Name: _____ Datum: _____ Punkte: _____

# Sicherheit und Verschlüsselung im öffentlichen WLAN

Man-in-the-Middle-Angriffe, gefälschte Zugangspunkte, Packet Sniffing, VPN-Tunnel und HTTPS-Verschlüsselung.

## LERNÜBERSICHT SICHERHEIT IM ÖFFENTLICHEN WLAN

**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 Sicherheit öffentlicher WLANs. Sie lernen unverschlüsselte Netzwerke, Man-in-the-Middle-Angriffe (MitM), Rogue Access Points, Packet Sniffing, VPN-Tunnel und die Sicherheit der Übertragung per HTTPS 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/sicherheit-oeffentliches-wlan/

# Ihr Lernfahrplan: Sicherheit in öffentlichen WLANs

- Gängige Risiken öffentlicher WLANs erkennen, darunter Packet Sniffing und gefälschte Zugangspunkte.
- VPN-Verschlüsselungstunnel einrichten, um Daten bei der Übertragung zu sichern.
- Erzwingen Sie HTTPS und sichere Browsereinstellungen für Mitarbeitende im Homeoffice.

## ANLEITUNG ZUM LEITFADEN SICHERHEIT IM ÖFFENTLICHEN WLAN

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: Sicherheit beim Fernzugriff. Zum Schluss folgt die Bonusaufgabe Schnell denken.

## SICHERHEIT IM ÖFFENTLICHEN WLAN UND SCHUTZ BEI DER ÜBERTRAGUNG (EINFÜHRUNG)

Unverschlüsselte öffentliche WLAN-Hotspots setzen den Netzwerkverkehr dem Mitschneiden von Paketen und Evil-Twin-Täuschungen aus. Wer den Datenverkehr durch sichere, verschlüsselte VPN-Tunnel zwingt und reine HTTPS-Regeln per HSTS durchsetzt, schützt Sitzungen vor dem Abfangen im lokalen Netzwerk.

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

## Kontrollpunkt 1: Auswahlaufgaben

**1. Was ist ein Man-in-the-Middle-Angriff (MitM)?**

- A. Abfangen und Verändern der Kommunikation zwischen zwei Parteien in einem gemeinsam genutzten Netzwerk
- B. Eine Technik zum Auslesen von Datenbanken, die auf Benutzerdatensätze abzielt
- C. Überlasten von Webservern mit Netzwerkanfragen
- D. Löschen lokaler Festplattenvolumes

**2. Was ist ein Rogue Access Point (Evil Twin)?**

- A. Ein bösartiger WLAN-Hotspot mit derselben SSID wie ein legitimes Netzwerk
- B. Ein Verwaltungswerkzeug zur Überwachung von Datenbanksicherungen
- C. Eine sichere VPN-Gateway-Konfiguration
- D. Ein DNS-Eintrag, der autorisierte Mailserver festlegt

**3. Wie schützt ein VPN den Datenverkehr in öffentlichen WLANs?**

- A. Es verpackt alle Netzwerkpakete in einen verschlüsselten Tunnel, sodass Sniffer sie nicht lesen können
- B. Es blockiert automatisch alle eingehenden Verbindungsanfragen
- C. Es ändert die MAC-Adresse der physischen Netzwerkkarte
- D. Es löscht zwischengespeicherte Cookies im Webbrowser

**4. Was ist Packet Sniffing?**

- A. Einsatz von Hardware- oder Softwarewerkzeugen zum Erfassen und Protokollieren von Netzwerkpaketen
- B. Durchsuchen lokaler Verzeichnisse nach doppelten Dateien
- C. Beschränkung von Datenbank-Leserechten anhand von Benutzerrollen
- D. Verschlüsseln von Speicherlaufwerken mit AES-256-Schlüsseln

**5. Welche Rolle spielt HTTPS?**

- A. Verschlüsseln des Sitzungsverkehrs zwischen Browser und Webserver
- B. Filtern eingehender E-Mails am Gateway
- C. Komprimieren von Bildern für schnellere Seitenladezeiten
- D. Verwaltung von Dateistrukturen in Netzwerkspeichern (NAS)

## Kontrollpunkt 2: Richtig oder falsch

### 6 Frage 6

6. Verbundene Nutzer können in offenen öffentlichen WLANs leicht Klartextdaten abfangen.

○ Richtig ○ Falsch

### 7 Frage 7

7. Nicht autorisierte Zugangspunkte (Evil Twins) sind immer von den Netzwerkadministratoren genehmigt.

○ Richtig ○ Falsch

### 8 Frage 8

8. Ein VPN ist unwirksam, wenn es darum geht, Datenverkehr in öffentlichen Netzwerken vor Packet Sniffing zu schützen.

○ Richtig ○ Falsch

### 9 Frage 9

9. HTTPS verschlüsselt nur den URL-Pfad und lässt die Paketnutzdaten im Klartext.

○ Richtig ○ Falsch

### 10 Frage 10

10. WLAN-Hotspots mit WPA3-Sicherheit bieten stärkeren Schutz als offene Netzwerke ohne Passwort.

○ 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. Das Mitlesen privater Passwörter in öffentlichen WLANs ist ein _____ der Kommunikation.**

**2. Die Analyse roher Pakete in einem lokalen Netzwerk nutzt _____ von Paketen.**

**3. Ein gefälschter Hotspot, der das WLAN eines Hotels imitiert, ist ein _____ .**

**4. Um Webverkehr bei der Übertragung abzusichern, muss er mit _____ verschlüsselt werden.**

**5. Um alle Netzwerkausgaben zu verschlüsseln, nutzt man einen _____ .**

**6. Ein verschlüsselter Kommunikationsweg durch öffentliche Netzwerke ist ein _____ .**

**WORTSCHATZ-WORTBANK**

ABFANGEN EVIL TWIN FIREWALL HTTPS SNIFFING TUNNEL VPN-CLIENT WPA-STANDARD

**Schreiben Sie Ihre Antworten hier:**

**1.** | **2.**

**3.** | **4.**

**5.** | **6.**

# Kontrollpunkt 4: Zuordnung von Sicherheits-Begriffen

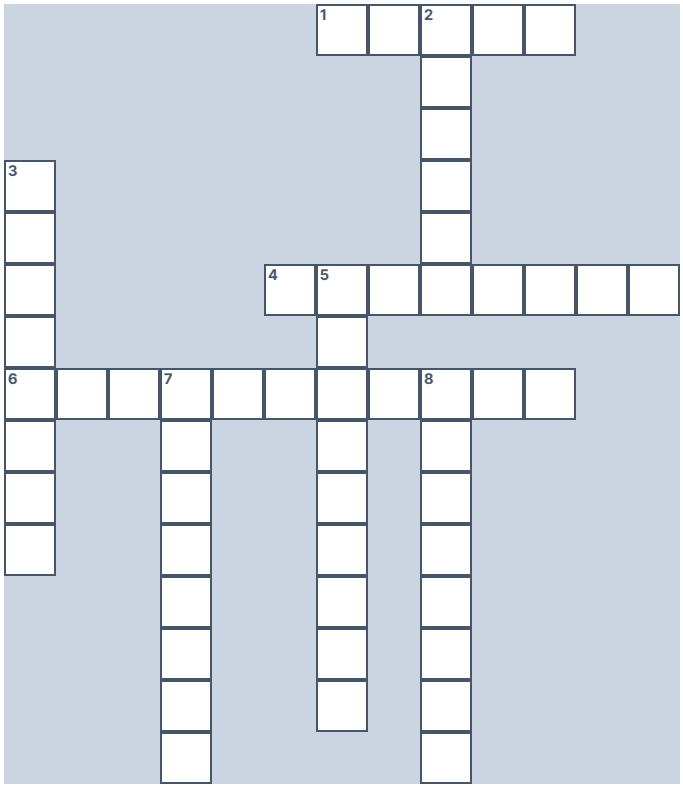
**DEFINITIONEN ZUORDNEN**

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

| | | | |
|---|---|---|---|
| ☐ | 1. ABFANGEN | A | Moderner WLAN-Sicherheitsstandard. |
| ☐ | 2. SNIFFING | B | Gesicherter Datenpfad während der Übertragung. |
| ☐ | 3. EVIL TWIN | C | Filtern eingehenden Datenverkehrs. |
| ☐ | 4. HTTPS | D | Gefälschter Hotspot, der ein WLAN imitiert. |
| ☐ | 5. VPN | E | Mitlesen von Traffic während der Übertragung. |
| ☐ | 6. TUNNEL | F | Mitschneiden von Netzwerkdatenpaketen. |
| ☐ | 7. WPA3 | G | Verschlüsseltes virtuelles privates Netzwerk. |
| ☐ | 8. FIREWALL | H | Sichere Webübertragung. |

## Kontrollpunkt 5: Kreuzworträtsel

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




### WAAGERECHT

**1. Sichere Übertragung im Web. (5)**

**4. Gefälschter Hotspot, der ein WLAN imitiert. (8)**

**6. Moderner WLAN-Sicherheitsstandard (WPA3). (11)**

### SENKRECHT

**2. Sicherer Datenweg während der Übertragung. (6)**

**3. Filtern eingehenden Datenverkehrs. (8)**

**5. Software für ein verschlüsseltes virtuelles privates Netzwerk. (9)**

**7. Mitschneiden von Netzwerkdatenpaketen. (8)**

**8. Mitlesen von Datenverkehr während der Übertragung. (8)**

# Kontrollpunkt 5, Alternative: Barrierefreie Kreuzworträtsel-Hinweise

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

## WAAGERECHT

**1 waagerecht: Sichere Übertragung im Web. (5 Buchstaben):**

**4 waagerecht: Gefälschter Hotspot, der ein WLAN imitiert. (8 Buchstaben):**

**6 waagerecht: Moderner WLAN-Sicherheitsstandard (WPA3). (11 Buchstaben):**

## SENKRECHT

**2 senkrecht: Sicherer Datenweg während der Übertragung. (6 Buchstaben):**

**3 senkrecht: Filtern eingehenden Datenverkehrs. (8 Buchstaben):**

**5 senkrecht: Software für ein verschlüsseltes virtuelles privates Netzwerk. (9 Buchstaben):**

**7 senkrecht: Mitschneiden von Netzwerkdatenpaketen. (8 Buchstaben):**

**8 senkrecht: Mitlesen von Datenverkehr während der Übertragung. (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.

C R L I G N R E M P X Q O C U

S T E E L J B V A B F C P X L

K Y N K X T K I D Q I M J D I

T N N N K Q P L G M R M Q R S

N T U T G W C T S Q E O H A S

E B T W D P S W Z V W C Z B W

I F K H Z A D I S N A D Q F X

L P C U B S A N N Z L N D A K

C A D O D T F H I I L D R N Q

N M E I R A H Z F S F Q V G F

P A A Q O N T N F P T X Q E K

V R U S D D T N I Y B F S N X

W J A R Z A P Y N Y L G I M R

J M L T O R S H G Q Q H Z A O

V G U B Y D R Y B H L Z G J O

**WORTSCHATZ-WORTLISTE**

ABFANGEN SNIFFING EVILTWIN HTTPS VPNCLIENT TUNNEL WPASTANDARD FIREWALL

# 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. ABFANGEN**
- **B. SNIFFING**
- **C. EVILTWIN**
- **D. HTTPS**
- **E. VPNCLIENT**
- **F. TUNNEL**
- **G. WPASTANDARD**
- **H. FIREWALL**

**DEFINITIONEN UND ZUORDNUNGSFELDER**

1. Moderner WLAN-Sicherheitsstandard (WPA3).
2. Gefälschter Hotspot, der ein WLAN imitiert.
3. Mitschneiden von Netzwerkdatenpaketen.
4. Sicherer Datenweg während der Übertragung.
5. Filtern eingehenden Datenverkehrs.
6. Mitlesen von Datenverkehr während der Übertragung.
7. Software für ein verschlüsseltes virtuelles privates Netzwerk.
8. Sichere Übertragung im Web.

## 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. E A N A G B N F
2. L E N V I W T I
3. V I L P E T C N N
4. N R D A A T A D W P S
5. F I N G F S N I
6. P H T S T
7. E T N L N U
8. E I W L F L A R

# Bonusaufgabe: Schnell denken

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

| | | | | |
|---|---|---|---|---|
| 1 | Gründe, Software zu aktualisieren | | | |
| 2 | Geräte, die sich automatisch mit WLANs verbinden | | | |
| 3 | Informationen, die Sie niemals weitergeben sollten | | | |
| 4 | Sichere Gewohnheiten, mit denen Sie heute beginnen können | | | |
| 5 | Möglichkeiten, in einem Café sicher zu bleiben | | | |
| 6 | Geräte, die gehackt werden können | | | |
| 7 | Dinge, die ein Hacker in einem offenen WLAN sehen kann | | | |
| 8 | Anzeichen für ein gefälschtes WLAN | | | |
| 9 | Alternativen zu öffentlichem WLAN | | | |
| 10 | Warnzeichen in einer E-Mail | | | |
| 11 | Dinge, die Sie in öffentlichen WLANs nicht tun | | | |
| 12 | Orte mit kostenlosem WLAN | | | |
| 13 | Möglichkeiten, Ihre Konten zu schützen | | | |
| 14 | Anzeichen, dass ein Computer infiziert ist | | | |
| 15 | WLAN-Namen, die verdächtig wirken | | | |

# Kontrollpunkt 8: Fallstudien zur Cybersicherheit

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

## FALLSTUDIE 1: EINDÄMMUNG VON PACKET SNIFFING IN ÖFFENTLICHEM WLAN



**Szenario:** Ein Vertriebsleiter im Außendienst, der mit einem öffentlichen WLAN am Flughafen verbunden ist, bemerkt, dass mehrere sensible geschäftliche E-Mails kurz nach dem Versand im Klartext geleakt wurden.

**Diskussionsfrage:** Analysieren Sie die Risiken öffentlicher Netzwerke und skizzieren Sie eine Lösung zur Verschlüsselung des Datenverkehrs.

## FALLSTUDIE 2: ABWEHR VON EVIL-TWIN-HOTSPOTS



**Szenario:** Angreifer richten einen gefälschten WLAN-Zugangspunkt namens „CoffeeShop_Guest“ ein, der einen echten Café-Hotspot nachahmt, und schneiden den Netzwerkverkehr ahnungsloser Gäste mit.

**Diskussionsfrage:** Beschreiben Sie die Prüfschritte, mit denen sich gefälschte Zugangspunkte erkennen und blockieren 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

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 22 | 5 | 18 | 19 | 3 | 8 | 12 | 21 | 5 | 19 | 19 | 5 | 12 | 14 | 19 | 9 | 5 |
| | | | | | | | | | | | | | | | | |
| 15 | 5 | 6 | 6 | 5 | 14 | 20 | 12 | 9 | 3 | 8 | 5 | 19 | 23 | 12 | 1 | 14 |
| | | | | | | | | | | | | | | | | |
| 13 | 9 | 20 | 22 | 16 | 14 | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |

**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: Warum ist öffentliches WLAN unsicher?

Offenes öffentliches WLAN verschlüsselt den Datenverkehr über die Funkverbindung nicht, sodass andere in der Nähe ungeschützte Daten abfangen können. [2]

### Q2: Was ist Paket-Sniffing?

Ein Packet Sniffer erfasst die Rohdaten, die über eine Netzwerkschnittstelle fließen, und legt Klartextpasswörter und Details des Datenverkehrs offen.

### Q3: Was ist ein Evil Twin?

Ein von Hackern eingerichteter gefälschter Zugangspunkt, der Namen und Einstellungen eines vertrauenswürdigen lokalen WLAN-Hotspots nachahmt.

### Q4: Wie schützt mich ein VPN?

Es leitet Ihren Datenverkehr durch einen verschlüsselten Tunnel und verbirgt Ihre Browseraktivität vor Sniffern im lokalen Netzwerk.

### Q5: Schützt mich HTTPS in öffentlichen WLANs?

Ja, es verschlüsselt die zwischen Ihrem Browser und der Website ausgetauschten Daten, und ein VPN fügt eine weitere Schutzebene hinzu.

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

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

### Q6: Was ist WPA3?

Der moderne Wi-Fi-Protected-Access-Standard mit stärkerer Verschlüsselung und Schutz vor Offline-Wörterbuchangriffen. [1]

### Q7: Kann öffentliches WLAN Schadsoftware übertragen?

Ja, Angreifer können den Datenverkehr abfangen und bösartige Download-Aufforderungen (Drive-by-Downloads) in Ihre Browsersitzung einschleusen.

### Q8: Welches Risiko birgt Filesharing?

Ist die Dateifreigabe aktiviert, können andere Nutzer im öffentlichen Netzwerk Ihren lokalen Ordner lesen oder verändern.

### Q9: Was ist ein Captive Portal?

Die Anmeldeseite, über die Hotel- oder Café-Netzwerke den Internetzugang freigeben und die Angreifer manchmal fälschen können.

### Q10: Sollte ich WLAN ausschalten, wenn ich es nicht nutze?

Ja, das Deaktivieren von WLAN verhindert, dass sich Ihr Gerät automatisch mit nicht vertrauenswürdigen Netzwerken verbindet.

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

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

### Q1: Wie nutzt ein Man-in-the-Middle-Angriff DNS aus?

Durch DNS-Spoofing auf einem bösartigen Router, um Zielbrowser auf ähnlich aussehende Phishing-Landingpages statt auf die Zieldomains zu leiten.

### Q2: Was ist Session-Hijacking?

Ein Angreifer schneidet in einem öffentlichen WLAN ein unverschlüsseltes Sitzungscookie mit und importiert es, um die Anmeldung mit Zugangsdaten zu umgehen.

### Q3: Was ist SSL-Stripping?

Ein MitM-Angriff, bei dem ein Angreifer die sichere HTTPS-Anfrage eines Nutzers auf unverschlüsseltes HTTP herabstuft und Anmeldedaten im Klartext abfängt.

### Q4: Wie schützt HSTS vor SSL-Stripping?

HTTP Strict Transport Security zwingt Browser, sich nur über HTTPS zu verbinden, und verweigert den Rückfall auf unverschlüsseltes HTTP. [3]

### Q5: Was ist ein Split-Tunnel-VPN?

Eine Konfiguration, die nur den Unternehmensverkehr über das VPN leitet und öffentliche Internetdaten direkt sendet, was das Risiko offener Leckpfade bergen kann.

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

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

### Q6: Warum ist WPA2 für KRACK anfällig?

Der Key Reinstallation Attack (KRACK) nutzt den Vier-Wege-Handshake von WPA2 aus, um Pakete ohne das WLAN-Passwort zu entschlüsseln.

### Q7: Was ist Client-Isolation?

Eine Router-Sicherheitseinstellung, die verhindert, dass verbundene WLAN-Geräte direkt miteinander kommunizieren, und so lokales Mitschneiden blockiert.

### Q8: Wie nutzen Angreifer gefälschte DNS-Server?

Sie konfigurieren betrügerische Router so, dass diese den Clients gefälschte DNS-Server zuweisen, wodurch sie alle Web-Abfragen abfangen und umschreiben können.

### Q9: Kann ein VPN meine lokale MAC-Adresse verbergen?

Nein. MAC-Adressen sind lokale Kennungen auf Schicht 2; nutzen Sie stattdessen die integrierte MAC-Randomisierung (private Adresse) Ihres Geräts.

### Q10: Was ist ein Angriff mit gefälschtem Captive Portal?

Ein Angreifer betreibt auf einem gefälschten Hotspot ein falsches Anmeldeportal, um unter dem Vorwand von kostenlosem WLAN Zugangsdaten zu stehlen.

# 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**

Remote-Mitarbeitende nutzen oft WLAN in Cafés, Hotels und Flughäfen, wo sie keinen Einfluss auf die Sicherheit des Netzwerks haben.

**2. SICHERHEITS-EINBLICK**

Ein gefälschter Evil-Twin-Hotspot kann den exakten Namen und die MAC-Adresse eines vertrauenswürdigen Netzwerks kopieren und so Geräte täuschen.

**3. SICHERHEITS-EINBLICK**

Paket-Sniffing-Software wie Wireshark ist kostenlos und kann unverschlüsselte HTTP-Passwörter im Klartext anzeigen.

**4. SICHERHEITS-EINBLICK**

WPA3-Sicherheit nutzt Simultaneous Authentication of Equals (SAE), um vor lokalen Brute-Force-Angriffen zu schützen.

**5. SICHERHEITS-EINBLICK**

SSL-Stripping-Angriffe umgehen einfache HTTPS-Schutzmaßnahmen, indem sie die ersten HTTP-Weiterleitungen am Gateway abfangen.

**6. SICHERHEITS-EINBLICK**

Antwort-Header für HTTP Strict Transport Security (HSTS) verhindern, dass Browser auf unverschlüsselte HTTP-Verbindungen zurückfallen. [3]

**7. SICHERHEITS-EINBLICK**

Das Ausschalten von „Automatisch verbinden“ verhindert, dass sich Smartphones an öffentlichen Orten mit nachgeahmten betrügerischen Netzwerken verbinden.

**8. SICHERHEITS-EINBLICK**

'Always-on'-VPN-Konfigurationen in Unternehmen leiten den gesamten Netzwerkverkehr von Mitarbeitenden im Homeoffice zwingend über die Firewalls des Unternehmens.

**9. SICHERHEITS-EINBLICK**

Nicht autorisierte Zugangspunkte können gefälschte DNS-Antworten ausgeben und Zieldomains auf Phishing-Server umleiten.

**10. SICHERHEITS-EINBLICK**

Ohne VPN können andere Nutzer in einem offenen Hotspot sehen, welche Websites und Server Ihr Gerät kontaktiert.

# 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] Wi-Fi Alliance. (n.d.). Security.

https://www.wi-fi.org/discover-wi-fi/security

[2] Federal Trade Commission. (2023). Are Public Wi-Fi Networks Safe? What You Need To Know.

https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[3] MDN Web Docs. (n.d.). Strict-Transport-Security header.

https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Strict-Transport-Security

[4] 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

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

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

## Lösungsschlüssel: Kontrollpunkt 1 – Auswahlaufgaben

### 1 Frage 1

**Richtige Antwort: A**

#### HINWEIS FÜR LEHRKRÄFTE

Was ist ein Man-in-the-Middle-Angriff (MitM)? → Abfangen und Verändern der Kommunikation zwischen zwei Parteien in einem gemeinsam genutzten Netzwerk

### 2 Frage 2

**Richtige Antwort: A**

#### HINWEIS FÜR LEHRKRÄFTE

Was ist ein Rogue Access Point (Evil Twin)? → Ein bösartiger WLAN-Hotspot mit derselben SSID wie ein legitimes Netzwerk

### 3 Frage 3

**Richtige Antwort: A**

#### HINWEIS FÜR LEHRKRÄFTE

Wie schützt ein VPN den Datenverkehr in öffentlichen WLANs? → Es verpackt alle Netzwerkpakete in einen verschlüsselten Tunnel, sodass Sniffer sie nicht lesen können

### 4 Frage 4

**Richtige Antwort: A**

#### HINWEIS FÜR LEHRKRÄFTE

Was ist Packet Sniffing? → Einsatz von Hardware- oder Softwarewerkzeugen zum Erfassen und Protokollieren von Netzwerkpaketen

### 5 Frage 5

**Richtige Antwort: A**

#### HINWEIS FÜR LEHRKRÄFTE

Welche Rolle spielt HTTPS? → Verschlüsseln des Sitzungsverkehrs zwischen Browser und Webserver

## Lösungsschlüssel: Kontrollpunkt 2 – Richtig oder Falsch

**6** **Frage 6** — **Richtige Antwort: Richtig**

### HINWEIS FÜR LEHRKRÄFTE

Verbundene Nutzer können in offenen öffentlichen WLANs leicht Klartextdaten abfangen.

**7** **Frage 7** — **Richtige Antwort: Falsch**

### HINWEIS FÜR LEHRKRÄFTE

Falsch: Ein Evil Twin ist ein nicht autorisierter Hotspot, den ein Angreifer einrichtet, um einen echten nachzuahmen.

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

### HINWEIS FÜR LEHRKRÄFTE

Falsch: Ein VPN verschlüsselt den Datenverkehr in einem Tunnel, sodass lokale Sniffer ihn nicht lesen können.

**9** **Frage 9** — **Richtige Antwort: Falsch**

### HINWEIS FÜR LEHRKRÄFTE

Falsch: HTTPS verschlüsselt den gesamten HTTP-Austausch, einschließlich URL-Pfad und Seiteninhalt.

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

### HINWEIS FÜR LEHRKRÄFTE

WLAN-Hotspots mit WPA3-Sicherheit bieten stärkeren Schutz als offene Netzwerke ohne Passwort.

# 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

| | | | |
|---|---|---|---|
| E 1. ABFANGEN | F 2. SNIFFING | D 3. EVIL TWIN | H 4. HTTPS |
| G 5. VPN | B 6. TUNNEL | A 7. WPA3 | C 8. FIREWALL |

## KONTROLLPUNKT 3: LÖSUNG SCHLÜSSELBEGRIFFE

| | | | |
|---|---|---|---|
| 1 ABFANGEN | 2 SNIFFING | 3 EVIL TWIN | 4 HTTPS |
| 5 VPN-CLIENT | 6 TUNNEL | | |

## KONTROLLPUNKT 6, ALTERNATIVE: LÖSUNG WORTZUORDNUNG

| | | | |
|---|---|---|---|
| 1 G – WPASTANDARD | 2 C – EVILTWIN | 3 B – SNIFFING | 4 F – TUNNEL |
| 5 H – FIREWALL | 6 A – ABFANGEN | 7 E – VPNCLIENT | 8 D – HTTPS |

## DISKUSSIONSHINWEISE FÜR LEHRKRÄFTE

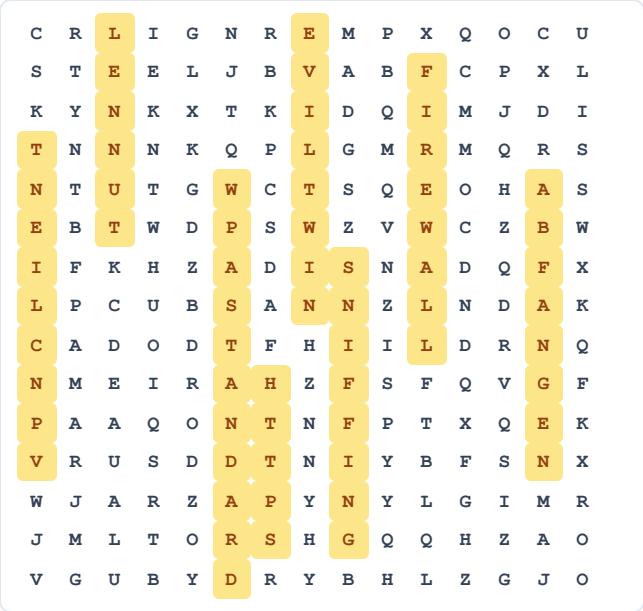
**Schlüsselbegriffe:**
Prüfen Sie, ob die Lernenden ABFANGEN, SNIFFING und EVIL TWIN in eigenen Worten erklären und jeweils ein Beispiel nennen können.

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

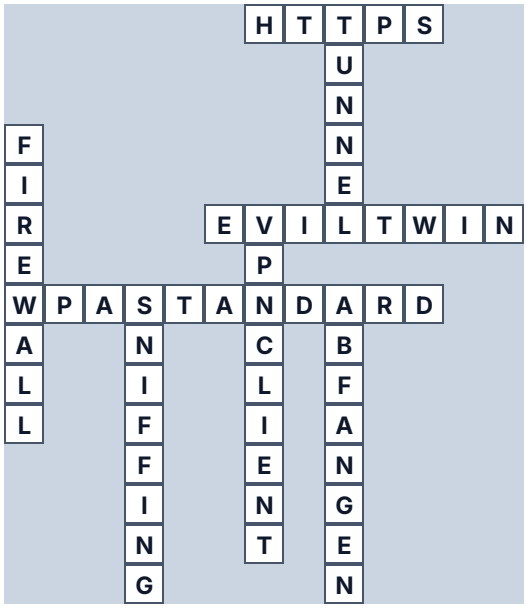
**Quellenbewertung:**
Lassen Sie die Lernenden mindestens eine Aussage anhand der Quellen des Arbeitsblatts prüfen und besprechen Sie, warum sich Zahlen, Preise und Regeln mit der Zeit ändern können.

# Rätsellösungen und Hinweise für Lehrkräfte

## LÖSUNG DES SUCHSELS




## KREUZWORTRÄTSEL-LÖSUNG




## LEITFADEN FÜR LEHRKRÄFTE ZU DEN KREUZWORTRÄTSEL-LÖSUNGEN

### WAAGERECHT

**1 waagerecht: HTTPS** Sichere Übertragung im Web. (5 Buchstaben)

**4 waagerecht: EVILTWIN** Gefälschter Hotspot, der ein WLAN imitiert. (8 Buchstaben)

**6 waagerecht: WPASTANDARD** Moderner WLAN-Sicherheitsstandard (WPA3). (11 Buchstaben)

### SENKRECHT

**2 senkrecht: TUNNEL** Sicherer Datenweg während der Übertragung. (6 Buchstaben)

**3 senkrecht: FIREWALL** Filtern eingehenden Datenverkehrs. (8 Buchstaben)

**5 senkrecht: VPNCLIENT** Software für ein verschlüsseltes virtuelles privates Netzwerk. (9 Buchstaben)

**7 senkrecht: SNIFFING** Mitschneiden von Netzwerkdatenpaketen. (8 Buchstaben)

**8 senkrecht: ABFANGEN** Mitlesen von Datenverkehr während der Übertragung. (8 Buchstaben)

# Lösungsschlüssel für Buchstabensalat und Chiffre

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

## LÖSUNGSSCHLÜSSEL BUCHSTABENSALAT

1. E A N A G B N F — **ABFANGEN**
2. L E N V I W T I — **EVILTWIN**
3. V I L P E T C N N — **VPNCLIENT**
4. N R D A A T A D W P S — **WPASTANDARD**
5. F I N G F S N I — **SNIFFING**
6. P H T S T — **HTTPS**
7. E T N L N U — **TUNNEL**
8. E I W L F L A R — **FIREWALL**

## LÖSUNGSSCHLÜSSEL ZUR GEHEIMEN CHIFFRE-AUFGABE

**"VERSCHLUESSELN SIE OEFFENTLICHES WLAN MIT VPN"**

# Lösungsschlüssel zu den Fallstudien

## A Fallstudie 1: Eindämmung von Packet Sniffing in öffentlichem WLAN

Lösung für Lehrkräfte

### BEWERTUNGSRICHTLINIE

**Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:**

- Szenarioanalyse: Ein Außendienstmitarbeiter, der mit einem öffentlichen WLAN am Flughafen verbunden ist, bemerkt, dass mehrere vertrauliche geschäftliche E-Mails kurz nach dem Versand im Klartext abgeflossen sind.
- Empfohlene Strategie und Lösung: Schreiben Sie auf allen Remote-Arbeitsplätzen die Nutzung eines Unternehmens-VPN-Clients vor. Setzen Sie Browsererweiterungen durch, die nur HTTPS zulassen, und blockieren Sie unverschlüsselte Protokolle (wie HTTP und FTP) an der Client-Firewall.

## B Fallstudie 2: Abwehr von Evil-Twin-Hotspots

Lösung für Lehrkräfte

### BEWERTUNGSRICHTLINIE

**Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:**

- Szenarioanalyse: Angreifer richten einen gefälschten WLAN-Zugangspunkt namens 'CoffeeShop_Guest' ein, der einen echten Café-Hotspot nachahmt, und fangen den Netzwerkverkehr ahnungsloser Gäste ab.
- Empfohlene Strategie und Lösung: Prüfen Sie die BSSID-MAC-Adressen der Access Points, um die Echtheit des Netzwerks zu überprüfen. Setzen Sie eine Posture-Validierung der Clients durch, um Verbindungen zu offenen Netzwerken zu blockieren, und schreiben Sie für vertrauliche Arbeit Mobilfunk-Hotspots vor.