नाम: _____ दिनांक: _____ अंक: _____

ऑनलाइन घोटाले और सोशल इंजीनियरिंग सुरक्षा गाइड

ईमेल फ़िशिंग, स्पूफ़ किए गए डोमेन, विशिंग, सपोर्ट घोटाले, आउट-ऑफ़-बैंड सत्यापन, BEC

ऑनलाइन घोटाले 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 ऑनलाइन स्कैम से बचाव से परिचित कराता है। आप नकली फ़िशिंग वेबसाइट, सोशल इंजीनियरिंग रणनीतियाँ, सपोर्ट स्कैम, वायर फ़्रॉड वेक्टर और भुगतान सत्यापन तरीकों 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/online-dhokhebazi/

आपका ऑनलाइन स्कैम सुरक्षा लर्निंग रोडमैप

- सपोर्ट स्कैम और टाइपोस्क्वैटिंग डोमेन के आम संकेतों की पहचान करें।
- स्पूफ़िंग के विरुद्ध ईमेल सत्यापन प्रोटोकॉल (SPF, DKIM, DMARC) लागू करें।
- बिज़नेस वायर धोखाधड़ी रोकने के लिए आउट-ऑफ़-बैंड लेनदेन सत्यापन स्थापित करें।

ऑनलाइन घोटाले 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 ऑनलाइन स्कैम सुरक्षा पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

ऑनलाइन घोटाले और सोशल इंजीनियरिंग से सुरक्षा (परिचय)

ऑनलाइन घोटाले फ़िशिंग, सपोर्ट पॉप-अप, विशिंग और वायर फ़्रॉड के ज़रिए मानव व्यवहार का फ़ायदा उठाते हैं। आउट-ऑफ़-बैंड लेन-देन सत्यापन और SPF/DKIM/DMARC डोमेन नियम लागू करने से गेटवे पर सोशल इंजीनियरिंग के रास्ते रोकने में मदद मिलती है।

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

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1. 1. सपोर्ट स्कैम का प्रमुख संकेतक क्या है?
   - A. पॉप-अप जो दावा करता है कि आपका सिस्टम संक्रमित है और आपसे फ़ोन नंबर पर कॉल करने को कहता है
   - B. आधिकारिक रजिस्ट्री से डाउनलोड किया गया स्वचालित सुरक्षा अपडेट
   - C. पासवर्ड मैनेजर का कॉर्पोरेट डोमेन पर क्रेडेंशियल भरने से इनकार करना
   - D. बाहरी ड्राइव कॉन्फ़िगरेशन पर चलने वाला बैकग्राउंड फ़ाइल बैकअप

2. 2. कौन-सी तकनीक बैंक विवरण चुराने के लिए फ़र्ज़ी प्रेषक डोमेन का उपयोग करती है?
   - A. ईमेल फ़िशिंग
   - B. पोर्ट स्कैनिंग
   - C. मेमोरी इंजेक्शन
   - D. क्रिप्टोग्राफ़िक श्रेडिंग

3. 3. वायर ट्रांसफ़र धोखाधड़ी क्या दर्शाती है?
   - A. सोशल इंजीनियरिंग से पीड़ितों को नकली कॉर्पोरेट खातों में पैसे भेजने के लिए बहकाना
   - B. रैनसमवेयर पेलोड से सिस्टम डेटाबेस को एन्क्रिप्ट करना
   - C. SQL इंजेक्शन कमांड से डेटाबेस क्वेरी करना
   - D. सिस्टम फ़ाइलों का बैकअप ऑफ़लाइन स्टोरेज डिस्क पर लेना

4. 4. ठग फ़र्ज़ी शॉपिंग वेबसाइट क्यों बनाते हैं?
   - A. खरीदारों के क्रेडिट कार्ड विवरण और भुगतान क्रेडेंशियल चुराना
   - B. सैंडबॉक्स वाले मैलवेयर विश्लेषण डेटाबेस तालिकाएँ होस्ट करना
   - C. ऑनलाइन ऑर्डर की डिलीवरी तेज़ करने के लिए
   - D. नए वेबसाइट डिज़ाइन मुफ़्त में परखने के लिए

5. 5. विशिंग का क्या अर्थ है?
   - A. क्रेडेंशियल चुराने के लिए फ़ोन नेटवर्क पर वॉइस फ़िशिंग घोटाले
   - B. असुरक्षित सिस्टम डिवाइस के लिए स्थानीय नेटवर्क स्कैन करना
   - C. अनधिकृत उल्लंघन के बाद सिस्टम डेटाबेस बहाल करना
   - D. अविश्वसनीय कोड को सुरक्षित वर्चुअल कंटेनर के अंदर चलाना

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न 6

6. फ़िशिंग घोटाले केवल अंतिम उपयोगकर्ताओं को निशाना बनाते हैं, कभी भी कार्यकारी व्हेलिंग लक्ष्यों को नहीं।

○ सही ○ गलत

7 प्रश्न 7

7. नकली डोमेन अक्सर भरोसेमंद ब्रांड की नकल करने के लिए मामूली टाइपो (जैसे amaz0n.com) का उपयोग करते हैं।

○ सही ○ गलत

8 प्रश्न 8

8. सपोर्ट घोटालों को कॉल करने वाले को रिमोट एक्सेस देकर सुलझाया जा सकता है।

○ सही ○ गलत

9 प्रश्न 9

9. सोशल इंजीनियरिंग डर और जल्दबाज़ी जैसे मानवीय मनोविज्ञान का फ़ायदा उठाकर सुरक्षा नियमों को बायपास करती है।

○ सही ○ गलत

10 प्रश्न 10

10. वायर ट्रांसफ़र अनुरोधों की पुष्टि हमेशा आउट-ऑफ़-बैंड संचार माध्यमों से की जानी चाहिए।

○ 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. उपयोगकर्ताओं को बहकाने वाले धोखाधड़ी के ईमेल _____ कहलाते हैं।
2. ईमेल भेजने वाले का नकली पता दिखाने की चाल _____ कहलाती है।
3. बैंक विवरण को निशाना बनाने वाले वॉइस स्कैम _____ कहलाते हैं।
4. लोगों को लालच देकर पैसे ऐंठने की धोखाधड़ी भरी हरकत _____ कहलाती है।
5. ईमेल सेवा संदिग्ध संदेशों को _____ ज़रिए स्पैम फ़ोल्डर में भेज देती है।
6. बैंक खाते में बिना अनुमति घुसने की कोशिश _____ कहलाती है।

शब्दावली शब्द-बैंक

फ़िल्टरिंग | फ़िशिंग | विशिंग | स्कैनिंग | स्कैमिंग | स्पूफ़िंग | हैकिंग | हैशिंग

अपने उत्तर यहाँ लिखें:

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

चेकपॉइंट 4: सुरक्षा अवधारणा मिलान

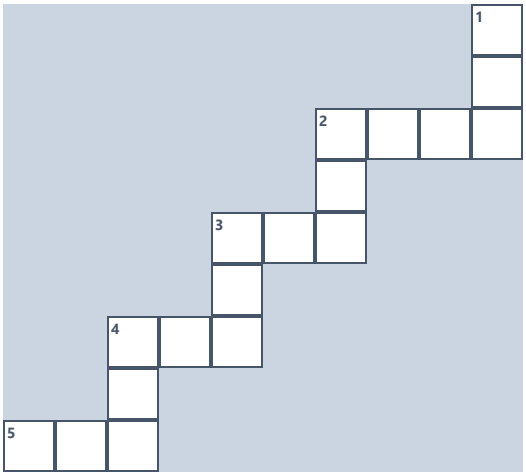
परिभाषा मिलान

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. फ़िशिंग**	**A**	बैंक लेन-देन को धोखे से आपराधिक खातों में भेजना।
☐	**2. स्पूफ़ किया गया**	**B**	पीड़ितों से पैसे या क्रेडेंशियल एक्सेस चुराने के लिए बनाई गई धोखाधड़ी की योजना।
☐	**3. विशिंग**	**C**	मोबाइल खाते के क्रेडेंशियल चुराने के लिए स्कैम टेक्स्ट संदेश भेजना।
☐	**4. घोटाला**	**D**	क्रेडेंशियल और खाते का विवरण चुराने के लिए बनाई गई धोखाधड़ी वाली वॉइस कॉल।
☐	**5. सत्यापन**	**E**	C-स्तर के अधिकारियों से क्रेडेंशियल चुराने के उद्देश्य से किए गए लक्षित फ़िशिंग हमले।
☐	**6. वायर ट्रांसफ़र**	**F**	वैध दिखने के लिए बनाया गया, नकल किया हुआ ईमेल प्रेषक या वेबसाइट पता।
☐	**7. व्हेलिंग**	**G**	लॉगिन क्रेडेंशियल और पासवर्ड चुराने के लिए बनाए गए धोखाधड़ी वाले ईमेल अभियान।
☐	**8. स्मिशिंग**	**H**	किसी विश्वसनीय दूसरे संपर्क माध्यम से भुगतान विवरण की पुष्टि करना।

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)

5. किसी भरोसेमंद व्यक्ति या संस्था का नकली पता दिखाकर धोखा देना (3)

ऊपर से नीचे

1. क्रेडेंशियल और खाते का ब्योरा चुराने के लिए बनाई गई धोखाधड़ी वाली वॉइस कॉल। (3)

2. लॉगिन क्रेडेंशियल और पासवर्ड चुराने के लिए बनाए गए धोखाधड़ी वाले ईमेल अभियान। (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):

5 बाएँ से दाएँ: किसी भरोसेमंद व्यक्ति या संस्था का नकली पता दिखाकर धोखा देना (3 अक्षर):

ऊपर से नीचे

1 ऊपर से नीचे: क्रेडेंशियल और खाते का ब्योरा चुराने के लिए बनाई गई धोखाधड़ी वाली वॉइस कॉल। (3 अक्षर):

2 ऊपर से नीचे: लॉगिन क्रेडेंशियल और पासवर्ड चुराने के लिए बनाए गए धोखाधड़ी वाले ईमेल अभियान। (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।

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

शब्दावली शब्द-सूची

फ़िशिंग · विशिंग · स्कैमिंग · स्कैनिंग · हैकिंग · हैशिंग · स्पूफ़िंग · 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. फ़िशिंग**
- **B. विशिंग**
- **C. स्कैमिंग**
- **D. स्कैनिंग**
- **E. हैकिंग**
- **F. हैशिंग**
- **G. स्पूफ़िंग**
- **H. फ़िल्टरिंग**

परिभाषाएँ और मिलान फ़ील्ड

1. क्रेडेंशियल और खाते का ब्योरा चुराने के लिए बनाई गई धोखाधड़ी वाली वॉइस कॉल।
2. अनुमति के बिना किसी के खाते या सिस्टम में घुसने की कोशिश।
3. पासवर्ड को अपठनीय कोड में बदलकर सहेजने की एकतरफ़ा विधि।
4. संदिग्ध संदेशों या ट्रैफ़िक को पहचानकर रोक देने की प्रक्रिया।
5. किसी भरोसेमंद व्यक्ति या संस्था का नकली पता दिखाकर धोखा देना।
6. लोगों को झूठे वादों से फँसाकर उनसे पैसे ऐंठने की धोखाधड़ी।
7. लॉगिन क्रेडेंशियल और पासवर्ड चुराने के लिए बनाए गए धोखाधड़ी वाले ईमेल अभियान।
8. संदिग्ध लिंक या फ़ाइल में ख़तरे खोजने के लिए की जाने वाली जाँच।

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. **शिं ग फ़ि** _____
2. **ग मिं स्कै** _____
3. **ग किं है** _____
4. **फ़िं ग स्पू** _____
5. **ग शिं वि** _____
6. **निं ग स्कै** _____
7. **ग शिं 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	वे वाक्यांश जो ठग अक्सर इस्तेमाल करते हैं			
3	भुगतान के वे तरीके जिन्हें ठग माँगते हैं			
4	ऑनलाइन स्कैम के प्रकार			
5	ऐसे ऑफ़र जो सच होने के लिए बहुत अच्छे हैं			
6	स्कैम की रिपोर्ट करने की जगहें			
7	साइबर सुरक्षा से जुड़े शब्द			
8	ऐसे लोग जिन्हें आप स्कैम के बारे में चेता सकते हैं			
9	ऐसी चीज़ें जिनका आप बैकअप लेते हैं			
10	ईमेल में चेतावनी के संकेत			
11	कंप्यूटर के संक्रमित होने के संकेत			
12	ऑनलाइन दुकान की जाँच करने के तरीके			
13	अपने अकाउंट सुरक्षित रखने के तरीके			
14	स्कैम का शिकार होने पर की जाने वाली चीज़ें			
15	डेटा लीक के बाद की जाने वाली चीज़ें			

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: कॉर्पोरेट वायर ट्रांसफ़र घोटाले की रोकथाम



परिदृश्य: एक वित्त विभाग को नकली वेंडर पते से एक तत्काल ईमेल मिलता है, जिसमें माँग की गई है कि भविष्य के इनवॉइस वायर नए रूटिंग नंबर पर भेजे जाएँ।

चर्चा प्रश्न: वायर फ़्रॉड सत्यापन नीति की रूपरेखा बताइए और ईमेल ऑथेंटिकेशन ब्लॉक निर्दिष्ट कीजिए।

केस स्टडी 2: कार्यकारी व्हेलिंग फ़िशिंग घटना



परिदृश्य: एक कार्यकारी अधिकारी ने सुरक्षित बोर्ड-मीटिंग दस्तावेज़ होने का दावा करने वाले फ़िशिंग लिंक पर क्लिक किया और एक नकली पोर्टल पर अपने प्राथमिक कॉर्पोरेट क्रेडेंशियल डाल दिए।

चर्चा प्रश्न: घटना-प्रतिक्रिया के चरणों का विवरण दीजिए और समझाइए कि कार्यकारी अधिकारी के लॉगिन का ऑडिट कैसे किया जाए।

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

44	61	13	53	32	39		44	28	61	38	46	33	32		44	52

34	60	47	42	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: ऑनलाइन घोटाला क्या है?

डिजिटल माध्यमों का उपयोग करके पीड़ितों को पैसे भेजने या व्यक्तिगत क्रेडेंशियल देने के लिए बहकाने वाली धोखाधड़ी की योजना।

Q2: ईमेल फ़िशिंग का मुख्य संकेतक क्या है?

ऐसा संदेश जो तात्कालिकता जताता है (जैसे खाता निलंबन) और आपको ऐसे लिंक पर भेजता है जो आधिकारिक डोमेन से मेल नहीं खाता।

Q3: टाइपोस्क्वैटिंग क्या है?

फ़र्ज़ी फ़िशिंग साइट होस्ट करने के लिए लोकप्रिय ब्रांडों की आम टाइपिंग गलतियों वाले डोमेन (जैसे amaz0n.com) रजिस्टर करना।

Q4: सपोर्ट स्कैम क्या है?

पॉप-अप जो दावा करता है कि आपका PC संक्रमित है और आपको नंबर पर कॉल करने तथा नकली सफ़ाई सॉफ़्टवेयर या रिमोट एक्सेस सेवाओं के लिए भुगतान करने को कहता है। [1]

Q5: विशिंग क्या है?

फ़िशिंग हमले जिनमें वॉइस फ़ोन कॉल के ज़रिए पीड़ितों को बैंक खाते या लॉगिन की जानकारी देने के लिए बहकाया जाता है।

चेकपॉइंट 10: बुनियादी साइबर सुरक्षा FAQ (भाग B)

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

Q6: वायर फ़्रॉड का क्या अर्थ है?

विक्रेताओं या एग्ज़ीक्यूटिव का रूप धरकर भुगतान लेन-देन को घोटाले वाले अकाउंट की ओर मोड़ना।

Q7: व्हेलिंग क्या है?

स्पीयर फ़िशिंग का अत्यधिक लक्षित रूप, जिसका निशाना सीधे C-लेवल कॉर्पोरेट अधिकारियों जैसे उच्च-मूल्य वाले लक्ष्य होते हैं।

Q8: स्मिशिंग क्या है?

मोबाइल डिवाइस पर भेजे जाने वाले घोटाले वाले टेक्स्ट संदेश, जिनमें फ़र्ज़ी पोर्टल या ट्रैकिंग अपडेट के लिंक होते हैं।

Q9: आउट-ऑफ़-बैंड सत्यापन महत्वपूर्ण क्यों है?

यह अलग संचार माध्यम (जैसे फ़ोन कॉल) से लेन-देन का विवरण पक्का करता है, जिससे समझौता किए गए ईमेल थ्रेड से बचाव होता है।

Q10: नकली एस्क्रो घोटाला कैसे काम करता है?

धोखेबाज़ फ़र्ज़ी एस्क्रो साइट बनाते हैं, दावा करते हैं कि राशि सुरक्षित रखी है, और फिर खरीदार की वायर की गई जमा राशि चुरा लेते हैं।

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग C)

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

Q1: ठग वायर फ़्रॉड को अंजाम देने के लिए BEC (Business Email Compromise) का उपयोग कैसे करते हैं?

वे किसी वैध कर्मचारी का ईमेल खाता हाईजैक करते हैं, इनवॉइस थ्रेड पर नज़र रखते हैं, और घोटाले वाले बैंक खातों के साथ अद्यतन बिलिंग विवरण भेज देते हैं।

Q2: ऑनलाइन घोटालों में IDN होमोग्राफ़ हमलों का क्या जोखिम है?

असली अक्षरों जैसे दिखने वाले गैर-ASCII वर्णों (जैसे सिरिलिक 'а') का उपयोग करके असली ब्रांडों की नकल करने वाले फ़र्ज़ी डोमेन पंजीकृत करना।

Q3: स्कैम की पहचान में ईमेल हेडर की जाँच क्यों महत्वपूर्ण है?

यह असली ओरिजिन सर्वर IP और SPF/DKIM सत्यापन स्थिति उजागर करता है, जिससे पता चलता है कि भेजने वाला डोमेन जाली है या नहीं।

Q4: सपोर्ट स्कैमर रिमोट डेस्कटॉप सॉफ़्टवेयर का दुरुपयोग कैसे करते हैं?

वे पीड़ित के डिवाइस से जुड़ने, मैलवेयर डालने और सहेजे गए पासवर्ड चुराने के लिए AnyDesk या TeamViewer जैसी यूटिलिटी का उपयोग करते हैं।

Q5: एडवांस-फ़ी स्कैम का लक्ष्य क्या होता है?

पीड़ितों को एक बड़े वित्तीय इनाम के बदले पहले ही प्रोसेसिंग शुल्क देने के लिए धोखा देना, जबकि ऐसा कोई इनाम होता ही नहीं।

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग D)

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

Q6: स्कैमर लक्षित फ़िशिंग के लिए सोशल मीडिया प्रोफ़ाइलिंग का उपयोग कैसे करते हैं?

वे कॉर्पोरेट संगठनात्मक ढाँचे और कर्मचारियों के नाम इकट्ठा करके विश्वसनीय स्पीयर-फ़िशिंग ईमेल तैयार करते हैं।

Q7: नकली वेब शॉप भारी छूट क्यों देते हैं?

खरीदारों को क्रेडिट कार्ड विवरण दर्ज करने के लिए फुसलाने और क्रेडेंशियल पकड़कर कार्डिंग फ़ोरम पर दोबारा उपयोग या बिक्री के लिए रखने के लिए।

Q8: DMARC रिकॉर्ड फ़िशिंग स्कैम को कैसे ब्लॉक करते हैं?

DMARC डोमेन मालिकों को यह कहने देता है कि जो मेल संरेखित SPF और DKIM जाँच में विफल हो, उसे प्राप्तकर्ता क्वारंटीन करें या अस्वीकार करें, जिससे सीधी स्पूफ़िंग रुकती है। [5]

Q9: क्रेडेंशियल हार्वेस्टिंग पोर्टल का खतरा क्या है?

नकली लैंडिंग पेज, जो Microsoft 365 या Google वर्कस्पेस जैसे ही दिखते हैं और लॉगिन क्रेडेंशियल दर्ज होते ही चुरा लेते हैं।

Q10: सुरक्षा टीमें घोटाले वाले डोमेन की रिपोर्ट कैसे करती हैं और उन्हें कैसे बंद कराती हैं?

रजिस्ट्रार के दुरुपयोग ईमेल, होस्टिंग प्रदाता और Google Safe Browsing रजिस्ट्री को धोखाधड़ी के प्रमाण जमा करके।

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। [2]

2. सुरक्षा इनसाइट

2025 में FBI के IC3 को रिपोर्ट किए गए नुकसानों में Business Email Compromise (BEC) से $3 बिलियन से अधिक का नुकसान हुआ। [2]

3. सुरक्षा इनसाइट

टाइपो-स्क्वैट किए गए डोमेन असली ब्रांड नामों से एक-दो अक्षर के अंतर पर होते हैं, इसलिए सरसरी नज़र में छूट सकते हैं।

4. सुरक्षा इनसाइट

टेक सपोर्ट घोटालों से 2025 में FBI के IC3 को रिपोर्ट किए गए नुकसान 2.1 अरब डॉलर से अधिक रहे। [2]

5. सुरक्षा इनसाइट

होमोग्राफ़ हमले ब्राउज़र के एड्रेस बार में एक जैसे दिखते हैं, जब तक ब्राउज़र punycode रूप न दिखाए।

6. सुरक्षा इनसाइट

SMS टेक्स्ट घोटाले (स्मिशिंग) लिंक वाले छोटे, तात्कालिक संदेशों का उपयोग करते हैं, जिससे पीड़ितों को धोखाधड़ी भाँपने के लिए बहुत कम संदर्भ मिलता है।

7. सिक्योरिटी इनसाइट

व्हेलिंग हमले कार्यकारी अधिकारियों के ईमेल को निशाना बनाते हैं क्योंकि उनके पास बड़े भुगतान वायर ट्रांसफ़र की पहुँच होती है।

8. सिक्योरिटी इनसाइट

ज्ञात, सहेजे हुए फ़ोन नंबर पर कॉल करके भुगतान में बदलाव की पुष्टि करना BEC वायर धोखाधड़ी के विरुद्ध एक प्रमुख बचाव है।

9. सिक्योरिटी इनसाइट

नकली एस्क्रो खाता वेबसाइटें ऑनलाइन मार्केटप्लेस में आम घोटाला हैं: वे सुरक्षित भुगतान सेवा जैसी दिखती हैं, लेकिन खरीदार का वायर ट्रांसफ़र चुरा लेती हैं।

10. सुरक्षा इनसाइट

Google Safe Browsing उपयोगकर्ताओं को उन साइटों को खोलने से पहले चेतावनी देता है जिन्हें उसने फ़िशिंग या मैलवेयर के लिए चिह्नित किया 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] 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

उत्तर कुंजी: चेकपॉइंट 1 – बहुविकल्पीय

1 प्रश्न 1 सही उत्तर: A

शिक्षण नोट

सपोर्ट स्कैम का प्रमुख संकेतक क्या है? → पॉप-अप जो दावा करता है कि आपका सिस्टम संक्रमित है और आपसे फ़ोन नंबर पर कॉल करने को कहता है

2 प्रश्न 2 सही उत्तर: A

शिक्षण नोट

कौन-सी तकनीक बैंक विवरण चुराने के लिए फ़र्ज़ी प्रेषक डोमेन का उपयोग करती है? → ईमेल फ़िशिंग

3 प्रश्न 3 सही उत्तर: A

शिक्षण नोट

वायर ट्रांसफ़र धोखाधड़ी क्या दर्शाती है? → सोशल इंजीनियरिंग से पीड़ितों को नकली कॉर्पोरेट खातों में पैसे भेजने के लिए बहकाना

4 प्रश्न 4 सही उत्तर: A

शिक्षण नोट

ठग फ़र्ज़ी शॉपिंग वेबसाइट क्यों बनाते हैं? → खरीदारों के क्रेडिट कार्ड विवरण और भुगतान क्रेडेंशियल चुराना

5 प्रश्न 5 सही उत्तर: A

शिक्षण नोट

विशिंग का क्या अर्थ है? → क्रेडेंशियल चुराने के लिए फ़ोन नेटवर्क पर वॉइस फ़िशिंग घोटाले

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 प्रश्न 6 — सही उत्तर: गलत

शिक्षण नोट

गलत: फ़िशिंग कार्यकारी अधिकारियों को भी निशाना बनाती है; व्हेलिंग वरिष्ठ नेताओं पर लक्षित फ़िशिंग है।

7 प्रश्न 7 — सही उत्तर: सही

शिक्षण नोट

नकली डोमेन अक्सर भरोसेमंद ब्रांड की नकल करने के लिए मामूली टाइपो (जैसे amaz0n.com) का उपयोग करते हैं।

8 प्रश्न 8 — सही उत्तर: गलत

शिक्षण नोट

गलत: सपोर्ट स्कैमर को रिमोट एक्सेस देने से वह मैलवेयर लगा सकता है और डेटा चुरा सकता है।

9 प्रश्न 9 — सही उत्तर: सही

शिक्षण नोट

सोशल इंजीनियरिंग डर और जल्दबाज़ी जैसे मानवीय मनोविज्ञान का फ़ायदा उठाकर सुरक्षा नियमों को बायपास करती है।

10 प्रश्न 10 — सही उत्तर: सही

शिक्षण नोट

वायर ट्रांसफ़र अनुरोधों की पुष्टि हमेशा आउट-ऑफ़-बैंड संचार माध्यमों से की जानी चाहिए।

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

G 1. फ़िशिंग	F 2. स्पूफ़ किया गया	D 3. विशिंग	B 4. घोटाला
H 5. सत्यापन	A 6. वायर ट्रांसफ़र	E 7. व्हेलिंग	C 8. स्मिशिंग

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 फ़िशिंग	2 स्पूफ़िंग	3 विशिंग	4 स्कैमिंग
5 फ़िल्टरिंग	6 हैकिंग		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

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

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी फ़िशिंग, स्पूफ़ किया गया और विशिंग 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।

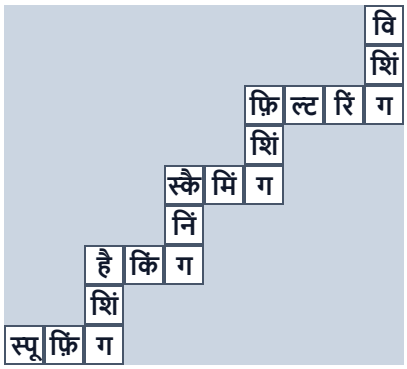
स्रोतों का मूल्यांकन:
विद्यार्थियों से वर्कशीट के स्रोतों में कम से कम एक कथन की पुष्टि करवाएँ और चर्चा करें कि आँकड़े, कीमतें और नियम समय के साथ क्यों बदल सकते हैं।

पहेलियों की कुंजियाँ और शिक्षक नोट

शब्द खोज समाधान

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

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)

5 बाएँ से दाएँ: स्पूफ़िंग किसी भरोसेमंद व्यक्ति या संस्था का नकली पता दिखाकर धोखा देना (3 अक्षर)

ऊपर से नीचे

1 ऊपर से नीचे: विशिंग क्रेडेंशियल और खाते का ब्योरा चुराने के लिए बनाई गई धोखाधड़ी वाली वॉइस कॉल। (3 अक्षर)

2 ऊपर से नीचे: फ़िशिंग लॉगिन क्रेडेंशियल और पासवर्ड चुराने के लिए बनाए गए धोखाधड़ी वाले ईमेल अभियान। (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. शिं ग फ़ि — **फ़िशिंग**
2. ग मिं स्कै — **स्कैमिंग**
3. ग किं है — **हैकिंग**
4. फ़िं ग स्पू — **स्पूफ़िंग**
5. ग शिं वि — **विशिंग**
6. निं ग स्कै — **स्कैनिंग**
7. ग शिं है — **हैशिंग**
8. फ़ि ग रिं ल्ट — **फ़िल्टरिंग**

गुप्त कूट चुनौती कुंजी

"स्कैनर सत्यापन से फ़िशिंग पहचानें"

केस स्टडी के उत्तर

A केस स्टडी 1: कॉर्पोरेट वायर ट्रांसफ़र घोटाले की रोकथाम

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक वित्त विभाग को स्पूफ़ किए गए विक्रेता पते से एक तात्कालिक ईमेल मिलता है, जिसमें आगे के इनवॉइस वायर नए राउटिंग नंबर पर भेजने को कहा गया है।
- अनुशंसित रणनीति और समाधान: सभी भुगतानों के लिए दोहरी अनुमति की नीति लागू करें। पहले से सहेजे गए फ़ोन नंबर से आउट-ऑफ़-बैंड सत्यापन करें, और गेटवे पर स्पूफ़ किए गए डोमेन वाले ईमेल ब्लॉक करें।

B केस स्टडी 2: कार्यकारी व्हेलिंग फ़िशिंग घटना

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक कार्यकारी अधिकारी ने बोर्ड-बैठक का सुरक्षित दस्तावेज़ होने का दावा करने वाले फ़िशिंग लिंक पर क्लिक किया और एक नकली पोर्टल पर अपने मुख्य कॉर्पोरेट क्रेडेंशियल दर्ज कर दिए।
- अनुशंसित रणनीति और समाधान: एग्ज़ीक्यूटिव का डिवाइस अलग करें। सभी कॉर्पोरेट सेशन टोकन और क्रेडेंशियल रीसेट करें। डेटा के बाहर जाने के लिए एक्सेस लॉग देखें, और सभी लॉगिन पर हार्डवेयर MFA लागू करें।