नाम: _____ दिनांक: _____ अंक: _____

सार्वजनिक Wi-Fi सुरक्षा और एन्क्रिप्शन

मैन-इन-द-मिडल हमले, फ़र्ज़ी एक्सेस पॉइंट, पैकेट स्निफ़िंग, VPN टनल और HTTPS एन्क्रिप्शन।

सार्वजनिक Wi-Fi सुरक्षा सीखने का अवलोकन

सुरक्षित किया गया
डेटा एन्क्रिप्शन
256-बिट AES मानक

अनुपालक
वैश्विक मानक
GDPR और CCPA फ़्रेमवर्क

ज़ीरो-ट्रस्ट
एक्सेस नीति
मल्टी-फ़ैक्टर ऑथेंटिकेशन

स्वागत है! यह गतिविधि पैकेट आपको सार्वजनिक Wi-Fi सुरक्षा से परिचित कराता है। आप बिना एन्क्रिप्शन वाले नेटवर्क, मैन-इन-द-मिडल (MitM) हमले, रोग एक्सेस पॉइंट, पैकेट स्निफ़िंग, VPN टनल और HTTPS ट्रांज़िट सुरक्षा के बारे में जानेंगे।

वर्कशीट चेकपॉइंट

- [ ] **भाग 1-4: साइबर सुरक्षा और खतरों की रोकथाम में महारत हासिल करें।**
- [ ] **भाग 5-7: क्रॉसवर्ड और वर्ड सर्च पहेलियाँ हल करें।**
- [ ] **भाग 8-9: केस स्टडी और कूट संदेश की चुनौती हल करें।**
- [ ] **भाग 10: बुनियादी और उन्नत FAQ पेज देखें।**
- [ ] **भाग 11: 10 रोचक वास्तविक तथ्यों को जानें।**
- [ ] **अतिरिक्त: झटपट सोचें चुनौती।**

VPN.com साइबर सुरक्षा गाइड खोलें

URL: https://www.vpn.com/hi/saibhar-suraksha/public-wifi-suraksha/

आपका सार्वजनिक Wi-Fi सुरक्षा लर्निंग रोडमैप

- पैकेट स्निफ़िंग और रोग एक्सेस पॉइंट सहित सार्वजनिक Wi-Fi के आम जोखिमों की पहचान करें।
- ट्रांज़िट डेटा सुरक्षित करने के लिए VPN एन्क्रिप्शन टनल लागू करें।
- दूरस्थ कर्मचारियों के लिए HTTPS और सुरक्षित वेब ब्राउज़र सेटिंग लागू करें।

सार्वजनिक Wi-Fi सुरक्षा गाइड निर्देश

बहुविकल्पीय और सही/गलत प्रश्नों के उत्तर दें, शब्द बैंक की मदद से रिक्त स्थान भरें, परिभाषाओं का मिलान करें, और क्रॉसवर्ड तथा वर्ड सर्च पहेलियाँ हल करें। अपने ज्ञान को रिमोट एक्सेस सुरक्षा पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

सार्वजनिक Wi-Fi सुरक्षा और ट्रांज़िट सुरक्षा (परिचय)

बिना एन्क्रिप्ट किए सार्वजनिक Wi-Fi हॉटस्पॉट नेटवर्क ट्रैफ़िक को पैकेट स्निफ़िंग और Evil Twin स्पूफ़िंग के सामने उजागर छोड़ देते हैं। ट्रैफ़िक को सुरक्षित VPN एन्क्रिप्शन टनल से भेजने और केवल-HTTPS HSTS नियम लागू करने से सत्र स्थानीय नेटवर्क में बीच में पकड़े जाने से सुरक्षित रहते हैं।

प्रत्येक चेकपॉइंट को ध्यान से पढ़ें और सही उत्तर चुनें या लिखें।

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1 **1. मैन-इन-द-मिडल (MitM) हमला क्या है?**

- A. साझा नेटवर्क पर दो पक्षों के बीच संचार को बीच में रोकना और बदलना
- B. उपयोगकर्ता रिकॉर्ड को निशाना बनाने वाली डेटाबेस निष्कर्षण तकनीक
- C. नेटवर्क ट्रैफ़िक अनुरोधों से वेब सर्वरों को ओवरलोड करना
- D. लोकल हार्ड ड्राइव स्टोरेज वॉल्यूम मिटाना

2 **2. रोग एक्सेस पॉइंट (Evil Twin) क्या है?**

- A. दुर्भावनापूर्ण Wi-Fi हॉटस्पॉट जो किसी वैध नेटवर्क के समान SSID के साथ कॉन्फ़िगर किया गया हो
- B. डेटाबेस बैकअप की निगरानी के लिए इस्तेमाल होने वाला प्रशासनिक टूल
- C. सुरक्षित VPN गेटवे कॉन्फ़िगरेशन
- D. अधिकृत मेल सर्वरों को मैप करने वाला DNS रिकॉर्ड

3 **3. VPN सार्वजनिक Wi-Fi ट्रैफ़िक की रक्षा कैसे करता है?**

- A. यह सभी नेटवर्क पैकेट को एन्क्रिप्टेड टनल में लपेट देता है, जिससे वे स्निफ़र के लिए अपठनीय हो जाते हैं
- B. यह सभी आने वाले कनेक्शन अनुरोधों को अपने आप ब्लॉक कर देता है
- C. यह भौतिक नेटवर्क कार्ड का MAC पता बदल देता है
- D. यह वेब ब्राउज़र की कैश की गई कुकीज़ हटा देता है

4 **4. पैकेट स्निफ़िंग क्या है?**

- A. नेटवर्क पैकेट पकड़ने और लॉग करने के लिए हार्डवेयर या सॉफ़्टवेयर टूल का उपयोग करना
- B. डुप्लिकेट फ़ाइलों के लिए स्थानीय डायरेक्टरी स्कैन करना
- C. उपयोगकर्ता भूमिकाओं के आधार पर डेटाबेस रीड अनुमतियाँ सीमित करना
- D. AES-256 कुंजियों से स्टोरेज ड्राइव को एन्क्रिप्ट करना

5 **5. HTTPS की भूमिका क्या है?**

- A. ब्राउज़र और वेब सर्वर के बीच सत्र ट्रैफ़िक को एन्क्रिप्ट करना
- B. गेटवे पर आने वाले ईमेल संदेशों को फ़िल्टर करना
- C. पेज तेज़ी से लोड करने के लिए इमेज कंप्रेस करना
- D. नेटवर्क-अटैच्ड स्टोरेज में फ़ाइल संरचनाओं का प्रबंधन

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न 6

6. जुड़े हुए उपयोगकर्ता खुले सार्वजनिक Wi-Fi नेटवर्क पर प्लेनटेक्स्ट डेटा आसानी से कैप्चर कर सकते हैं।

○ सही ○ गलत

7 प्रश्न 7

7. रोग एक्सेस पॉइंट (Evil Twin) को नेटवर्क एडमिनिस्ट्रेटर हमेशा अधिकृत करते हैं।

○ सही ○ गलत

8 प्रश्न 8

8. VPN सार्वजनिक नेटवर्क पर पैकेट स्निफ़िंग से ट्रैफ़िक की सुरक्षा करने में अप्रभावी है।

○ सही ○ गलत

9 प्रश्न 9

9. HTTPS केवल URL पाथ को एन्क्रिप्ट करता है और पैकेट पेलोड को सादे टेक्स्ट में छोड़ देता है।

○ सही ○ गलत

10 प्रश्न 10

10. WPA3 सुरक्षा वाले Wi-Fi हॉटस्पॉट खुले, बिना पासवर्ड वाले नेटवर्क की तुलना में अधिक मज़बूत सुरक्षा देते हैं।

○ सही ○ गलत

चेकपॉइंट 3: मुख्य शब्द भरें

नीचे दिए गए प्रत्येक वाक्य को पढ़ें और रिक्त स्थान को वर्ड बैंक के सही शब्द से भरें।

1. खुले वाई-फ़ाई पर आपके डेटा को पढ़ने लायक न रखने वाली तकनीक _____ कहलाती है।

2. किसी हॉटस्पॉट से जुड़ने से पहले उसके नाम का स्टाफ़ से _____ कर लेना नकली नेटवर्क से बचाता है।

3. होटल के Wi-Fi की नकल करने वाला फ़र्ज़ी हॉटस्पॉट _____ है।

4. वेब ट्रैफ़िक के ट्रांज़िट को सुरक्षित करने के लिए _____ से एन्क्रिप्ट करना ज़रूरी है।

5. सारा नेटवर्क आउटपुट एन्क्रिप्ट करने के लिए क्लाइंट _____ का उपयोग होता है।

6. सार्वजनिक नेटवर्कों से गुज़रने वाला एन्क्रिप्टेड संचार मार्ग एक _____ है।

शब्दावली शब्द-बैंक

ईविल ट्विन | एचटीटीपीएस | एन्क्रिप्शन | टनल | वीपीएन | सत्यापन | स्निफ़िंग | WPA3

अपने उत्तर यहाँ लिखें:

1.
2.
3.
4.
5.
6.

चेकपॉइंट 4: सुरक्षा अवधारणा मिलान

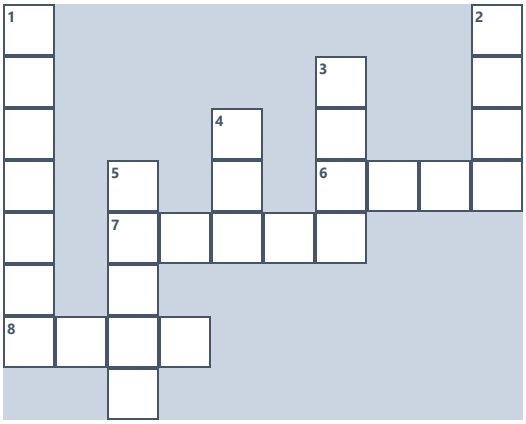
परिभाषा मिलान

बाईं ओर के प्रत्येक शब्दावली पद को दाईं ओर की सही परिभाषा से मिलाएँ; भरने योग्य इनपुट बॉक्स में संबंधित अक्षर (A-H) लिखें।

☐	**1. इंटरसेप्शन**	**A**	आधुनिक Wi-Fi सुरक्षा मानक।
☐	**2. स्निफ़िंग**	**B**	पारगमन के दौरान सुरक्षित डेटा पथ।
☐	**3. ईविल ट्विन**	**C**	आने वाले ट्रैफ़िक को फ़िल्टर करना।
☐	**4. HTTPS**	**D**	Wi-Fi की नकल करने वाला रोग हॉटस्पॉट।
☐	**5. VPN**	**E**	ट्रांज़िट में ट्रैफ़िक को पढ़ना।
☐	**6. टनल**	**F**	नेटवर्क डेटा पैकेट कैप्चर करना।
☐	**7. WPA3**	**G**	एन्क्रिप्टेड वर्चुअल प्राइवेट नेटवर्क।
☐	**8. फ़ायरवॉल**	**H**	सुरक्षित वेब ट्रांसमिशन।

चेकपॉइंट 5: क्रॉसवर्ड पहेली

सक्रिय सफ़ेद खानों में अक्षर टाइप करके क्रॉसवर्ड पहेली हल करें। संख्याएँ नीचे दिए गए संकेतों से मेल खाती हैं।



बाएँ से दाएँ

6. जानकारी को कूट रूप में बदलकर दूसरों के लिए अपठनीय बनाने की विधि (4)

7. Wi-Fi की नकल करने वाला फ़र्ज़ी हॉटस्पॉट। (5)

8. किसी दावे या पहचान की सच्चाई की पुष्टि करना (4)

ऊपर से नीचे

1. सुरक्षित वेब ट्रांसमिशन। (7)

2. वह जानकारी जिससे ऑनलाइन पता चलता है कि आप कौन हैं (4)

3. एन्क्रिप्टेड वर्चुअल प्राइवेट नेटवर्क। (4)

4. ट्रांज़िट में डेटा का सुरक्षित मार्ग। (3)

5. इंटरनेट पर आपके उपकरण को पहचान दिलाने वाला अंकीय पता (5)

चेकपॉइंट 5, वैकल्पिक: सुलभ क्रॉसवर्ड संकेत

स्क्रीन-रीडर और कीबोर्ड उपयोगकर्ता क्रॉसवर्ड के उत्तर सीधे नीचे दिए गए टेक्स्ट फ़ील्ड में टाइप कर सकते हैं।

बाएँ से दाएँ

6 बाएँ से दाएँ: जानकारी को कूट रूप में बदलकर दूसरों के लिए अपठनीय बनाने की विधि (4 अक्षर):

7 बाएँ से दाएँ: Wi-Fi की नकल करने वाला फ़र्ज़ी हॉटस्पॉट। (5 अक्षर):

8 बाएँ से दाएँ: किसी दावे या पहचान की सच्चाई की पुष्टि करना (4 अक्षर):

ऊपर से नीचे

1 ऊपर से नीचे: सुरक्षित वेब ट्रांसमिशन। (7 अक्षर):

2 ऊपर से नीचे: वह जानकारी जिससे ऑनलाइन पता चलता है कि आप कौन हैं (4 अक्षर):

3 ऊपर से नीचे: एन्क्रिप्टेड वर्चुअल प्राइवेट नेटवर्क। (4 अक्षर):

4 ऊपर से नीचे: ट्रांज़िट में डेटा का सुरक्षित मार्ग। (3 अक्षर):

5 ऊपर से नीचे: इंटरनेट पर आपके उपकरण को पहचान दिलाने वाला अंकीय पता (5 अक्षर):

चेकपॉइंट 6: छिपे शब्द खोजें

नीचे दी गई ग्रिड में छिपे 8 प्रमुख शब्दावली शब्द खोजें। शब्द क्षैतिज, ऊर्ध्वाधर या तिरछे हो सकते हैं।

ज	द	दि	ते	वी	ति	च	ह	री	रा	व	त	सा	स	ई
ते	ता	घ	इ	नी	ल	रि	द	ए	जे	घ	छ	ई	के	द
प	प	ति	के	ट	मि	ट	सा	य	न्क्रि	च	ऊ	नी	जी	इ
त	पी	म	पे	ब	प	जि	मी	ने	ले	प्श	इ	ट	न	ल
सी	ई	य	छ	र	ए	दे	कि	जा	सा	वा	न	ड	रे	स
ख	आ	नि	फ	ढ	च	मा	ई	ना	का	रे	स	त्या	प	न
दे	सि	मी	क	पि	टी	ता	ति	वि	ज	श	भ	ऊ	अ	ऊ
ए	रि	वि	श	य	टी	वि	व	वा	ल	पा	ल	च	से	कि
न	य	घ	प	के	पी	की	व	सि	री	द्वि	त	की	कि	सि
ए	ना	ने	पा	ते	ए	ण	ए	ता	सा	मी	न	न	नी	ऋ
पी	ले	घ	ति	जि	स	ला	ए	जी	ले	ड	ल	द	जे	प
वी	घ	के	च	से	दे	री	ए	पी	उ	अ	जे	मि	ह	घ
व	आ	च	मी	च	ट	थ	फ	ग	ना	सी	का	चा	ज	फ
नी	जी	ता	ठ	से	लि	ट	आ	इ	से	रा	न	के	री	पा
वा	सि	य	नि	पि	ने	ख	के	वे	ऊ	ड	नी	दे	दि	भ

शब्दावली शब्द-सूची

ईविलट्विन · एचटीटीपीएस · वीपीएन · टनल · एन्क्रिप्शन · आईपीपता · पहचान · सत्यापन

चेकपॉइंट 6, वैकल्पिक: सुलभ शब्दावली मिलान

वर्ड सर्च के 8 शब्दावली पदों में से प्रत्येक को उसकी सही परिभाषा से मिलाएँ; खाली स्थान में अक्षर (A-H) लिखें।

शब्दावली के शब्द

- **A. ईविलट्विन**
- **B. एचटीटीपीएस**
- **C. वीपीएन**
- **D. टनल**
- **E. एन्क्रिप्शन**
- **F. आईपीपता**
- **G. पहचान**
- **H. सत्यापन**

परिभाषाएँ और मिलान फ़ील्ड

1. वह जानकारी जिससे ऑनलाइन पता चलता है कि आप कौन हैं।
2. एन्क्रिप्टेड वर्चुअल प्राइवेट नेटवर्क।
3. सुरक्षित वेब ट्रांसमिशन।
4. इंटरनेट पर आपके उपकरण को पहचान दिलाने वाला अंकीय पता।
5. किसी दावे या पहचान की सच्चाई की पुष्टि करना।
6. Wi-Fi की नकल करने वाला फ़र्ज़ी हॉटस्पॉट।
7. जानकारी को कूट रूप में बदलकर दूसरों के लिए अपठनीय बनाने की विधि।
8. ट्रांज़िट में डेटा का सुरक्षित मार्ग।

चेकपॉइंट 7: उलझे शब्दों की चुनौती

नीचे के अक्षरों को सुलझाकर साइबर सुरक्षा की प्रमुख अवधारणाएँ और शब्द पता करें। अपने उत्तर दिए गए इनपुट बॉक्स में लिखें।

1. **ट्वि ल ई न वि** _____
2. **वी ए न पी** _____
3. **न ए प्शा न्क्रि** _____
4. **न चा प ह** _____
5. **पी स टी टी ए ए च** _____
6. **न ल ट** _____
7. **प ता आ पी ई** _____
8. **स न प त्या** _____

अतिरिक्त गतिविधि: झटपट सोचें

हर श्रेणी में 3 उत्तर। जो सबसे पहले सूची भर दे, वह जीतता है।

1	सॉफ़्टवेयर अपडेट करने के कारण			
2	ऐसे डिवाइस जो Wi-Fi से अपने-आप कनेक्ट हो जाते हैं			
3	ऐसी जानकारी जो आपको कभी साझा नहीं करनी चाहिए			
4	सुरक्षित आदतें जो आप आज से शुरू कर सकते हैं			
5	कैफ़े में सुरक्षित रहने के तरीके			
6	ऐसे डिवाइस जिन्हें हैक किया जा सकता है			
7	ऐसी चीज़ें जो हैकर खुले Wi-Fi पर देख सकता है			
8	नकली Wi-Fi नेटवर्क के संकेत			
9	सार्वजनिक Wi-Fi के विकल्प			
10	ईमेल में चेतावनी के संकेत			
11	ऐसी चीज़ें जो आप सार्वजनिक Wi-Fi पर नहीं करते			
12	मुफ़्त Wi-Fi वाली जगहें			
13	अपने अकाउंट सुरक्षित रखने के तरीके			
14	कंप्यूटर के संक्रमित होने के संकेत			
15	संदिग्ध लगने वाले Wi-Fi नाम			

चेकपॉइंट 8: साइबर सुरक्षा केस स्टडी

नीचे दिए गए वास्तविक परिदृश्यों को हल करने के लिए सीखी हुई अवधारणाओं का उपयोग करें।

केस स्टडी 1: सार्वजनिक Wi-Fi पर पैकेट स्निफ़िंग की रोकथाम



परिदृश्य: सार्वजनिक हवाई अड्डे के Wi-Fi नेटवर्क से जुड़ा एक रिमोट सेल्स एग्ज़ीक्यूटिव देखता है कि प्लेनटेक्स्ट में भेजे गए कई संवेदनशील बिज़नेस ईमेल भेजने के कुछ ही देर बाद लीक हो गए।

चर्चा प्रश्न: सार्वजनिक नेटवर्क के जोखिमों का विश्लेषण कीजिए और ट्रैफ़िक एन्क्रिप्शन समाधान की रूपरेखा बताइए।

केस स्टडी 2: Evil Twin फ़र्ज़ी हॉटस्पॉट से बचाव



परिदृश्य: हमलावर 'CoffeeShop_Guest' नाम का फ़र्ज़ी वायरलेस एक्सेस पॉइंट तैनात करते हैं, जो किसी असली कैफ़े हॉटस्पॉट की नकल करता है और अनजान मेहमानों का नेटवर्क ट्रैफ़िक पकड़ता है।

चर्चा प्रश्न: फ़र्ज़ी एक्सेस पॉइंट का पता लगाने और उन्हें ब्लॉक करने के सत्यापन चरणों का विवरण दीजिए।

चेकपॉइंट 9: कूट संदेश को डिकोड करें

साइबर सुरक्षा पेशेवर नेटवर्क संपत्तियों को ऑनलाइन ख़तरा पैदा करने वालों से बचाता है। नीचे दी गई अक्षर-से-संख्या कुंजी का उपयोग करके संदेश को डिक्रिप्ट करें और खाली स्थानों में मेल खाते अक्षर लिखें।

अक्षर-से-संख्या एन्क्रिप्शन कुंजी

अ=1 आ=2 इ=3 ई=4 उ=5 ऊ=6 ऋ=7 ए=8 ऐ=9 ओ=10 औ=11 ऑ=12

क=13 ख=14 ग=15 घ=16 ङ=17 च=18 छ=19 ज=20 झ=21 ञ=22 ट=23 ठ=24

ड=25 ढ=26 ण=27 त=28 थ=29 द=30 ध=31 न=32 प=33 फ=34 ब=35 भ=36

म=37 य=38 र=39 ल=40 व=41 श=42 ष=43 स=44 ह=45 ा=46 ि=47 ी=48

ु=49 ू=50 ृ=51 े=52 ै=53 ो=54 ौ=55 ॉ=56 ं=57 ँ=58 ः=59 ़=60

्=61

41	48	33	48	8	32		44	52		33	35	61	40	47	13

41	46	4	34	60	46	4		8	32	61	13	61	39	47	33	61	23

13	39	52	57

डिकोड किया गया संदेश:

सुझाव: हर संख्या वर्णमाला में उस अक्षर की स्थिति दर्शाती है (जैसे 1 = अ, 2 = आ, 61 = ्)।

चेकपॉइंट 10: बुनियादी साइबर सुरक्षा FAQ (भाग A)

ऑनलाइन खतरों को कम करने से जुड़े आम सवाल और जवाब देखें।

Q1: सार्वजनिक Wi-Fi असुरक्षित क्यों है?

खुला सार्वजनिक Wi-Fi हवा में ट्रैफ़िक को एन्क्रिप्ट नहीं करता, इसलिए आसपास के लोग किसी भी असुरक्षित डेटा को पकड़ सकते हैं। [2]

Q2: पैकेट स्निफ़िंग क्या है?

पैकेट स्निफ़र नेटवर्क इंटरफ़ेस पर बह रहे कच्चे डेटा को पकड़ लेता है, जिससे सादे पाठ वाले पासवर्ड और ट्रैफ़िक का विवरण उजागर हो जाता है।

Q3: Evil Twin क्या है?

हैकरों द्वारा बनाया गया फ़र्ज़ी एक्सेस पॉइंट जो किसी भरोसेमंद स्थानीय Wi-Fi हॉटस्पॉट के नाम और सेटिंग की नकल करता है।

Q4: VPN मेरी सुरक्षा कैसे करता है?

यह आपके ट्रैफ़िक को एन्क्रिप्टेड टनल से रूट करता है, जिससे आपकी ब्राउज़िंग गतिविधि स्थानीय नेटवर्क स्निफ़र से छिपी रहती है।

Q5: क्या सार्वजनिक Wi-Fi पर HTTPS मेरी सुरक्षा करता है?

हाँ, यह आपके ब्राउज़र और वेबसाइट के बीच आदान-प्रदान होने वाले डेटा को एन्क्रिप्ट करता है, और VPN सुरक्षा की एक और परत जोड़ता है।

चेकपॉइंट 10: बुनियादी साइबर सुरक्षा FAQ (भाग B)

ऑनलाइन खतरों को कम करने से जुड़े आम सवाल और जवाब देखें।

Q6: WPA3 क्या है?

आधुनिक Wi-Fi Protected Access मानक, जो मज़बूत एन्क्रिप्शन और ऑफ़लाइन डिक्शनरी हमलों से सुरक्षा देता है। [1]

Q7: क्या सार्वजनिक Wi-Fi मैलवेयर पहुँचा सकता है?

हाँ, हमलावर ट्रैफ़िक को बीच में पकड़ सकते हैं और आपके ब्राउज़र सत्र में दुर्भावनापूर्ण डाउनलोड प्रॉम्प्ट (ड्राइव-बाय डाउनलोड) डाल सकते हैं।

Q8: फ़ाइल शेयरिंग का जोखिम क्या है?

यदि फ़ाइल शेयरिंग चालू है, तो सार्वजनिक नेटवर्क पर मौजूद अन्य उपयोगकर्ता आपकी स्थानीय फ़ोल्डर डायरेक्टरी पढ़ या बदल सकते हैं।

Q9: कैप्टिव पोर्टल क्या है?

होटल या कैफ़े के नेटवर्क इंटरनेट एक्सेस देने के लिए जिस लॉगिन पेज का उपयोग करते हैं, जिसकी हमलावर कभी-कभी नकल कर सकते हैं।

Q10: क्या उपयोग न होने पर मुझे Wi-Fi बंद कर देना चाहिए?

हाँ, Wi-Fi बंद करने से आपका डिवाइस अपने-आप अविश्वसनीय नेटवर्क से कनेक्ट नहीं होता।

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग C)

सुरक्षा फ़्रेमवर्क, मैलवेयर विश्लेषण और डेटा अनुपालन के उन्नत तकनीकी पहलुओं को जानें।

Q1: मैन-इन-द-मिडिल हमला DNS का फ़ायदा कैसे उठाता है?

लक्षित डोमेन के बजाय ब्राउज़रों को मिलते-जुलते फ़िशिंग लैंडिंग पेजों पर भेजने के लिए दुष्ट राउटर पर DNS स्पूफ़िंग का उपयोग करके।

Q2: सेशन हाईजैकिंग क्या है?

हमलावर सार्वजनिक Wi-Fi पर बिना एन्क्रिप्शन वाली सत्र कुकी को स्निफ़ करके उसे इंपोर्ट करता है ताकि क्रेडेंशियल लॉगिन को बायपास कर सके।

Q3: SSL स्ट्रिपिंग क्या है?

एक MitM हमला, जिसमें हमलावर उपयोगकर्ता के सुरक्षित HTTPS अनुरोध को बिना एन्क्रिप्शन वाले HTTP में डाउनग्रेड कर देता है और लॉगिन को सादे पाठ में पकड़ लेता है।

Q4: HSTS, SSL स्ट्रिपिंग से कैसे बचाता है?

HTTP Strict Transport Security ब्राउज़र को केवल HTTPS से कनेक्ट होने के लिए मजबूर करता है और असुरक्षित HTTP पर लौटने से मना करता है। [3]

Q5: स्प्लिट-टनल VPN क्या है?

ऐसा कॉन्फ़िगरेशन जो केवल कॉर्पोरेट ट्रैफ़िक को VPN से भेजता है और सार्वजनिक इंटरनेट डेटा सीधे भेजता है, जिससे लीक पथ के उजागर होने का जोखिम हो सकता है।

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग D)

सुरक्षा फ़्रेमवर्क, मैलवेयर विश्लेषण और डेटा अनुपालन के उन्नत तकनीकी पहलुओं को जानें।

Q6: WPA2 KRACK के प्रति असुरक्षित क्यों है?

Key Reinstallation Attack WPA2 के फ़ोर-वे हैंडशेक का फ़ायदा उठाकर Wi-Fi पासवर्ड के बिना पैकेट डिक्रिप्ट कर देता है।

Q7: क्लाइंट आइसोलेशन क्या है?

राउटर सुरक्षा सेटिंग जो जुड़े हुए Wi-Fi उपकरणों को आपस में सीधे संवाद करने से रोकती है और स्थानीय स्निफ़िंग को ब्लॉक करती है।

Q8: हमलावर नकली DNS सर्वर का उपयोग कैसे करते हैं?

वे फ़र्ज़ी राउटर को इस तरह कॉन्फ़िगर करते हैं कि क्लाइंट को नकली DNS सर्वर मिलें, जिससे वे सभी वेब लुकअप को बीच में पकड़कर बदल सकें।

Q9: क्या VPN मेरा लोकल MAC पता छिपा सकता है?

नहीं। MAC पते स्थानीय लेयर-2 पहचानकर्ता हैं; इसके बजाय अपने डिवाइस की अंतर्निहित MAC रैंडमाइज़ेशन (निजी पता) सेटिंग इस्तेमाल करें।

Q10: कैप्टिव पोर्टल स्पूफ़िंग हमला क्या है?

हमलावर जो मुफ़्त Wi-Fi पहुँच के बहाने क्रेडेंशियल चुराने के लिए फ़र्ज़ी हॉटस्पॉट पर नकली ऑथेंटिकेशन पोर्टल चलाता है।

भाग 11: 10 वास्तविक साइबर सुरक्षा तथ्य और अंतर्दृष्टियाँ

सुरक्षा उल्लंघनों, बचाव तंत्रों और अनुपालन मानकों से जुड़े वास्तविक तथ्य देखें।

1. सुरक्षा इनसाइट

रिमोट कर्मचारी अक्सर कैफ़े, होटल और हवाई अड्डों पर Wi-Fi इस्तेमाल करते हैं, जहाँ वे नेटवर्क की सुरक्षा को नियंत्रित नहीं कर सकते।

2. सुरक्षा इनसाइट

Evil Twin फ़र्ज़ी हॉटस्पॉट किसी भरोसेमंद नेटवर्क का सटीक नाम और MAC पता कॉपी करके उपकरणों को भ्रमित कर सकता है।

3. सुरक्षा इनसाइट

Wireshark जैसे पैकेट स्निफ़िंग सॉफ़्टवेयर मुफ़्त हैं और अन-एन्क्रिप्टेड HTTP पासवर्ड को सादे टेक्स्ट में दिखा सकते हैं।

4. सुरक्षा इनसाइट

WPA3 सुरक्षा स्थानीय ब्रूट फ़ोर्स हमलों से बचाव के लिए Simultaneous Authentication of Equals (SAE) का उपयोग करती है।

5. सुरक्षा इनसाइट

SSL स्ट्रिपिंग हमले गेटवे पर शुरुआती HTTP रीडायरेक्ट को इंटरसेप्ट करके बुनियादी HTTPS सुरक्षा को बायपास कर देते हैं।

6. सुरक्षा इनसाइट

HTTP Strict Transport Security (HSTS) रिस्पॉन्स हेडर ब्राउज़र को असुरक्षित HTTP कनेक्शन पर लौटने से रोकते हैं। [3]

7. सिक्योरिटी इनसाइट

'Auto-Connect' बंद करने से स्मार्टफ़ोन सार्वजनिक जगहों पर हूबहू दिखने वाले फ़र्ज़ी नेटवर्कों से जुड़ने से बचते हैं।

8. सिक्योरिटी इनसाइट

एंटरप्राइज़ 'always-on' VPN कॉन्फ़िगरेशन सभी दूरस्थ कर्मचारियों के नेटवर्क ट्रैफ़िक को कॉर्पोरेट फ़ायरवॉल से होकर गुज़रने के लिए बाध्य करते हैं।

9. सिक्योरिटी इनसाइट

रोग एक्सेस पॉइंट जाली DNS जवाब दे सकते हैं, जिससे लक्षित डोमेन फ़िशिंग सर्वरों पर रीडायरेक्ट हो जाते हैं।

10. सुरक्षा इनसाइट

VPN के बिना, खुले हॉटस्पॉट पर अन्य उपयोगकर्ता देख सकते हैं कि आपका डिवाइस किन साइटों और सर्वरों से संपर्क करता है।

तकनीकी संदर्भ और स्रोत

यह अध्ययन गाइड और इंटरैक्टिव पहेलियाँ वैश्विक NIST, OWASP और डेटा गोपनीयता अनुपालन मानकों से तैयार की गई हैं।

शैक्षणिक और उद्योग संदर्भ

[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

उत्तर कुंजी: चेकपॉइंट 1 – बहुविकल्पीय

1 प्रश्न 1 — **सही उत्तर: A**

शिक्षण नोट

मैन-इन-द-मिडल (MitM) हमला क्या है? → साझा नेटवर्क पर दो पक्षों के बीच संचार को बीच में रोकना और बदलना

2 प्रश्न 2 — **सही उत्तर: A**

शिक्षण नोट

रोग एक्सेस पॉइंट (Evil Twin) क्या है? → दुर्भावनापूर्ण Wi-Fi हॉटस्पॉट जो किसी वैध नेटवर्क के समान SSID के साथ कॉन्फ़िगर किया गया हो

3 प्रश्न 3 — **सही उत्तर: A**

शिक्षण नोट

VPN सार्वजनिक Wi-Fi ट्रैफ़िक की रक्षा कैसे करता है? → यह सभी नेटवर्क पैकेट को एन्क्रिप्टेड टनल में लपेट देता है, जिससे वे स्निफ़र के लिए अपठनीय हो जाते हैं

4 प्रश्न 4 — **सही उत्तर: A**

शिक्षण नोट

पैकेट स्निफ़िंग क्या है? → नेटवर्क पैकेट पकड़ने और लॉग करने के लिए हार्डवेयर या सॉफ़्टवेयर टूल का उपयोग करना

5 प्रश्न 5 — **सही उत्तर: A**

शिक्षण नोट

HTTPS की भूमिका क्या है? → ब्राउज़र और वेब सर्वर के बीच सत्र ट्रैफ़िक को एन्क्रिप्ट करना

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 **प्रश्न 6** **सही उत्तर: सही**

शिक्षण नोट

जुड़े हुए उपयोगकर्ता खुले सार्वजनिक Wi-Fi नेटवर्क पर प्लेनटेक्स्ट डेटा आसानी से कैप्चर कर सकते हैं।

7 **प्रश्न 7** **सही उत्तर: गलत**

शिक्षण नोट

गलत: Evil Twin हमलावर द्वारा किसी असली हॉटस्पॉट की नकल करने के लिए बनाया गया अनधिकृत हॉटस्पॉट है।

8 **प्रश्न 8** **सही उत्तर: गलत**

शिक्षण नोट

गलत: VPN ट्रैफ़िक को टनल में एन्क्रिप्ट करता है, इसलिए लोकल स्निफ़र उसे पढ़ नहीं सकते।

9 **प्रश्न 9** **सही उत्तर: गलत**

शिक्षण नोट

गलत: HTTPS पूरे HTTP आदान-प्रदान को एन्क्रिप्ट करता है, जिसमें URL पाथ और पेज की सामग्री भी शामिल है।

10 **प्रश्न 10** **सही उत्तर: सही**

शिक्षण नोट

WPA3 सुरक्षा वाले Wi-Fi हॉटस्पॉट खुले, बिना पासवर्ड वाले नेटवर्क की तुलना में अधिक मज़बूत सुरक्षा देते हैं।

शब्दावली कुंजियाँ और ग्रेडिंग रूब्रिक

शिक्षक के लिए ग्रेडिंग रूब्रिक: हर सही मिलान (कुल 8 अंक) और संदर्भ शब्द (कुल 6 अंक) के लिए 1 अंक दें।

चेकपॉइंट 4: उत्तर – अवधारणा मिलान

E 1. इंटरसेप्शन	F 2. स्निफ़िंग	D 3. ईविल ट्विन	H 4. HTTPS
G 5. VPN	B 6. टनल	A 7. WPA3	C 8. फ़ायरवॉल

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 एन्क्रिप्शन	2 सत्यापन	3 ईविल ट्विन	4 एचटीटीपीएस
5 वीपीएन	6 टनल		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

1 G – पहचान	2 C – वीपीएन	3 B – एचटीटीपीएस	4 F – आईपीपता
5 H – सत्यापन	6 A – ईविलट्विन	7 E – एन्क्रिप्शन	8 D – टनल

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी इंटरसेप्शन, स्निफ़िंग और ईविल ट्विन को अपने शब्दों में समझा सकते हैं और हर एक का उदाहरण दे सकते हैं।

केस स्टडी:
विद्यार्थियों से कहें कि वे अपनी सिफ़ारिशें राय के बजाय वर्कशीट के तथ्यों पर आधारित करें।

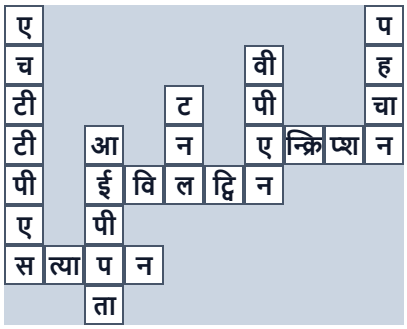
स्रोतों का मूल्यांकन:
विद्यार्थियों से वर्कशीट के स्रोतों में कम से कम एक कथन की पुष्टि करवाएँ और चर्चा करें कि आँकड़े, कीमतें और नियम समय के साथ क्यों बदल सकते हैं।

पहेलियों की कुंजियाँ और शिक्षक नोट

शब्द खोज समाधान

ज	द	दि	ते	वी	ति	च	ह	री	रा	व	त	सा	स	ई
ते	ता	घ	इ	नी	ल	रि	द	ए	जे	घ	छ	ई	के	द
प	प	ति	के	ट	मि	ट	सा	य	न्क्रि	च	ऊ	नी	जी	इ
त	पी	म	पे	ब	प	जि	मी	ने	ले	प्श	इ	ट	न	ल
सी	ई	य	छ	र	ए	दे	कि	जा	सा	वा	न	ड	रे	स
ख	आ	नि	फ	ढ	च	मा	ई	ना	का	रे	स	त्या	प	न
दे	सि	मी	क	पि	टी	ता	ति	वि	ज	श	भ	ऊ	अ	ऊ
ए	रि	वि	श	य	टी	वि	व	वा	ल	पा	ल	च	से	कि
न	य	घ	प	के	पी	की	व	सि	री	द्वि	त	की	कि	सि
ए	ना	ने	पा	ते	ए	ण	ए	ता	सा	मी	न	न	नी	ऋ
पी	ले	घ	ति	जि	स	ला	ए	जी	ले	ड	ल	द	जे	प
वी	घ	के	च	से	दे	री	ए	पी	उ	अ	जे	मि	ह	घ
व	आ	च	मी	च	ट	थ	फ	ग	ना	सी	का	चा	ज	फ
नी	जी	ता	ठ	से	लि	ट	आ	इ	से	रा	न	के	री	पा
वा	सि	य	नि	पि	ने	ख	के	वे	ऊ	ड	नी	दे	दि	भ

क्रॉसवर्ड समाधान



क्रॉसवर्ड समाधान के लिए शिक्षक गाइड

बाएँ से दाएँ

6 बाएँ से दाएँ: एन्क्रिप्शन जानकारी को कूट रूप में बदलकर दूसरों के लिए अपठनीय बनाने की विधि (4 अक्षर)

7 बाएँ से दाएँ: ईविलट्विन Wi-Fi की नकल करने वाला फ़र्ज़ी हॉटस्पॉट। (5 अक्षर)

8 बाएँ से दाएँ: सत्यापन किसी दावे या पहचान की सच्चाई की पुष्टि करना (4 अक्षर)

ऊपर से नीचे

1 ऊपर से नीचे: एचटीटीपीएस सुरक्षित वेब ट्रांसमिशन। (7 अक्षर)

2 ऊपर से नीचे: पहचान वह जानकारी जिससे ऑनलाइन पता चलता है कि आप कौन हैं (4 अक्षर)

3 ऊपर से नीचे: वीपीएन एन्क्रिप्टेड वर्चुअल प्राइवेट नेटवर्क। (4 अक्षर)

4 ऊपर से नीचे: टनल ट्रांज़िट में डेटा का सुरक्षित मार्ग। (3 अक्षर)

5 ऊपर से नीचे: आईपीपता इंटरनेट पर आपके उपकरण को पहचान दिलाने वाला अंकीय पता (5 अक्षर)

अक्षर-फेर शब्द और कूट संदेश हल कुंजी

शब्द-अनस्क्रैम्बल गतिविधि और Secret Cipher Challenge की ग्रेडिंग कुंजी।

शब्द अनस्क्रैम्बल कुंजी

1. द्विलईनवि — **ईविलट्विन**
2. वीएनपी — **वीपीएन**
3. नएप्शक्रि — **एन्क्रिप्शन**
4. नचापह — **पहचान**
5. पीसटीटीएएच — **एचटीटीपीएस**
6. नलट — **टनल**
7. पताआपीई — **आईपीपता**
8. सनपत्या — **सत्यापन**

गुप्त कूट चुनौती कुंजी

"वीपीएन से पब्लिक वाईफ़ाई एन्क्रिप्ट करें"

केस स्टडी के उत्तर

A केस स्टडी 1: सार्वजनिक Wi-Fi पर पैकेट स्निफ़िंग की रोकथाम

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: हवाई अड्डे के सार्वजनिक Wi-Fi नेटवर्क से जुड़ा एक रिमोट सेल्स एग्ज़ीक्यूटिव देखता है कि कई संवेदनशील बिज़नेस ईमेल प्लेनटेक्स्ट में भेजे जाने के कुछ ही देर बाद लीक हो गए।
- अनुशंसित रणनीति और समाधान: सभी रिमोट वर्कस्टेशन पर एंटरप्राइज़ VPN क्लाइंट का उपयोग अनिवार्य करें। केवल HTTPS वाले ब्राउज़र एक्सटेंशन लागू करें, और क्लाइंट फ़ायरवॉल पर बिना एन्क्रिप्शन वाले प्रोटोकॉल (जैसे HTTP और FTP) ब्लॉक करें।

B केस स्टडी 2: Evil Twin फ़र्ज़ी हॉटस्पॉट से बचाव

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: हमलावर किसी वैध कैफ़े हॉटस्पॉट की नकल करते हुए 'CoffeeShop_Guest' नाम का एक फ़र्ज़ी वायरलेस एक्सेस पॉइंट लगा देते हैं और अनजान मेहमानों का नेटवर्क ट्रैफ़िक पकड़ लेते हैं।
- अनुशंसित रणनीति और समाधान: नेटवर्क की प्रामाणिकता सत्यापित करने के लिए एक्सेस पॉइंट के BSSID MAC पतों का ऑडिट करें। खुले नेटवर्क से कनेक्शन रोकने के लिए क्लाइंट पोस्चर वैलिडेशन लागू करें, और संवेदनशील काम के लिए सेल्युलर हॉटस्पॉट अनिवार्य करें।