sehen Sie sich häufige Fragen und Antworten zur Abwehr von Online-Bedrohungen an.

Q1: Was ist Online-Betrug?

Ein betrügerisches Vorgehen über digitale Kanäle, um Opfer dazu zu bringen, Geld zu überweisen oder persönliche Zugangsdaten preiszugeben.

Q2: Was ist das wichtigste Anzeichen für E-Mail-Phishing?

Eine Nachricht, die Dringlichkeit vortäuscht (etwa eine Kontosperrung) und Sie auf einen Link leitet, der nicht zur offiziellen Domain passt.

Q3: Was ist Typosquatting?

Registrierung von Domains mit häufigen Tippfehlern bekannter Marken (wie amaz0n.com), um gefälschte Phishing-Websites zu betreiben.

Q4: Was ist ein Support-Betrug?

Ein Pop-up, das behauptet, Ihr PC sei infiziert, und Sie auffordert, eine Nummer anzurufen und für gefälschte Bereinigungssoftware oder Fernzugriffsdienste zu bezahlen. [1]

Q5: Was ist Vishing?

Phishing-Angriffe per Telefonanruf, bei denen Opfer dazu verleitet werden, Bankkonto- oder Anmeldedaten preiszugeben.

Kontrollpunkt 10: Grundlegende häufige Fragen zur Cybersicherheit (Teil B)

Sehen Sie sich häufige Fragen und Antworten zur Abwehr von Online-Bedrohungen an.

Q6: Was bedeutet Überweisungsbetrug (Wire Fraud)?

Umleitung von Zahlungsvorgängen auf Konten von Betrügern, indem sich diese als Lieferanten oder Führungskräfte ausgeben.

Q7: Was ist Whaling?

Eine sehr gezielte Form des Spear-Phishing, die sich direkt gegen hochrangige Ziele wie Führungskräfte der C-Ebene richtet.

Q8: Was ist Smishing?

Betrügerische Textnachrichten an Mobilgeräte mit Links zu gefälschten Portalen oder angeblichen Sendungsverfolgungen.

Q9: Warum ist eine Überprüfung über einen separaten Kanal (Out-of-Band) entscheidend?

Sie bestätigt Transaktionsdetails über einen separaten Kommunikationskanal (etwa einen Anruf) und umgeht so kompromittierte E-Mail-Verläufe.

Q10: Wie funktioniert ein Betrug mit gefälschter Treuhand (Escrow)?

Betrüger erstellen eine gefälschte Treuhand-Website (Escrow), behaupten, das Geld werde sicher verwahrt, und stehlen dann die Überweisung des Käufers.

Kontrollpunkt 10: Fortgeschrittene häufige Fragen zur Sicherheit (Teil C)

Erkunden Sie fortgeschrittene technische Aspekte von Sicherheits-Frameworks, Malware-Analyse und Daten-Compliance.

Q1: Wie nutzen Betrüger BEC (Business Email Compromise) für Überweisungsbetrug?

Sie kapern das E-Mail-Konto eines echten Mitarbeiters, verfolgen Rechnungsverläufe und senden geänderte Zahlungsangaben mit betrügerischen Bankkonten.

Q2: Welches Risiko bergen IDN-Homographenangriffe bei Online-Betrug?

Verwendung von Nicht-ASCII-Zeichen, die normalen Buchstaben gleichen (z. B. das kyrillische 'a'), um gefälschte Domains zu registrieren, die echte Marken nachahmen.

Q3: Warum ist die Prüfung von E-Mail-Headern bei der Erkennung von Betrug wichtig?

Er zeigt die tatsächliche IP des Ursprungsservers und den Status der SPF-/DKIM-Prüfung und damit, ob die Absenderdomain gefälscht ist.

Q4: Wie nutzen Support-Betrüger Fernwartungssoftware aus?

Sie verbinden sich mit Programmen wie AnyDesk oder TeamViewer mit dem Gerät des Opfers, schleusen Schadsoftware ein und stehlen gespeicherte Passwörter.

Q5: Was ist das Ziel von Vorschussbetrug?

Opfer dazu bringen, vorab Bearbeitungsgebühren für eine hohe finanzielle Belohnung zu zahlen, die es nicht gibt.

Kontrollpunkt 10: Fortgeschrittene häufige Fragen zur Sicherheit (Teil D)

Erkunden Sie fortgeschrittene technische Aspekte von Sicherheits-Frameworks, Malware-Analyse und Daten-Compliance.

Q6: Wie nutzen Betrüger die Profilbildung in sozialen Medien für gezieltes Phishing?

Sie stellen Organisationsstrukturen von Unternehmen und Mitarbeiternamen zusammen, um überzeugende Spear-Phishing-E-Mails zu verfassen.

Q7: Warum bieten gefälschte Onlineshops hohe Rabatte an?

Um Käufer zur Eingabe ihrer Kreditkartendaten zu verleiten und diese zur Wiederverwendung oder zum Weiterverkauf in Carding-Foren abzugreifen.

Q8: Wie blockieren DMARC-Einträge Phishing-Betrug?

Mit DMARC können Domaininhaber Empfänger auffordern, E-Mails, die abgestimmte SPF- und DKIM-Prüfungen nicht bestehen, in Quarantäne zu verschieben oder abzulehnen, wodurch direktes Spoofing blockiert wird. [5]

Q9: Welche Bedrohung geht von Portalen zum Abgreifen von Zugangsdaten aus?

Gefälschte Landingpages, die genau wie Microsoft 365 oder Google Workspace aussehen und Anmeldedaten bei der Eingabe stehlen.

Q10: Wie melden und deaktivieren Sicherheitsteams betrügerische Domains?

Durch Einreichen von Betrugsbeweisen bei der Missbrauchs-E-Mail-Adresse des Registrars, beim Hosting-Anbieter und bei Google Safe Browsing.

Teil 11: 10 Fakten und Einblicke zur Cybersicherheit aus der Praxis

Lernen Sie reale Fakten zu Sicherheitsvorfällen, Abwehrmechanismen und Compliance-Standards kennen.

1. SICHERHEITS-EINBLICK

Phishing und Spoofing waren 2025 die beim IC3 des FBI am häufigsten gemeldete Deliktart, mit 191,561 Beschwerden. [2]

2. SICHERHEITS-EINBLICK

Business Email Compromise (BEC) verursachte 2025 Verluste von über $3 Milliarden, die dem IC3 des FBI gemeldet wurden. [2]

3. SICHERHEITS-EINBLICK

Typosquatting-Domains unterscheiden sich von echten Markennamen nur um ein oder zwei Zeichen, sodass man sie bei einem flüchtigen Blick übersehen kann.

4. SICHERHEITS-EINBLICK

Betrug mit vorgetäuschtem technischem Support verursachte 2025 Verluste von über $2.1 Milliarden, die dem IC3 des FBI gemeldet wurden. [2]

5. SICHERHEITS-EINBLICK

Homograph-Angriffe sehen in der Adressleiste des Browsers identisch aus, sofern der Browser nicht die Punycode-Darstellung anzeigt.

6. SICHERHEITS-EINBLICK

SMS-Betrug (Smishing) nutzt kurze, dringliche Nachrichten mit Links, die Opfern wenig Kontext bieten, um den Betrug zu erkennen.

7. SICHERHEITS-EINBLICK

Whaling-Angriffe zielen auf E-Mail-Konten von Führungskräften, weil diese über große Überweisungen verfügen.

8. SICHERHEITS-EINBLICK

Zahlungsänderungen durch einen Anruf unter einer bekannten, gespeicherten Telefonnummer zu bestätigen, ist ein wichtiger Schutz vor Überweisungsbetrug per BEC.

9. SICHERHEITS-EINBLICK

Gefälschte Treuhand-Websites (Escrow) sind ein häufiger Betrug auf Online-Marktplätzen: Sie sehen aus wie ein sicherer Zahlungsdienst, stehlen aber die Überweisung des Käufers.

10. SICHERHEITS-EINBLICK

Google Safe Browsing warnt Nutzer, bevor sie Websites öffnen, die Google als Phishing oder Malware markiert hat.

Technische Referenzen und Quellen

Der Lernleitfaden und die interaktiven Rätsel wurden aus globalen Standards von NIST und OWASP sowie aus Datenschutz-Compliance-Standards zusammengestellt.

WISSENSCHAFTLICHE UND FACHLICHE QUELLEN

[1] Federal Trade Commission. (n.d.). How To Spot, Avoid, and Report Tech Support Scams.

https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

[2] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[3] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).

https://www.rfc-editor.org/rfc/rfc7489.html

Lösungsschlüssel: Kontrollpunkt 1 – Auswahlaufgaben

1 Frage 1

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Was ist das wichtigste Anzeichen für einen Support-Betrug? → Ein Pop-up, das behauptet, Ihr System sei infiziert, und Sie auffordert, eine Telefonnummer anzurufen

2 Frage 2

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Welche Technik nutzt gefälschte Absenderdomains, um Bankdaten zu stehlen? → E-Mail-Phishing

3 Frage 3

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Was beschreibt Überweisungsbetrug? → Opfer mithilfe von Social Engineering dazu bringen, Geld auf gefälschte Firmenkonten zu überweisen

4 Frage 4

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Warum erstellen Betrüger gefälschte Online-Shops? → Um Kreditkartendaten und Zahlungsinformationen von Käufern zu stehlen

5 Frage 5

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Was bedeutet Vishing? → Telefonbetrug (Voice-Phishing) über Telefonnetze, um Zugangsdaten zu stehlen

Lösungsschlüssel: Kontrollpunkt 2 – Richtig oder Falsch

6 **Frage 6** — **Richtige Antwort: Falsch**

HINWEIS FÜR LEHRKRÄFTE

Falsch: Phishing zielt auch auf Führungskräfte ab; Whaling ist Phishing, das sich gegen die oberste Führungsebene richtet.

7 **Frage 7** — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Gefälschte Domains verwenden oft kleine Tippfehler (wie amaz0n.com), um vertrauenswürdige Marken nachzuahmen.

8 **Frage 8** — **Richtige Antwort: Falsch**

HINWEIS FÜR LEHRKRÄFTE

Falsch: Wer einem Support-Betrüger Fernzugriff gewährt, ermöglicht ihm, Schadsoftware einzuschleusen und Daten zu stehlen.

9 **Frage 9** — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Social Engineering nutzt menschliche Psychologie wie Angst und Zeitdruck aus, um Sicherheitsregeln zu umgehen.

10 **Frage 10** — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Überweisungsanfragen sollten immer über einen separaten, unabhängigen Kommunikationsweg (Out-of-Band) überprüft werden.

Vokabelschlüssel und Bewertungsraster

Bewertungsraster für Lehrkräfte: Vergeben Sie 1 Punkt für jede richtige Zuordnung (insgesamt 8 Punkte) und jeden Kontextbegriff (insgesamt 6 Punkte).

KONTROLLPUNKT 4: LÖSUNG BEGRIFFSZUORDNUNG

G 1. PHISHING	F 2. GEFÄLSCHT	D 3. VISHING	B 4. BETRUG
H 5. ÜBERPRÜFUNG	A 6. KABEL	E 7. WHALING	C 8. SMISHING

KONTROLLPUNKT 3: LÖSUNG SCHLÜSSELBEGRIFFE

1 PHISHING	2 GEFÄLSCHT	3 VISHING	4 BETRUG
5 VERIFIZIERUNG	6 ÜBERWEISUNG		

KONTROLLPUNKT 6, ALTERNATIVE: LÖSUNG WORTZUORDNUNG

1 B – GEFAELSCHT	2 E – VERIFIZIERUNG	3 F – UEBERWEISUNG	4 H – SMISHING
5 G – WHALING	6 C – VISHING	7 A – PHISHING	8 D – BETRUG

DISKUSSIONSHINWEISE FÜR LEHRKRÄFTE

Schlüsselbegriffe:
Prüfen Sie, ob die Lernenden PHISHING, GEFÄLSCHT und VISHING in eigenen Worten erklären und jeweils ein Beispiel nennen können.

Fallstudien:
Bitten Sie die Lernenden, ihre Empfehlungen mit Fakten aus dem Arbeitsblatt statt mit Vermutungen zu begründen.

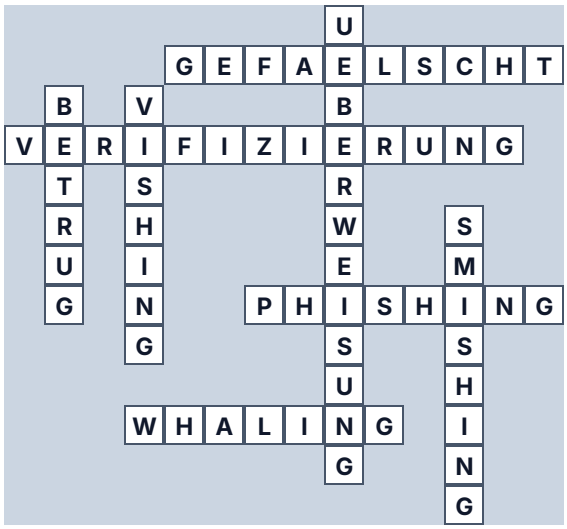
Quellenbewertung:
Lassen Sie die Lernenden mindestens eine Aussage anhand der Quellen des Arbeitsblatts prüfen und besprechen Sie, warum sich Zahlen, Preise und Regeln mit der Zeit ändern können.

Rätsellösungen und Hinweise für Lehrkräfte

LÖSUNG DES SUCHSELS

G	I	R	Z	S	F	Q	G	V	F	A	A	Q	O	N
N	G	P	T	X	Q	K	E	R	U	P	S	D	N	Y
U	N	G	B	F	S	X	F	W	J	H	A	R	Z	Y
S	I	U	Y	W	L	G	A	I	M	I	R	J	M	L
I	H	R	T	H	O	H	E	Q	Q	S	H	Z	A	O
E	S	T	V	A	G	U	L	B	Y	H	R	Y	B	H
W	I	E	L	L	Z	G	S	J	O	I	P	N	W	C
R	M	B	M	I	Z	Y	C	G	Y	N	O	W	U	K
E	S	V	P	N	B	N	H	V	T	G	M	G	V	D
B	Y	U	K	G	R	B	T	X	Z	Y	M	R	Q	X
E	V	E	R	I	F	I	Z	I	E	R	U	N	G	I
U	P	D	A	D	J	Q	V	W	W	L	J	H	T	H
G	B	V	I	S	H	I	N	G	E	I	K	T	S	V
R	Z	E	H	E	S	C	A	L	Q	C	Z	M	K	V
R	U	A	S	W	J	M	M	H	H	N	H	R	F	K

KREUZWORTRÄTSEL-LÖSUNG



LEITFADEN FÜR LEHRKRÄFTE ZU DEN KREUZWORTRÄTSEL-LÖSUNGEN

WAAGERECHT

2 waagerecht: GEFAELSCHT So ist eine nachgeahmte Absender- oder Website-Adresse, die seriös wirken soll. (10 Buchstaben)

5 waagerecht: VERIFIZIERUNG Bestätigung von Zahlungsdetails über einen vertrauenswürdigen zweiten Kontaktweg. (13 Buchstaben)

7 waagerecht: PHISHING Betrügerische E-Mail-Kampagnen, mit denen Anmeldedaten und Passwörter gestohlen werden sollen. (8 Buchstaben)

8 waagerecht: WHALING Gezielte Phishing-Angriffe, die Zugangsdaten von Führungskräften der C-Ebene stehlen sollen. (7 Buchstaben)

SENKRECHT

1 senkrecht: UEBERWEISUNG Bei diesem Betrug werden Banktransaktionen auf Konten von Kriminellen umgeleitet. (12 Buchstaben)

3 senkrecht: BETRUG Masche, mit der Opfern Geld oder Zugangsdaten gestohlen werden sollen. (6 Buchstaben)

4 senkrecht: VISHING Betrügerische Sprachanrufe, mit denen Zugangsdaten und Kontodetails gestohlen werden sollen. (7 Buchstaben)

6 senkrecht: SMISHING Versand betrügerischer SMS, um Zugangsdaten für Mobilfunkkonten zu stehlen. (8 Buchstaben)

Lösungsschlüssel für Buchstabensalat und Chiffre

Lösungsschlüssel für die Wort-Entwirr-Aufgabe und die Geheime Chiffre-Aufgabe.

LÖSUNGSSCHLÜSSEL BUCHSTABENSALAT

1. NSHPIHGI — **PHISHING**
2. VSGNIHI — **VISHING**
3. EVIRENGRZFIUI — **VERIFIZIERUNG**
4. GHILNWA — **WHALING**
5. CLTEASEGHF — **GEFAELSCHT**
6. URBTGE — **BETRUG**
7. ISRUEEGUNBWE — **UEBERWEISUNG**
8. SMHGSNII — **SMISHING**

LÖSUNGSSCHLÜSSEL ZUR GEHEIMEN CHIFFRE-AUFGABE

"ERKENNEN SIE PHISHING DURCH VERIFIZIERUNG"

Lösungsschlüssel zu den Fallstudien

A Fallstudie 1: Verhinderung von Betrug mit Firmenüberweisungen

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Die Finanzabteilung erhält eine dringende E-Mail von einer gefälschten Lieferantenadresse mit der Bitte, künftige Rechnungszahlungen an eine neue Bankverbindung zu überweisen.
- Empfohlene Strategie und Lösung: Führen Sie für alle Zahlungen eine Richtlinie mit doppelter Autorisierung ein. Setzen Sie eine Out-of-Band-Verifizierung über eine vorab gespeicherte Telefonnummer um und blockieren Sie E-Mails von gefälschten Domains am Gateway.

B Fallstudie 2: Whaling-Phishing-Vorfall auf Führungsebene

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Eine Führungskraft hat auf einen Phishing-Link geklickt, der angeblich ein sicheres Dokument für eine Vorstandssitzung enthielt, und ihre wichtigsten Firmen-Zugangsdaten auf einem gefälschten Portal eingegeben.
- Empfohlene Strategie und Lösung: Isolieren Sie das Gerät der Führungskraft. Setzen Sie alle Sitzungstoken und Zugangsdaten des Unternehmens zurück. Prüfen Sie die Zugriffsprotokolle auf Datenabflüsse und führen Sie für alle Anmeldungen Hardware-MFA ein.