नाम: _____ दिनांक: _____ अंक: _____

फ़िशिंग हमले और सोशल इंजीनियरिंग

स्पीयर फ़िशिंग, व्हेलिंग घोटाले, SPF/DKIM/DMARC प्रोटोकॉल, प्रेषक स्पूफ़िंग और कर्मचारी सुरक्षा प्रशिक्षण।

फ़िशिंग हमले 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 फ़िशिंग हमलों और सोशल इंजीनियरिंग से परिचित कराता है। आप स्पीयर फ़िशिंग, व्हेलिंग, डोमेन स्पूफ़िंग, SPF/DKIM/DMARC प्रोटोकॉल, लिंक सुरक्षा और कर्मचारी जागरूकता प्रशिक्षण का अध्ययन करेंगे।

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/phishing-hamare/

आपका फ़िशिंग शमन लर्निंग रोडमैप

- आम फ़िशिंग, विशिंग और सपोर्ट पॉप-अप स्कैम की पहचान करें।
- आउट-ऑफ़-बैंड लेन-देन सत्यापन प्रक्रियाएँ लागू करें।
- स्पूफ़ किए गए डोमेन को ब्लॉक करने के लिए SPF, DKIM और DMARC नियम कॉन्फ़िगर करें।

फ़िशिंग हमले 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 ईमेल प्रमाणीकरण पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

फ़िशिंग हमले और सोशल इंजीनियरिंग (परिचय)

फ़िशिंग हमले उपयोगकर्ता के लॉगिन क्रेडेंशियल चुराने के लिए लक्षित संदेश, व्हेलिंग घोटाले और डोमेन स्पूफ़िंग का उपयोग करते हैं। कॉर्पोरेट सिस्टम सुरक्षित करने के लिए गेटवे पर SPF, DKIM और DMARC नियम तथा आउट-ऑफ़-बैंड अनुमोदन चरण लागू करने पड़ते हैं।

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

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1 **1. स्पीयर फ़िशिंग क्या है?**

- A. किसी विशेष व्यक्ति या संगठन के अनुसार तैयार किया गया लक्षित फ़िशिंग ईमेल
- B. लाखों यादृच्छिक पतों पर भेजा गया बड़ा थोक ईमेल
- C. वेब सर्वरों को ट्रैफ़िक से भर देने वाला नेटवर्क हमला
- D. उपयोगकर्ता रिकॉर्ड को निशाना बनाने वाली डेटाबेस एक्सट्रैक्शन तकनीक

2 **2. कौन-सा प्रोटोकॉल किसी डोमेन को स्पूफ़िंग से लड़ने के लिए DNS में अपने अधिकृत भेजने वाले IP एड्रेस सूचीबद्ध करने देता है?**

- A. SPF
- B. DKIM
- C. DMARC
- D. HTTPS

3 **3. व्हेलिंग हमला क्या है?**

- A. फ़िशिंग अभियान जो विशेष रूप से उच्च-प्रोफ़ाइल कॉर्पोरेट अधिकारियों को निशाना बनाता है
- B. डेटाबेस बैकअप को निशाना बनाने वाला SQL इंजेक्शन हमला
- C. स्थानीय क्षेत्र नेटवर्क राउटर उपकरण की भौतिक चोरी
- D. स्वचालित क्रेडेंशियल स्टफ़िंग ब्रूट-फ़ोर्स स्कैन

4 **4. DKIM क्या करता है?**

- A. प्रेषक की प्रामाणिकता सत्यापित करने के लिए ईमेल में क्रिप्टोग्राफ़िक हस्ताक्षर जोड़ता है
- B. फ़ायरवॉल पर आने वाले नेटवर्क पैकेट ट्रैफ़िक को ब्लॉक करता है
- C. स्टोरेज में रखे डेटाबेस वॉल्यूम को एन्क्रिप्ट करता है
- D. सिग्नेचर-आधारित मैलवेयर के लिए ईमेल अटैचमेंट स्कैन करता है

5 **5. DMARC की भूमिका क्या है?**

- A. प्राप्त करने वाले ईमेल सर्वरों को निर्देश देना कि विफल SPF/DKIM जाँच को कैसे संभालें
- B. पहले से गणना की गई रेनबो तालिकाओं से सिस्टम पासवर्ड डिक्रिप्ट करना
- C. डिलीवरी से पहले ईमेल अटैचमेंट कंप्रेस करना
- D. नेटवर्क रूटिंग एक्सेस विशेषाधिकार कॉन्फ़िगर करना

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न 6

6. स्पीयर फ़िशिंग लाखों यादृच्छिक पतों पर भेजे गए सामान्य बल्क ईमेल पर निर्भर करती है।

○ सही ○ गलत

7 प्रश्न 7

7. DMARC नीतियाँ मेल सर्वरों को अनधिकृत स्पूफ़ किए गए संदेशों को अस्वीकार करने का निर्देश दे सकती हैं।

○ सही ○ गलत

8 प्रश्न 8

8. SPF सत्यापन ईमेल बॉडी के क्रिप्टोग्राफ़िक हस्ताक्षर की पुष्टि करके काम करता है।

○ सही ○ गलत

9 प्रश्न 9

9. व्हेलिंग हमले डेटाबेस फ़ाइलों तक पहुँचने के लिए निचले स्तर के कॉर्पोरेट प्रशासकों को निशाना बनाते हैं।

○ सही ○ गलत

10 प्रश्न 10

10. भुगतान अनुरोधों का आउट-ऑफ़-बैंड सत्यापन वित्तीय वायर ट्रांसफ़र स्कैम रोकने में मदद करता है।

○ 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. भोले-भाले लोगों को झूठे वादों से ठगने की कोशिश _____ कहलाती है।
2. चुराए गए पासवर्ड से किसी के खाते में घुसना एक तरह की _____ है।
3. मेल सर्वर संदिग्ध संदेशों को _____ से रोककर आपके इनबॉक्स तक पहुँचने नहीं देता।
4. पासवर्ड को सीधे सहेजने के बजाय _____ से बदलकर रखना चोरी का नुकसान घटाता है।
5. संदिग्ध लिंक और अटैचमेंट की _____ करके मैलवेयर पहले ही पकड़ा जा सकता है।
6. सी-लेवल अधिकारियों को निशाना बनाने वाला फ़िशिंग अभियान _____ कहलाता है।

शब्दावली शब्द-बैंक

फ़िल्टरिंग | व्हेलिंग | स्कैनिंग | स्कैमिंग | हैकिंग | हैशिंग | DKIM | DMARC

अपने उत्तर यहाँ लिखें:

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

चेकपॉइंट 4: सुरक्षा अवधारणा मिलान

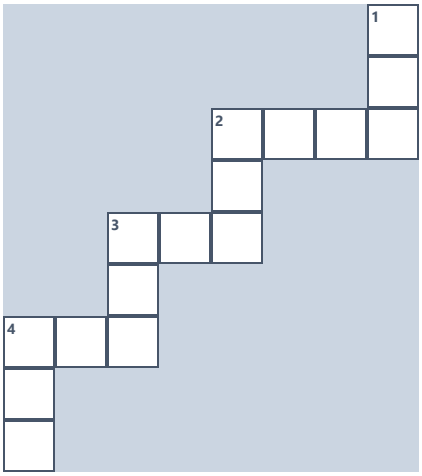
परिभाषा मिलान

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. स्पीयर**	**A**	आवाज़ आधारित स्कैम कॉल।
☐	**2. स्पूफ़िंग**	**B**	C-स्तर के अधिकारियों को निशाना बनाना।
☐	**3. SPF**	**C**	पॉलिसी अस्वीकार निर्देश।
☐	**4. DKIM**	**D**	DNS द्वारा अधिकृत प्रेषक IP।
☐	**5. DMARC**	**E**	सोशल इंजीनियरिंग ईमेल।
☐	**6. व्हेलिंग**	**F**	व्यक्तिगत रूप से लक्षित ईमेल।
☐	**7. फ़िशिंग**	**G**	भेजने वाले का ईमेल पता जाली बनाना।
☐	**8. विशिंग**	**H**	ईमेल में क्रिप्टोग्राफ़िक हस्ताक्षर।

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

2. संदिग्ध संदेशों या ट्रैफ़िक को पहचानकर रोक देने की प्रक्रिया (4)

3. लोगों को झूठे वादों से फँसाकर उनसे पैसे ऐंठने की धोखाधड़ी (3)

4. अनुमति के बिना किसी के खाते या सिस्टम में घुसने की कोशिश (3)

ऊपर से नीचे

1. आवाज़ पर आधारित स्कैम कॉल। (3)

2. सोशल इंजीनियरिंग वाला ईमेल। (3)

3. संदिग्ध लिंक या फ़ाइल में ख़तरे खोजने के लिए की जाने वाली जाँच (3)

4. पासवर्ड को अपठनीय कोड में बदलकर सहेजने की एकतरफ़ा विधि (3)

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

2 बाएँ से दाएँ: संदिग्ध संदेशों या ट्रैफ़िक को पहचानकर रोक देने की प्रक्रिया (4 अक्षर):

3 बाएँ से दाएँ: लोगों को झूठे वादों से फँसाकर उनसे पैसे ऐंठने की धोखाधड़ी (3 अक्षर):

4 बाएँ से दाएँ: अनुमति के बिना किसी के खाते या सिस्टम में घुसने की कोशिश (3 अक्षर):

ऊपर से नीचे

1 ऊपर से नीचे: आवाज़ पर आधारित स्कैम कॉल। (3 अक्षर):

2 ऊपर से नीचे: सोशल इंजीनियरिंग वाला ईमेल। (3 अक्षर):

3 ऊपर से नीचे: संदिग्ध लिंक या फ़ाइल में ख़तरे खोजने के लिए की जाने वाली जाँच (3 अक्षर):

4 ऊपर से नीचे: पासवर्ड को अपठनीय कोड में बदलकर सहेजने की एकतरफ़ा विधि (3 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।

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

शब्दावली शब्द-सूची

व्हेलिंग फ़िशिंग विशिंग स्कैमिंग स्कैनिंग हैकिंग हैशिंग फ़िल्टरिंग

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. व्हेलिंग
B. फ़िशिंग
C. विशिंग
D. स्कैमिंग
E. स्कैनिंग
F. हैकिंग
G. हैशिंग
H. फ़िल्टरिंग

परिभाषाएँ और मिलान फ़ील्ड	
	1. सोशल इंजीनियरिंग वाला ईमेल।
	2. सी-लेवल अधिकारियों को निशाना बनाना।
	3. संदिग्ध संदेशों या ट्रैफ़िक को पहचानकर रोक देने की प्रक्रिया।
	4. आवाज़ पर आधारित स्कैम कॉल।
	5. पासवर्ड को अपठनीय कोड में बदलकर सहेजने की एकतरफ़ा विधि।
	6. संदिग्ध लिंक या फ़ाइल में ख़तरे खोजने के लिए की जाने वाली जाँच।
	7. लोगों को झूठे वादों से फँसाकर उनसे पैसे ऐंठने की धोखाधड़ी।
	8. अनुमति के बिना किसी के खाते या सिस्टम में घुसने की कोशिश।

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. **लिंग व्हे**
2. **ग शिं वि**
3. **ग निं स्कै**
4. **शिं ग है**
5. **ग शिं फ़ि**
6. **मिं ग स्कै**
7. **ग किं है**
8. **फ़ि ग रिं ल्ट**

अतिरिक्त गतिविधि: झटपट सोचें

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

1	ऐसे डिवाइस जिन्हें हैक किया जा सकता है			
2	फ़िशिंग ईमेल के संकेत			
3	कंप्यूटर के संक्रमित होने के संकेत			
4	झूठी जल्दबाज़ी पैदा करने वाले शब्द			
5	प्रेषक की जाँच करने के तरीके			
6	IT मदद के लिए आप जिनसे पूछ सकते हैं			
7	ऐसी चीज़ें जिनका आप बैकअप लेते हैं			
8	आपकी जानी-पहचानी मछलियाँ या समुद्री जीव			
9	ऐसी कंपनियाँ जिनका रूप ठग धारण करते हैं			
10	सुरक्षित आदतें जो आप आज से शुरू कर सकते हैं			
11	नकली लिंक पर क्लिक करने के बाद की जाने वाली चीज़ें			
12	डेटा लीक के बाद की जाने वाली चीज़ें			
13	ऐसे माध्यम जहाँ फ़िशिंग होती है			
14	ऐसी चीज़ें जिन्हें आप ईमेल से कभी नहीं भेजते			
15	अपने अकाउंट सुरक्षित रखने के तरीके			

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: C-सूट व्हेलिंग हमले का समाधान



परिदृश्य: एक चीफ़ फ़ाइनेंशियल ऑफ़िसर को CEO की ओर से होने का दावा करने वाला अत्यंत व्यक्तिगत ईमेल मिलता है, जिसमें गोपनीय डोमेन खरीद पूरी करने के लिए तुरंत $50,000 वायर करने को कहा गया है।

चर्चा प्रश्न: ब्रांड स्पूफ़िंग के जोखिमों का विश्लेषण कीजिए और SPF/DKIM/DMARC तथा ऑथेंटिकेशन नियंत्रणों का विवरण दीजिए।

केस स्टडी 2: SPF/DKIM/DMARC गेटवे नीतियाँ लागू करना



परिदृश्य: एक उद्यम सुरक्षा ऑडिट में विफल हो रहा है क्योंकि आउटबाउंड मार्केटिंग ईमेल अक्सर स्पैम के रूप में चिह्नित हो जाते हैं, और हैकर कंपनी के ब्रांड डोमेन की सक्रिय रूप से स्पूफ़िंग कर रहे हैं।

चर्चा प्रश्न: ईमेल की प्रामाणिकता सत्यापित करने के लिए तकनीकी और प्रशासनिक नियंत्रण स्थापित कीजिए।

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

15	52	23	41	52		12	25	47	23		44	52		44	54	42	40

3	57	20	48	32	47	38	39	47	57	15		33	45	18	46	32	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: फ़िशिंग क्या है?

फ़िशिंग एक सोशल इंजीनियरिंग हमला है जिसमें अपराधी संवेदनशील डेटा साझा कराने के लिए उपयोगकर्ताओं को धोखाधड़ी वाले संदेश भेजते हैं।

Q2: फ़िशिंग और स्पीयर फ़िशिंग में क्या अंतर है?

फ़िशिंग सामान्य सामग्री के साथ व्यापक समूहों को निशाना बनाती है, जबकि स्पीयर फ़िशिंग अनुकूलित जानकारी का उपयोग करके विशिष्ट पीड़ितों को निशाना बनाती है।

Q3: व्हेलिंग क्या है?

व्हेलिंग एक अत्यधिक लक्षित फ़िशिंग हमला है जो प्रशासनिक अधिकार रखने वाले उच्च-स्तरीय कार्यकारियों को निशाना बनाता है।

Q4: ईमेल स्पूफ़िंग क्या है?

ईमेल स्पूफ़िंग में जाली प्रेषक पते वाले ईमेल संदेश बनाए जाते हैं ताकि प्राप्तकर्ता स्रोत पर भरोसा कर ले।

Q5: SPF स्पूफ़िंग को कैसे रोकता है?

यह DNS में अधिकृत भेजने वाले IP पतों की सूची प्रकाशित करता है, जिससे प्राप्तकर्ता सर्वर मेल का स्रोत सत्यापित कर पाते हैं। [1]

चेकपॉइंट 10: बुनियादी साइबर सुरक्षा FAQ (भाग B)

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

Q6: DKIM क्या है?

DomainKeys Identified Mail ईमेल हेडर में क्रिप्टोग्राफ़िक हस्ताक्षर जोड़ता है, जो साबित करता है कि किसी डोमेन ने ज़िम्मेदारी ली और संदेश बदला नहीं गया।

Q7: DMARC का पूरा नाम क्या है?

डोमेन-आधारित संदेश प्रमाणीकरण, रिपोर्टिंग और अनुपालन। [2]

Q8: DMARC नीति क्या है?

नीति जो मेल सर्वरों को बताती है कि SPF/DKIM में विफल संदेशों के साथ कैसा व्यवहार करना है (none, quarantine या reject)। [2]

Q9: विशिंग क्या है?

वॉइस फ़िशिंग, जिसमें हमलावर फ़र्ज़ी फ़ोन कॉल के ज़रिए प्रशासनिक या वित्तीय जानकारी निकलवाते हैं।

Q10: लिंक स्कैनर कैसे मदद करते हैं?

वे आने वाले ईमेल के लिंक स्कैन करके बदल देते हैं, ताकि क्लिक के समय गंतव्य वेब पेज की सुरक्षा जाँची जा सके।

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग C)

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

Q1: होमोग्राफ़ हमला कैसे काम करता है?

हमलावर किसी वैध डोमेन नाम की दृश्य नकल करने के लिए मिलते-जुलते गैर-ASCII Unicode वर्णों से डोमेन नाम पंजीकृत करते हैं।

Q2: प्यूनीकोड प्रतिनिधित्व क्या है?

ऐसी एन्कोडिंग जो Unicode डोमेन नामों को 'xn--' से शुरू होने वाली ASCII-संगत स्ट्रिंग में बदलती है ताकि DNS उन्हें संभाल सके।

Q3: 'p=reject' सबसे सुरक्षित DMARC स्थिति क्यों है?

यह प्राप्तकर्ता सर्वरों से SMTP सत्र के दौरान उस मेल को अस्वीकार करने को कहता है जो DMARC (संरेखित SPF/DKIM) में विफल रहता है, जिससे सीधी स्पूफ़िंग रुकती है। [2]

Q4: हमलावर SPF नियमों को कैसे बायपास करते हैं?

मिलते-जुलते डोमेन (टाइपोस्क्वाटिंग) का फ़ायदा उठाकर या वैध तृतीय-पक्ष मेल सेवाओं पर समझौता किए गए खातों का उपयोग करके।

Q5: बिज़नेस ईमेल कंप्रोमाइज़ (BEC) क्या है?

कॉर्पोरेट घोटाला, जिसमें हमलावर कपटपूर्ण भुगतान अधिकृत करने के लिए बिज़नेस ईमेल खातों को हाईजैक करते हैं या उनकी नकल करते हैं।

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग D)

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

Q6: मल्टी-फ़ैक्टर ऑथेंटिकेशन फ़िशिंग को कैसे रोकता है?

इसमें द्वितीयक टोकन (जैसे हार्डवेयर कुंजियाँ) चाहिए, जिन्हें केवल हमशक्ल लैंडिंग पेज से चुराया नहीं जा सकता।

Q7: क्रेडेंशियल हार्वेस्टिंग लैंडिंग पेज क्या है?

हूबहू दिखने वाला लॉगिन पोर्टल, जिसे दर्ज किए गए यूज़रनेम, पासवर्ड और MFA टोकन को रीयल टाइम में पकड़ने के लिए बनाया जाता है।

Q8: सबडोमेन हाइजैकिंग क्या है?

हमलावर किसी अप्रयुक्त DNS सबडोमेन पॉइंटर पर नियंत्रण पा लेता है ताकि भरोसेमंद पैरेंट डोमेन के तहत दुर्भावनापूर्ण फ़िशिंग लैंडिंग पेज होस्ट कर सके।

Q9: DKIM अलाइनमेंट जाँच कैसे काम करती है?

यह सत्यापित करता है कि 'From' हेडर का डोमेन उसी डोमेन से मेल खाता है जिसने DKIM हेडर में संदेश पर क्रिप्टोग्राफ़िक रूप से हस्ताक्षर किए थे।

Q10: ईमेल गेटवे की भूमिका क्या है?

आने वाले ईमेल को फ़िल्टर करना, लिंक की जाँच करना, अटैचमेंट को सैंडबॉक्स करना और SPF/DKIM/DMARC अनुपालन सत्यापित करना।

भाग 11: 10 वास्तविक साइबर सुरक्षा तथ्य और अंतर्दृष्टियाँ

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

1. सुरक्षा इनसाइट

2025 में FBI के IC3 को सबसे अधिक रिपोर्ट किया गया अपराध प्रकार फ़िशिंग और स्पूफ़िंग था, जिसमें 191,561 शिकायतें थीं। [4]

2. सुरक्षा इनसाइट

2025 में FBI के IC3 को रिपोर्ट किए गए नुकसानों में बिज़नेस ईमेल कॉम्प्रोमाइज़ (BEC) से $3 बिलियन से अधिक का नुकसान हुआ। [4]

3. सुरक्षा इनसाइट

होमोग्राफ़ हमले सिरिलिक के हमशक्ल अक्षरों का उपयोग करके ब्राउज़र में एग्ज़ैक्ट-मैच ब्रांड डोमेन की दृश्य नकल बनाते हैं।

4. सुरक्षा इनसाइट

'p=reject' के साथ, डोमेन प्राप्तकर्ताओं से डिलीवरी के दौरान विफल होने वाले मेल को अस्वीकार करने को कहता है, उसे स्पैम में दर्ज करने को नहीं। [2]

5. सुरक्षा इनसाइट

CEO को निशाना बनाने वाले व्हेलिंग हमले आम तौर पर गोपनीय विलय या डोमेन खरीद के लिए तत्काल भुगतान माँगते हैं।

6. सुरक्षा इनसाइट

क्रेडेंशियल हार्वेस्टिंग पोर्टल असली लॉगिन पेजों की नकल करते हैं ताकि पीड़ित अपने पासवर्ड सीधे हमलावर के फ़ॉर्म में टाइप कर दें।

7. सिक्योरिटी इनसाइट

CISA का संयुक्त फ़िशिंग मार्गदर्शन DMARC, SPF, DKIM और फ़िशिंग-प्रतिरोधी MFA के साथ उपयोगकर्ता प्रशिक्षण की सिफ़ारिश करता है। [3]

8. सिक्योरिटी इनसाइट

SPF मूल्यांकन 10 DNS-केरी वाले पदों तक सीमित है; सीमा पार होने पर 'permerror' नतीजा मिलता है। [1]

9. सिक्योरिटी इनसाइट

FIDO2 हार्डवेयर सुरक्षा कुंजियाँ दूरस्थ क्रेडेंशियल चोरी के विरुद्ध क्रिप्टोग्राफ़िक रूप से समर्थित सुरक्षा देती हैं।

10. सुरक्षा इनसाइट

फ़िशिंग हमलावरों के किसी संगठन में पहली बार घुसने के सबसे आम तरीकों में से एक है, इसीलिए नियमित जागरूकता प्रशिक्षण एक प्रभावी बचाव 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] IETF. (2014). RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1.

https://www.rfc-editor.org/rfc/rfc7208.html

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

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

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

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

[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

स्पीयर फ़िशिंग क्या है? → किसी विशेष व्यक्ति या संगठन के अनुसार तैयार किया गया लक्षित फ़िशिंग ईमेल

2 प्रश्न 2 सही उत्तर: A

शिक्षण नोट

SPF किसी डोमेन के अधिकृत भेजने वाले होस्ट DNS में प्रकाशित करता है ताकि प्राप्तकर्ता envelope sender की जाँच कर सकें।

3 प्रश्न 3 सही उत्तर: A

शिक्षण नोट

व्हेलिंग हमला क्या है? → फ़िशिंग अभियान जो विशेष रूप से उच्च-प्रोफ़ाइल कॉर्पोरेट अधिकारियों को निशाना बनाता है

4 प्रश्न 4 सही उत्तर: A

शिक्षण नोट

DKIM क्या करता है? → प्रेषक की प्रामाणिकता सत्यापित करने के लिए ईमेल में क्रिप्टोग्राफ़िक हस्ताक्षर जोड़ता है

5 प्रश्न 5 सही उत्तर: A

शिक्षण नोट

DMARC की भूमिका क्या है? → प्राप्त करने वाले ईमेल सर्वरों को निर्देश देना कि विफल SPF/DKIM जाँच को कैसे संभालें

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 **प्रश्न 6** — सही उत्तर: गलत

शिक्षण नोट

गलत: स्पियर फ़िशिंग विशिष्ट लोगों के अनुरूप बनाई जाती है, सामान्य बल्क फ़िशिंग के विपरीत।

7 **प्रश्न 7** — सही उत्तर: सही

शिक्षण नोट

DMARC नीतियाँ मेल सर्वरों को अनधिकृत स्पूफ़ किए गए संदेशों को अस्वीकार करने का निर्देश दे सकती हैं।

8 **प्रश्न 8** — सही उत्तर: गलत

शिक्षण नोट

गलत: SPF भेजने वाले IP को DNS से मिलाकर जाँचता है; क्रिप्टोग्राफ़िक सिग्नेचर DKIM सत्यापित करता है।

9 **प्रश्न 9** — सही उत्तर: गलत

शिक्षण नोट

गलत: व्हेलिंग वरिष्ठ अधिकारियों को निशाना बनाती है, जो भुगतान मंज़ूर कर सकते हैं और संवेदनशील डेटा तक पहुँच सकते हैं।

10 **प्रश्न 10** — सही उत्तर: सही

शिक्षण नोट

सही: भुगतान अनुरोधों की पुष्टि किसी अलग, जाने-माने चैनल से करने से वायर फ़्रॉड रोकने में मदद मिलती है।

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

F 1. स्पीयर	G 2. स्पूफ़िंग	D 3. SPF	H 4. DKIM
C 5. DMARC	B 6. व्हेलिंग	E 7. फ़िशिंग	A 8. विशिंग

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 स्कैमिंग	2 हैकिंग	3 फ़िल्टरिंग	4 हैशिंग
5 स्कैनिंग	6 व्हेलिंग		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

1 B – फ़िशिंग	2 A – व्हेलिंग	3 H – फ़िल्टरिंग	4 C – विशिंग
5 G – हैशिंग	6 E – स्कैनिंग	7 D – स्कैमिंग	8 F – हैकिंग

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी स्पीयर, स्पूफ़िंग और SPF 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।

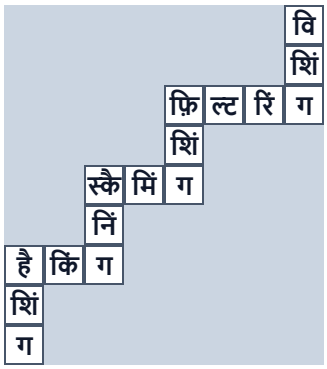
स्रोतों का मूल्यांकन:
विद्यार्थियों से वर्कशीट के स्रोतों में कम से कम एक कथन की पुष्टि करवाएँ और चर्चा करें कि आँकड़े, कीमतें और नियम समय के साथ क्यों बदल सकते हैं।

पहेलियों की कुंजियाँ और शिक्षक नोट

शब्द खोज समाधान

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

क्रॉसवर्ड समाधान



क्रॉसवर्ड समाधान के लिए शिक्षक गाइड

बाएँ से दाएँ

2 बाएँ से दाएँ: फ़िल्टरिंग संदिग्ध संदेशों या ट्रैफ़िक को पहचानकर रोक देने की प्रक्रिया (4 अक्षर)

3 बाएँ से दाएँ: स्कैमिंग लोगों को झूठे वादों से फँसाकर उनसे पैसे ऐंठने की धोखाधड़ी (3 अक्षर)

4 बाएँ से दाएँ: हैकिंग अनुमति के बिना किसी के खाते या सिस्टम में घुसने की कोशिश (3 अक्षर)

ऊपर से नीचे

1 ऊपर से नीचे: विशिंग आवाज़ पर आधारित स्कैम कॉल। (3 अक्षर)

2 ऊपर से नीचे: फ़िशिंग सोशल इंजीनियरिंग वाला ईमेल। (3 अक्षर)

3 ऊपर से नीचे: स्कैनिंग संदिग्ध लिंक या फ़ाइल में ख़तरे खोजने के लिए की जाने वाली जाँच (3 अक्षर)

4 ऊपर से नीचे: हैशिंग पासवर्ड को अपठनीय कोड में बदलकर सहेजने की एकतरफ़ा विधि (3 अक्षर)

अक्षर-फेर शब्द और कूट संदेश हल कुंजी

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

शब्द अनस्क्रैम्बल कुंजी

1. लिंग व्हे → **व्हेलिंग**
2. गशिंवि → **विशिंग**
3. गनिंस्कै → **स्कैनिंग**
4. शिंगहै → **हैशिंग**
5. गशिंफ़ि → **फ़िशिंग**
6. मिंगस्कै → **स्कैमिंग**
7. गकिंहै → **हैकिंग**
8. फ़िगरिंल्ट → **फ़िल्टरिंग**

गुप्त कूट चुनौती कुंजी

"गेटवे ऑडिट से सोशल इंजीनियरिंग पहचानें"

केस स्टडी के उत्तर

A केस स्टडी 1: C-सूट व्हेलिंग हमले का समाधान

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक चीफ़ फ़ाइनेंशियल ऑफ़िसर को CEO की ओर से आया दिखता एक बेहद व्यक्तिगत ईमेल मिलता है, जिसमें एक गोपनीय डोमेन खरीद पूरी करने के लिए तुरंत $50,000 वायर करने को कहा गया है।
- अनुशंसित रणनीति और समाधान: स्पूफ़ किए गए सेंडर डोमेन ब्लॉक करने के लिए DMARC को 'p=reject' नीति के साथ कॉन्फ़िगर करें। गेटवे पर बाहरी प्रेषक की चेतावनी वाले बैनर जोड़ें, और सभी वित्तीय लेन-देन के लिए मौखिक, आउट-ऑफ़-बैंड पुष्टि अनिवार्य करें।

B केस स्टडी 2: SPF/DKIM/DMARC गेटवे नीतियाँ लागू करना

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक एंटरप्राइज़ सुरक्षा ऑडिट में विफल हो रहा है, क्योंकि उसके आउटबाउंड मार्केटिंग ईमेल अक्सर स्पैम के रूप में चिह्नित हो जाते हैं और हैकर कंपनी के ब्रांड डोमेन की सक्रिय रूप से स्पूफ़िंग कर रहे हैं।
- अनुशंसित रणनीति और समाधान: अधिकृत भेजने वाले IP बताते हुए SPF के लिए TXT रिकॉर्ड प्रकाशित करें। आउटबाउंड मेल सर्वर पर DKIM साइनिंग कुंजियाँ कॉन्फ़िगर करें, और दुरुपयोग पहचानने के लिए आने वाली DMARC XML फ़ीडबैक रिपोर्ट का विश्लेषण करें।