नाम: _____ दिनांक: _____ अंक: _____

पहचान चोरी की रोकथाम और संपत्ति सुरक्षा गाइड

क्रेडेंशियल लीक, MFA, डार्क वेब मॉनिटरिंग, क्रेडिट फ़्रीज़ अलर्ट, सोशल इंजीनियरिंग

पहचान चोरी की रोकथाम का शिक्षण 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 पहचान चोरी की रोकथाम और शमन से परिचित कराता है। आप क्रेडेंशियल लीक, मल्टी-फ़ैक्टर प्रमाणीकरण, डार्क वेब मॉनिटरिंग, क्रेडिट फ़्रीज़ अलर्ट और सोशल इंजीनियरिंग से बचाव 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/parichay-chori/

आपका पहचान सुरक्षा लर्निंग रोडमैप

- डार्क वेब फ़ोरम पर क्रेडेंशियल के उजागर होने के जोखिम को समझें।
- मल्टी-फ़ैक्टर ऑथेंटिकेशन (MFA) और क्रेडिट फ़्रीज़ अलर्ट लागू करें।
- लक्षित सोशल इंजीनियरिंग घोटालों के विरुद्ध कॉर्पोरेट सुरक्षा बचाव तैयार करें।

पहचान चोरी गाइड के 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 पहचान सुरक्षा पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

पहचान चोरी की रोकथाम और संपत्ति सुरक्षा (परिचय)

पहचान चोरी लीक हुए क्रेडेंशियल और कमज़ोर लॉगिन का फ़ायदा उठाकर निजी और कॉर्पोरेट खातों को हाइजैक करती है। MFA, क्रेडिट फ़्रीज़, डार्क वेब स्कैनर और SPF/DKIM/DMARC फ़्रेमवर्क तैनात करना डिजिटल छद्मरूपण के विरुद्ध महत्वपूर्ण बचाव बनता है।

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

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1 **1. पहचान चोर लॉगिन क्रेडेंशियल चुराने के लिए मुख्य रूप से कौन-सी विधि अपनाते हैं?**

- A. नकली ईमेल अलर्ट भेजकर उपयोगकर्ताओं को नकली पोर्टल पर पासवर्ड डालने के लिए बहकाना
- B. उपयोगकर्ता के कॉर्पोरेट कार्यालय के पास रेडियो प्रसारण सुनना
- C. उपयोगकर्ता के स्थानीय सर्वर स्टोरेज ड्राइव को डीफ़्रैगमेंट करना
- D. बाहरी नेटवर्क बैकअप कॉन्फ़िगरेशन को डिस्कनेक्ट करना

2 **2. कौन-सा सुरक्षा नियंत्रण क्रेडेंशियल लीक के विरुद्ध सबसे मज़बूत सुरक्षा देता है?**

- A. हार्डवेयर कुंजियों का उपयोग करके मल्टी-फ़ैक्टर ऑथेंटिकेशन
- B. डिफ़ॉल्ट ब्राउज़र फ़ॉर्मेट से लंबे पासवर्ड बनाना
- C. हर छह महीने में ईमेल उपयोगकर्ता नाम बदलना
- D. संग्रहीत कुकी ट्रैकिंग ब्राउज़र इतिहास हटाना

3 **3. क्रेडिट फ़्रीज़िंग क्या दर्शाती है?**

- A. चोरों को अनधिकृत ऋण खोलने से रोकने के लिए क्रेडिट रिपोर्ट को लॉक करना
- B. डेटाबेस से बैंक खाते के लेन-देन इतिहास मिटाना
- C. स्कैनर पर क्रेडिट कार्ड मैग्नेटिक स्वाइप रीडर बंद करना
- D. लोकल डेटाबेस हार्ड ड्राइव को एट-रेस्ट एन्क्रिप्ट करना

4 **4. डार्क वेब मॉनिटरिंग क्यों उपयोगी है?**

- A. यदि उपयोगकर्ताओं के लीक हुए क्रेडेंशियल अवैध डेटाबेस में दिखें तो उन्हें सचेत करता है
- B. यह सक्रिय मैलवेयर को वर्चुअल सैंडबॉक्स में चलने से रोकता है
- C. यह वर्चुअल नेटवर्क पर ब्राउज़र रूटिंग की गति बढ़ाता है
- D. यह बैकएंड डेटाबेस SQL इंजेक्शन एक्सेस प्रयासों को ब्लॉक करता है

5 **5. सोशल इंजीनियरिंग का क्या अर्थ है?**

- A. लोगों को बहकाकर उनसे स्वेच्छा से गोपनीय क्रेडेंशियल उगलवाना
- B. सक्रिय सुरक्षा एक्सप्लॉइट के लिए कॉर्पोरेट सर्वर पोर्ट स्कैन करना
- C. सिस्टम डेटाबेस फ़ाइलों का ऑफ़लाइन हार्ड ड्राइव पर बैकअप लेना
- D. नेटवर्क पैकेट को तीन एन्क्रिप्टेड onion नोड्स से रूट करना

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न 6

6. पहचान चोरी केवल ऑनलाइन डिजिटल खातों को प्रभावित करती है, भौतिक डाक को नहीं।

○ सही ○ गलत

7 प्रश्न 7

7. सभी व्यक्तिगत खातों पर MFA लागू करने से अधिकतर क्रेडेंशियल-स्टफ़िंग बॉट हमले ब्लॉक हो जाते हैं।

○ सही ○ गलत

8 प्रश्न 8

8. क्रेडिट फ़्रीज़ क्रेडिट जाँच को ब्लॉक करता है, लेकिन आपको अपने ही बैंक खाते तक पहुँचने से रोकता है।

○ सही ○ गलत

9 प्रश्न 9

9. पासवर्ड मैनेजर नकली डोमेन पर पासवर्ड ऑटो-फ़िल करने से मना करके उपयोगकर्ताओं को फ़िशिंग से बचाते हैं।

○ सही ○ गलत

10 प्रश्न 10

10. फ़िशिंग ईमेल अक्सर भावनात्मक और जल्दबाज़ी वाली प्रतिक्रिया भड़काने के लिए तात्कालिकता भरी भाषा का उपयोग करते 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. पहचान के चोर निजी पासवर्ड और उपयोगकर्ता _____ को निशाना बनाते हैं।
2. पहचान की चोरी का सबसे आम नतीजा आर्थिक _____ है।
3. साइन-इन के लिए अस्थायी कोड माँगना आपकी _____ को मज़बूत करता है।
4. खातों में संदिग्ध लेनदेन पर लगातार नज़र रखना _____ कहलाता है।
5. अनधिकृत क्रेडिट जाँच रोकने के लिए _____ ज़रूरी है।
6. दो-चरण सत्यापन और क्रेडिट फ़्रीज़ जैसे _____ अपनाने से पहचान की चोरी का जोखिम घटता है।

शब्दावली शब्द-बैंक

क्रेडिट फ़्रीज़ | क्रेडेंशियल्स | खाता निगरानी | खाता सुरक्षा | धोखाधड़ी | फ़िशिंग | सुरक्षा उपाय | स्पूफ़िंग

अपने उत्तर यहाँ लिखें:

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

चेकपॉइंट 4: सुरक्षा अवधारणा मिलान

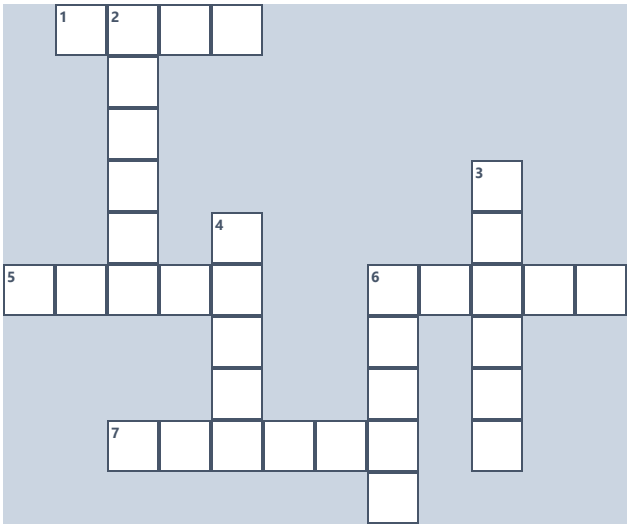
परिभाषा मिलान

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. क्रेडेंशियल**	**A**	खाते के लॉगिन की सुरक्षा करने वाला द्वितीयक सत्यापन चरण (जैसे हार्डवेयर कुंजी)।
☐	**2. लीक**	**B**	किसी वैध संगठन की नकल करने के लिए नकली वेबसाइट या ईमेल बनाना।
☐	**3. MFA**	**C**	धोखाधड़ी वाले ऋण आवेदन रोकने के लिए क्रेडिट फ़ाइलों तक पहुँच सीमित करना।
☐	**4. निगरानी**	**D**	व्यक्तिगत उपयोगकर्ता रिकॉर्ड वाले निजी डेटाबेस का अनधिकृत रूप से उजागर होना।
☐	**5. फ़्रीज़**	**E**	पहचान की चोरी से बचाव के लिए इस्तेमाल होने वाला प्रशिक्षण और तकनीकी नियंत्रण।
☐	**6. रक्षा**	**F**	उपयोगकर्ताओं को क्रेडेंशियल देने के लिए बहकाने के उद्देश्य से फ़र्ज़ी संदेश भेजना।
☐	**7. स्पूफ़िंग**	**G**	चुराए गए कॉर्पोरेट डेटा के लिए ऑनलाइन फ़ोरम और हैकर चैनल स्कैन करना।
☐	**8. फ़िशिंग**	**H**	डिजिटल पहचान प्रमाणित करने के लिए उपयोग होने वाले यूज़रनेम, पासवर्ड और निजी टोकन।

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

1. झूठ बोलकर या पहचान चुराकर किया गया आर्थिक छल (4)

5. पहचान को छिपाए रखने की स्थिति (5)

6. आपकी रिपोर्ट तक नए ऋणदाताओं की पहुँच बंद करना (5)

7. जोखिम घटाने के लिए उठाए गए कदम (6)

ऊपर से नीचे

2. खातों में संदिग्ध गतिविधि पर लगातार नज़र (6)

3. आपके ऋण-इतिहास का लेखा-जोखा (6)

4. लॉगिन को अनधिकृत पहुँच से बचाने की व्यवस्था (5)

6. खाते में प्रवेश के लिए यूज़रनेम और पासवर्ड जैसी जानकारी (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

1 बाएँ से दाएँ: झूठ बोलकर या पहचान चुराकर किया गया आर्थिक छल (4 अक्षर):

5 बाएँ से दाएँ: पहचान को छिपाए रखने की स्थिति (5 अक्षर):

6 बाएँ से दाएँ: आपकी रिपोर्ट तक नए ऋणदाताओं की पहुँच बंद करना (5 अक्षर):

7 बाएँ से दाएँ: जोखिम घटाने के लिए उठाए गए कदम (6 अक्षर):

ऊपर से नीचे

2 ऊपर से नीचे: खातों में संदिग्ध गतिविधि पर लगातार नज़र (6 अक्षर):

3 ऊपर से नीचे: आपके ऋण-इतिहास का लेखा-जोखा (6 अक्षर):

4 ऊपर से नीचे: लॉगिन को अनधिकृत पहुँच से बचाने की व्यवस्था (5 अक्षर):

6 ऊपर से नीचे: खाते में प्रवेश के लिए यूज़रनेम और पासवर्ड जैसी जानकारी (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।

ते	वी	ति	च	ह	री	रा	व	त	सा	स	ई	ते	घ	इ
नी	ल्स	ल	रि	द	जे	घ	छ	खा	ई	के	द	प	ति	के
ट	य	मि	ट	सा	य	च	ऊ	नी	ता	जी	इ	त	म	पे
ब	शि	प	जि	मी	ने	ले	इ	सी	य	सु	छ	र	दे	कि
जा	डें	सा	वा	ड	क्रे	रे	स	ख	नि	फ	र	ढ	धो	मा
ना	क्रे	का	रे	दे	डि	सि	खा	मी	क	पि	ता	क्षा	खा	ति
ज	श	भ	ऊ	अ	ट	ऊ	ए	ता	रि	वि	श	य	ध	वि
ज़	व	वा	पा	ल	रि	च	से	कि	नि	य	घ	प	ड़ी	के
फ़्री	की	व	सि	री	पो	त	की	कि	सि	ग	ना	ने	पा	ते
ट	ण	ए	ता	सा	र्ट	मी	न	नी	ऋ	ले	रा	घ	ति	जि
डि	सु	र	क्षा	उ	पा	य	ला	ए	जी	ले	ड	नी	ल	गो
क्रे	द	जे	घ	के	च	से	दे	री	ए	पी	उ	अ	प	जे
मि	घ	व	आ	च	मी	च	ट	थ	फ	ग	ना	नी	सी	का
ज	फ	नी	जी	ता	ठ	से	लि	ट	आ	इ	य	से	रा	के
री	पा	वा	सि	य	नि	पि	ने	ख	के	ता	वे	ऊ	ड	नी

शब्दावली शब्द-सूची

क्रेडेंशियल्स, क्रेडिटफ़्रीज़, धोखाधड़ी, खातासुरक्षा, क्रेडिटरिपोर्ट, सुरक्षाउपाय, गोपनीयता, खातानिगरानी

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. क्रेडेंशियल्स
B. क्रेडिटफ़्रीज़
C. धोखाधड़ी
D. खातासुरक्षा
E. क्रेडिटरिपोर्ट
F. सुरक्षाउपाय
G. गोपनीयता
H. खातानिगरानी

परिभाषाएँ और मिलान फ़ील्ड
1. खातों में संदिग्ध गतिविधि पर लगातार नज़र।
2. खाते में प्रवेश के लिए यूज़रनेम और पासवर्ड जैसी जानकारी।
3. पहचान को छिपाए रखने की स्थिति।
4. जोखिम घटाने के लिए उठाए गए कदम।
5. लॉगिन को अनधिकृत पहुँच से बचाने की व्यवस्था।
6. आपके ऋण-इतिहास का लेखा-जोखा।
7. आपकी रिपोर्ट तक नए ऋणदाताओं की पहुँच बंद करना।
8. झूठ बोलकर या पहचान चुराकर किया गया आर्थिक छल।

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. **य शि क्रे ल्स डें**
2. **धो ध ड़ी खा**
3. **क्रे ट रि र्ट पो डि**
4. **नी ता य गो प**
5. **ट ज़ क्रे फ़ी डि**
6. **र खा सु क्षा ता**
7. **पा सु उ य क्षा र**
8. **नि नी खा रा ग ता**

अतिरिक्त गतिविधि: झटपट सोचें

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

1	पहचान चोरी होने पर की जाने वाली चीज़ें			
2	सोशल मीडिया पर साझा न करने वाली चीज़ें			
3	ऐसी चीज़ें जिनका आप बैकअप लेते हैं			
4	आपके बटुए में रखे कार्ड या पहचान पत्र			
5	ऐसे दस्तावेज़ जिन्हें आपको सुरक्षित रखना चाहिए			
6	डेटा लीक के बाद की जाने वाली चीज़ें			
7	सॉफ़्टवेयर अपडेट करने के कारण			
8	ऐसी जानकारी जो पहचान चुराने वाला चाहता है			
9	ऐसे डिवाइस जिन्हें हैक किया जा सकता है			
10	ऐसी जगहें जहाँ से आपका डेटा लीक हो सकता है			
11	सुरक्षित आदतें जो आप आज से शुरू कर सकते हैं			
12	कंप्यूटर के संक्रमित होने के संकेत			
13	अपनी पहचान साबित करने के तरीके			
14	पहचान की चोरी के संकेत			
15	ईमेल में चेतावनी के संकेत			

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: कार्यकारी पहचान प्रतिरूपण से सुरक्षा



परिदृश्य: एक हाई-प्रोफ़ाइल C-suite अधिकारी को ग्राहकों से धोखाधड़ी करने के लिए उनके निजी ईमेल की नकल करने वाले टाइपो-स्क्वैटेड डोमेन नामों से निशाना बनाया गया है। एक ब्रांड सुरक्षा योजना डिज़ाइन कीजिए।

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

केस स्टडी 2: डार्क वेब पर कॉर्पोरेट क्रेडेंशियल का उजागर होना



परिदृश्य: एक डार्क वेब डेटाबेस डंप में एक उद्यम के सिस्टम एडमिनिस्ट्रेटरों के कई सौ कॉर्पोरेट क्रेडेंशियल शामिल हैं। एक शमन रणनीति डिज़ाइन कीजिए।

चर्चा प्रश्न: क्रेडेंशियल सफ़ाई प्रक्रिया की रूपरेखा बताइए और पासवर्ड मैनेजर रोल-आउट की योजना बनाइए।

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

37	40	61	23	48	34	60	53	13	61	23	39

33	61	39	37	46	27	48	13	39	27	44	52	33	45	18	46	32

35	18	46	8	58

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: पहचान चोरी क्या है?

ऐसा अपराध जिसमें हमलावर आर्थिक लाभ के लिए किसी और की नकल करने हेतु व्यक्तिगत रिकॉर्ड (जैसे पासवर्ड या SSN) चुराता है।

Q2: पहचान चोरी का सबसे आम कारण क्या है?

फ़िशिंग वह प्रमुख तरीका है जिससे चोर पासवर्ड हासिल करते हैं, और वे उपयोगकर्ताओं को नकली, स्पूफ़ की गई वेबसाइटों पर फुसलाते हैं।

Q3: मल्टी-फ़ैक्टर ऑथेंटिकेशन (MFA) पहचान की सुरक्षा कैसे करता है?

MFA में लॉग इन के लिए दूसरा प्रमाण (जैसे हार्डवेयर कुंजी) चाहिए, जो आपका पासवर्ड चुरा लेने पर भी हमलावरों को रोकता है।

Q4: क्रेडिट फ़्रीज़ क्या है?

मुफ़्त सेवा जो क्रेडिट ब्यूरो को आपकी क्रेडिट फ़ाइल साझा करने से रोकती है, जिससे चोर आपके नाम पर नए ऋण नहीं खोल पाते। [2]

Q5: डार्क वेब मॉनिटरिंग क्या है?

हैकर फ़ोरम में लीक हुए ईमेल, पासवर्ड और निजी रिकॉर्ड खोजने वाला सॉफ़्टवेयर, जो आपका डेटा उजागर होने पर आपको सचेत करता है।

चेकपॉइंट 10: बुनियादी साइबर सुरक्षा FAQ (भाग B)

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

Q6: क्रेडेंशियल स्टफ़िंग का क्या अर्थ है?

स्वचालित बॉट जो सैकड़ों वेबसाइटों पर लीक हुई पासवर्ड सूचियाँ आज़माकर सक्रिय खातों पर कब्ज़ा कर लेते हैं।

Q7: ईमेल स्पूफ़िंग खतरनाक क्यों है?

यह हमलावरों को ईमेल में भेजने वाले का नाम जाली बनाने देता है, जिससे फ़िशिंग संदेश भरोसेमंद सहकर्मियों से आए हुए लगते हैं।

Q8: पासवर्ड मैनेजर पहचान की चोरी को कैसे रोकते हैं?

वे हर खाते के लिए जटिल, अद्वितीय पासवर्ड संग्रहीत करते हैं और नकली फ़िशिंग डोमेन पर क्रेडेंशियल ऑटो-फ़िल करने से मना कर देते हैं।

Q9: स्पीयर फ़िशिंग क्या है?

अत्यधिक लक्षित फ़िशिंग हमला, जिसे धोखा देने की संभावना बढ़ाने के लिए पीड़ित के नाम और विवरणों के अनुसार तैयार किया जाता है।

Q10: क्रेडिट अलर्ट फ़्रीज़ से कैसे अलग है?

अलर्ट ऋणदाताओं को खाते खोलने से पहले आपकी पहचान सत्यापित करने को कहता है, जबकि फ़्रीज़ आपकी क्रेडिट फ़ाइल तक पहुँच को पूरी तरह ब्लॉक कर देता है। [2]

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग C)

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

Q1: SIM स्वैपिंग पहचान चोरी तक कैसे पहुँचती है?

हमलावर वाहक कंपनी के कर्मचारियों को मनाकर पीड़ित का फ़ोन नंबर नए SIM कार्ड पर ट्रांसफ़र करा लेते हैं और SMS-आधारित 2FA कोड हाइजैक कर लेते हैं।

Q2: पहचान चोरी रोकने में DMARC की क्या भूमिका है?

DMARC डोमेन मालिकों को स्पूफ़ किए गए ईमेल को इनबॉक्स तक पहुँचने से रोकने देता है, जिससे नकली ईमेल कंपनी के डोमेन की नकल नहीं कर पाते।

Q3: सिंथेटिक आइडेंटिटी चोरी का पता लगाना कठिन क्यों है?

चोर असली SSN को नकली नामों और जन्मतिथियों के साथ मिलाकर बिल्कुल नए क्रेडिट प्रोफ़ाइल बनाते हैं, जिससे बुनियादी धोखाधड़ी अलर्ट बच जाते हैं।

Q4: डेटा ब्रोकर व्यक्तिगत पहचानों का दुरुपयोग कैसे करते हैं?

ब्रोकर प्रोफ़ाइल डोज़ियर बनाने के लिए सार्वजनिक रिकॉर्ड, वेब व्यवहार और खरीद इतिहास जमा करते हैं, जो लीक या बेचे जा सकते हैं।

Q5: SMS-आधारित MFA को असुरक्षित क्यों माना जाता है?

SMS ट्रैफ़िक इंटरसेप्शन, फ़िशिंग और कैरियर-स्तर के SIM-स्वैपिंग एक्सप्लॉइट के प्रति संवेदनशील है।

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग D)

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

Q6: क्रेडिट फ़ाइल लॉक क्या है?

फ़्रीज़ जैसी एक व्यावसायिक सेवा, जिसमें उपयोगकर्ता मोबाइल ऐप से अपनी क्रेडिट फ़ाइल को तुरंत अनलॉक या लॉक कर सकते हैं।

Q7: कॉर्पोरेट डेटा उल्लंघन पहचान की चोरी को कैसे बढ़ावा देते हैं?

लीक हुए डेटाबेस लाखों सादे क्रेडेंशियल उजागर कर देते हैं, जिससे चोरों को लक्षित पहचान धोखाधड़ी करने के लिए ज़रूरी कच्चा डेटा मिल जाता है।

Q8: सोशल मीडिया पर ज़्यादा जानकारी साझा करने का जोखिम क्या है?

पालतू जानवरों के नाम, जन्मस्थान और माँ का विवाह-पूर्व नाम सार्वजनिक रूप से साझा करने से चोरों को खाता रिकवरी के आम सवालों के जवाब मिल जाते हैं।

Q9: बायोमेट्रिक लॉगिन पहचान प्रोफ़ाइल की सुरक्षा कैसे करते हैं?

बायोमेट्रिक्स लॉगिन को फ़िंगरप्रिंट या चेहरे जैसी विशेषताओं से जोड़ता है; डिवाइस पर रखे जाने पर इन्हें चुराना कठिन होता है, लेकिन संग्रहीत बायोमेट्रिक डेटा लीक हो सकता है।

Q10: Red Flags Rule पहचान चोरी से कैसे लड़ता है?

संघीय विनियम जिसके तहत वित्तीय संस्थानों को पहचान चोरी के चेतावनी संकेतों का पता लगाने और उन पर कार्रवाई करने के लिए लिखित कार्यक्रम बनाने होते हैं।

भाग 11: 10 वास्तविक साइबर सुरक्षा तथ्य और अंतर्दृष्टियाँ

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

1. सुरक्षा इनसाइट

FTC द्वारा संचालित IdentityTheft.gov अमेरिकी पीड़ितों को पहचान चोरी की रिपोर्ट करने और व्यक्तिगत रिकवरी योजना पाने की सुविधा देता है। [1]

2. सुरक्षा इनसाइट

हार्डवेयर सुरक्षा कुंजियाँ फ़िशिंग-प्रतिरोधी MFA हैं, जो CISA द्वारा आग्रह किया गया सबसे मज़बूत प्रकार का MFA है। [4]

3. सुरक्षा इनसाइट

समझौता हुए पासवर्ड डेटा उल्लंघनों का एक आम प्रवेश बिंदु हैं, जो आगे चलकर पहचान की धोखाधड़ी को बढ़ावा देते हैं।

4. सुरक्षा इनसाइट

क्रेडिट फ़्रीज़ संघीय कानून के तहत निःशुल्क है और अनलॉक किए जाने तक ऋणदाताओं को क्रेडिट फ़ाइल जाँचने से रोकता है। [2]

5. सुरक्षा इनसाइट

DMARC डोमेन मालिकों को मेल सर्वरों से यह कहने देता है कि जाँच में विफल स्पूफ़ किए गए ईमेल को अस्वीकार या क्वारंटीन करें। [7]

6. सुरक्षा इनसाइट

SIM स्वैपिंग हैकरों को बैंकिंग पोर्टल पर SMS-आधारित टू-फ़ैक्टर ऑथेंटिकेशन बायपास करने देती है।

7. सिक्योरिटी इनसाइट

सिंथेटिक पहचान धोखाधड़ी असली और नकली विवरण मिला देती है, जिससे ऋणदाताओं के लिए उसे पहचानना कठिन होता है।

8. सिक्योरिटी इनसाइट

कई लोग अपने ऑनलाइन खातों में एक ही पासवर्ड दोहराते हैं, इसलिए एक उल्लंघन से कई खाते उजागर हो सकते हैं।

9. सिक्योरिटी इनसाइट

डेटा ब्रोकर बड़ी संख्या में उपभोक्ताओं की विस्तृत प्रोफ़ाइलें बनाते हैं, जिससे गोपनीयता का जोखिम एक जगह केंद्रित हो जाता है।

10. सुरक्षा इनसाइट

पहचान की चोरी से उबरने में महीनों लग सकते हैं, जैसे शुल्कों पर विवाद करना और क्रेडिट रिपोर्ट ठीक कराना।

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.). IdentityTheft.gov: Report identity theft and get a recovery plan.
https://www.identitytheft.gov/

[2] Federal Trade Commission. (2025). Credit Freezes and Fraud Alerts.
https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts

[3] Federal Trade Commission. (n.d.). What To Know About Identity Theft.
https://consumer.ftc.gov/articles/what-know-about-identity-theft

[4] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[5] 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

[6] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[7] 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

पहचान चोर लॉगिन क्रेडेंशियल चुराने के लिए मुख्य रूप से कौन-सी विधि अपनाते हैं? → नकली ईमेल अलर्ट भेजकर उपयोगकर्ताओं को नकली पोर्टल पर पासवर्ड डालने के लिए बहकाना

2 **प्रश्न 2** — **सही उत्तर: A**

शिक्षण नोट

कौन-सा सुरक्षा नियंत्रण क्रेडेंशियल लीक के विरुद्ध सबसे मज़बूत सुरक्षा देता है? → हार्डवेयर कुंजियों का उपयोग करके मल्टी-फ़ैक्टर ऑथेंटिकेशन

3 **प्रश्न 3** — **सही उत्तर: A**

शिक्षण नोट

क्रेडिट फ़्रीज़िंग क्या दर्शाती है? → चोरों को अनधिकृत ऋण खोलने से रोकने के लिए क्रेडिट रिपोर्ट को लॉक करना

4 **प्रश्न 4** — **सही उत्तर: A**

शिक्षण नोट

डार्क वेब मॉनिटरिंग क्यों उपयोगी है? → यदि उपयोगकर्ताओं के लीक हुए क्रेडेंशियल अवैध डेटाबेस में दिखें तो उन्हें सचेत करता है

5 **प्रश्न 5** — **सही उत्तर: A**

शिक्षण नोट

सोशल इंजीनियरिंग का क्या अर्थ है? → लोगों को बहकाकर उनसे स्वेच्छा से गोपनीय क्रेडेंशियल उगलवाना

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 प्रश्न 6 — सही उत्तर: गलत

शिक्षण नोट

पहचान की चोरी ऑफ़लाइन भी शुरू हो सकती है, जैसे चोरी हुई डाक या दस्तावेज़।

7 प्रश्न 7 — सही उत्तर: सही

शिक्षण नोट

सभी व्यक्तिगत खातों पर MFA लागू करने से अधिकतर क्रेडेंशियल-स्टफ़िंग बॉट हमले ब्लॉक हो जाते हैं।

8 प्रश्न 8 — सही उत्तर: गलत

शिक्षण नोट

क्रेडिट फ़्रीज़ नई क्रेडिट जाँच रोकता है लेकिन आपके मौजूदा अकाउंट को प्रभावित नहीं करता।

9 प्रश्न 9 — सही उत्तर: सही

शिक्षण नोट

पासवर्ड मैनेजर नकली डोमेन पर पासवर्ड ऑटो-फ़िल करने से मना करके उपयोगकर्ताओं को फ़िशिंग से बचाते हैं।

10 प्रश्न 10 — सही उत्तर: सही

शिक्षण नोट

फ़िशिंग ईमेल अक्सर भावनात्मक और जल्दबाज़ी वाली प्रतिक्रिया भड़काने के लिए तात्कालिकता भरी भाषा का उपयोग करते 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

H 1. क्रेडेंशियल	D 2. लीक	A 3. MFA	G 4. निगरानी
C 5. फ़्रीज़	E 6. रक्षा	B 7. स्पूफ़िंग	F 8. फ़िशिंग

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 क्रेडेंशियल्स	2 धोखाधड़ी	3 खाता सुरक्षा	4 खाता निगरानी
5 क्रेडिट फ़्रीज़	6 सुरक्षा उपाय		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

1 H – खातानिगरानी	2 A – क्रेडेंशियल्स	3 G – गोपनीयता	4 F – सुरक्षाउपाय
5 D – खातासुरक्षा	6 E – क्रेडिटरिपोर्ट	7 B – क्रेडिटफ़्रीज़	8 C – धोखाधड़ी

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी क्रेडेंशियल, लीक और MFA 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।

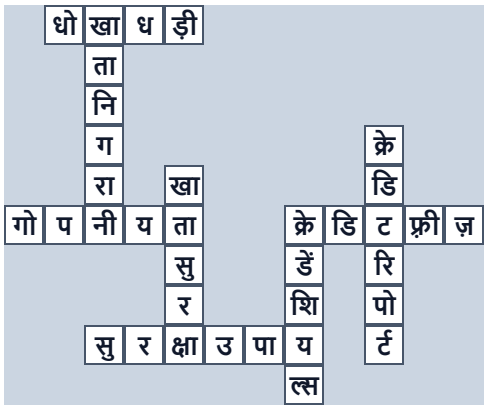
स्रोतों का मूल्यांकन:
विद्यार्थियों से वर्कशीट के स्रोतों में कम से कम एक कथन की पुष्टि करवाएँ और चर्चा करें कि आँकड़े, कीमतें और नियम समय के साथ क्यों बदल सकते हैं।

पहेलियों की कुंजियाँ और शिक्षक नोट

शब्द खोज समाधान

ते	वी	ति	च	ह	री	रा	व	त	सा	स	ई	ते	घ	इ
नी	ल्स	ल	रि	द	जे	घ	छ	खा	ई	के	द	प	ति	के
ट	य	मि	ट	सा	य	च	ऊ	नी	ता	जी	इ	त	म	पे
ब	शि	प	जि	मी	ने	ले	इ	सी	य	सु	छ	र	दे	कि
जा	डें	सा	वा	ड	क्रे	रे	स	ख	नि	फ	र	ढ	धो	मा
ना	क्रे	का	रे	दे	डि	सि	खा	मी	क	पि	ता	क्षा	खा	ति
ज	श	भ	ऊ	अ	ट	ऊ	ए	ता	रि	वि	श	य	ध	वि
ज़	व	वा	पा	ल	रि	च	से	कि	नि	य	घ	प	ड़ी	के
फ़्री	की	व	सि	री	पो	त	की	कि	सि	ग	ना	ने	पा	ते
ट	ण	ए	ता	सा	र्ट	मी	न	नी	ऋ	ले	रा	घ	ति	जि
डि	सु	र	क्षा	उ	पा	य	ला	ए	जी	ले	ड	नी	ल	गो
क्रे	द	जे	घ	के	च	से	दे	री	ए	पी	उ	अ	प	जे
मि	घ	व	आ	च	मी	च	ट	थ	फ	ग	ना	नी	सी	का
ज	फ	नी	जी	ता	ठ	से	लि	ट	आ	इ	य	से	रा	के
री	पा	वा	सि	य	नि	पि	ने	ख	के	ता	वे	ऊ	ड	नी

क्रॉसवर्ड समाधान



क्रॉसवर्ड समाधान के लिए शिक्षक गाइड

बाएँ से दाएँ

1 बाएँ से दाएँ: धोखाधड़ी झूठ बोलकर या पहचान चुराकर किया गया आर्थिक छल (4 अक्षर)

5 बाएँ से दाएँ: गोपनीयता पहचान को छिपाए रखने की स्थिति (5 अक्षर)

6 बाएँ से दाएँ: क्रेडिटफ़्रीज़ आपकी रिपोर्ट तक नए ऋणदाताओं की पहुँच बंद करना (5 अक्षर)

7 बाएँ से दाएँ: सुरक्षाउपाय जोखिम घटाने के लिए उठाए गए कदम (6 अक्षर)

ऊपर से नीचे

2 ऊपर से नीचे: खातानिगरानी खातों में संदिग्ध गतिविधि पर लगातार नज़र (6 अक्षर)

3 ऊपर से नीचे: क्रेडिटरिपोर्ट आपके ऋण-इतिहास का लेखा-जोखा (6 अक्षर)

4 ऊपर से नीचे: खातासुरक्षा लॉगिन को अनधिकृत पहुँच से बचाने की व्यवस्था (5 अक्षर)

6 ऊपर से नीचे: क्रेडेंशियल्स खाते में प्रवेश के लिए यूज़रनेम और पासवर्ड जैसी जानकारी (5 अक्षर)

अक्षर-फेर शब्द और कूट संदेश हल कुंजी

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

शब्द अनस्क्रैम्बल कुंजी

1. य शि क्रे ल्स डें — **क्रेडेंशियल्स**
2. धो ध ड़ी खा — **धोखाधड़ी**
3. क्रे ट रि र्ट पो डि — **क्रेडिटरिपोर्ट**
4. नी ता य गो प — **गोपनीयता**
5. ट ज़ क्रे फ़्री डि — **क्रेडिटफ़्रीज़**
6. र खा सु क्षा ता — **खातासुरक्षा**
7. पा सु उ य क्षा र — **सुरक्षाउपाय**
8. नि नी खा रा ग ता — **खातानिगरानी**

गुप्त कूट चुनौती कुंजी

"मल्टीफ़ैक्टर प्रमाणीकरण से पहचान बचाएँ"

केस स्टडी के उत्तर

A केस स्टडी 1: कार्यकारी पहचान प्रतिरूपण से सुरक्षा

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक हाई-प्रोफ़ाइल C-suite एग्ज़ीक्यूटिव को ग्राहकों से धोखाधड़ी के लिए उनके निजी ईमेल की नकल करने वाले टाइपो-स्क्वाटेड डोमेन नामों से निशाना बनाया गया है। ब्रांड सुरक्षा योजना तैयार करें।
- अनुशंसित रणनीति और समाधान: एग्ज़ीक्यूटिव के नाम की सभी आम वर्तनी वाले रूप रजिस्टर करें। डोमेन स्पूफ़िंग रोकने के लिए ईमेल ऑथेंटिकेशन प्रोटोकॉल (DMARC, DKIM, SPF) लगाएँ। सभी C-suite कॉर्पोरेट लॉगिन पर हार्डवेयर MFA लागू करें।

B केस स्टडी 2: डार्क वेब पर कॉर्पोरेट क्रेडेंशियल का उजागर होना

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक डार्क वेब डेटाबेस डंप में एक एंटरप्राइज़ के सिस्टम एडमिनिस्ट्रेटरों के कई सौ कॉर्पोरेट क्रेडेंशियल हैं। एक शमन रणनीति तैयार करें।
- अनुशंसित रणनीति और समाधान: पूरी कंपनी के स्तर पर पासवर्ड रीसेट करें। एंटरप्राइज़ पासवर्ड मैनेजर का उपयोग अनिवार्य करें। सभी सिस्टम पोर्टल पर MFA लागू करें और निरंतर स्वचालित डार्क वेब मॉनिटरिंग अलर्ट सेट करें।