نام: _____ تاریخ: _____ نمبر: _____

شناخت کی چوری کی روک تھام اور اثاثے سیکیورٹی گائیڈ

کریڈینشل لیکس، MFA، ڈارک ویب مانیٹرنگ، کریڈٹ فریز الرٹس، سوشل انجینئرنگ

شناخت کی چوری کی روک تھام کا تعلیمی جائزہ

محفوظ شدہ
ڈیٹا کی خفیہ کاری
256 بٹ AES معیار

تعمیل شدہ
عالمی معیارات
GDPR اور CCPA فریم ورکس

زیرو ٹرسٹ
رسائی کی پالیسی
ملٹی فیکٹر تصدیق

خوش آمدید! یہ سرگرمی پیکٹ آپ کو شناخت کی چوری کی روک تھام اور تدارک سے متعارف کراتا ہے۔ آپ اسناد کے لیکس، ملٹی فیکٹر تصدیق، ڈارک ویب مانیٹرنگ، کریڈٹ فریز الرٹس، اور سوشل انجینئرنگ سے دفاع کا جائزہ لیں گے۔

ورک شیٹ کے چیک پوائنٹس

- ☐ **حصہ 1-4: سائبر سیکیورٹی اور خطرات سے بچاؤ میں مہارت حاصل کریں۔**
- ☐ **حصہ 5-7: کراس ورڈ اور ورڈ سرچ پہیلیاں حل کریں۔**
- ☐ **حصہ 8-9: کیس اسٹڈیز اور سائفر چیلنج حل کریں۔**
- ☐ **حصہ 10: بنیادی اور اعلیٰ FAQ صفحات کا جائزہ لیں۔**
- ☐ **حصہ 11: 10 دلچسپ حقیقی دنیا کے حقائق دریافت کریں۔**
- ☐ **اضافی: تیزی سے سوچیں چیلنج**

VPN.com سائبر سیکیورٹی گائیڈ کھولیں

URL: https://www.vpn.com/cybersecurity/identity-theft/

آپ کی شناخت کے تحفظ کا لرننگ روڈ میپ

- ڈارک ویب فورمز پر اسناد کے افشا کے خطرات کو سمجھیں۔
- ملٹی فیکٹر تصدیق (MFA) اور کریڈٹ فریز الرٹس نافذ کریں۔
- ہدف بنائے گئے سوشل انجینئرنگ فراڈز کے خلاف کارپوریٹ سیکیورٹی دفاع ڈیزائن کریں۔

شناخت کی چوری گائیڈ کی ہدایات

کثیر انتخابی اور درست/غلط سوالات حل کریں، لفظوں کے ذخیرے کی مدد سے خالی جگہیں پُر کریں، تعریفوں کا ملان کریں، اور کراس ورڈ اور ورڈ سرچ پہیلیاں حل کریں۔ اپنے علم کو شناخت کے تحفظ پر لاگو کریں۔ اور آخر میں اضافی سرگرمی "تیزی سے سوچیں"۔

شناخت کی چوری کی روک تھام اور اثاثوں کی سیکیورٹی (تعارف)

شناخت کی چوری افشا شدہ اسناد اور کمزور لاگ اِنز کا فائدہ اٹھا کر ذاتی اور کارپوریٹ اکاؤنٹس ہائی جیک کرتی ہے۔ MFA، کریڈٹ فریز، ڈارک ویب اسکینرز اور SPF/DKIM/DMARC فریم ورکس کی تعیناتی ڈیجیٹل نقالی کے خلاف ایک اہم دفاع بناتی ہے۔

ہر چیک پوائنٹ کو غور سے پڑھیں اور درست جواب منتخب کریں یا لکھیں۔

چیک پوائنٹ 1: کثیر انتخابی چیلنج

1 1. شناخت چور لاگ اِن اسناد چرانے کے لیے کون سا بنیادی طریقہ استعمال کرتے ہیں؟

- A. جعلی ای میل الرٹس بھیجنا جو صارفین کو جعلی پورٹلز پر پاس ورڈ درج کرنے پر بہکاتے ہیں
- B. صارف کے کارپوریٹ دفتر کے قریب ریڈیو نشریات سننا
- C. صارف کی مقامی سرور اسٹوریج ڈرائیو کو ڈیفریگمنٹ کرنا
- D. بیرونی نیٹ ورک بیک اپ کنفیگریشنز کو منقطع کرنا

2 2. کون سا سیکیورٹی کنٹرول اسناد کے لیکس کے خلاف سب سے مضبوط دفاع فراہم کرتا ہے؟

- A. ہارڈ ویئر کیز کے ساتھ ملٹی فیکٹر تصدیق
- B. براؤزر کے ڈیفالٹ فارمیٹس سے لمبے پاس ورڈز بنانا
- C. ہر چھ ماہ بعد ای میل یوزر نیم بدلنا
- D. محفوظ شدہ کوکی ٹریکنگ براؤزر ہسٹریز حذف کرنا

3 3. کریڈٹ فریزنگ کی نمائندگی کیا کرتا ہے؟

- A. غیر مجاز قرضے لینے سے چوروں کو روکنے کے لیے کریڈٹ رپورٹس کو لاک کرنا
- B. ڈیٹا بیس سے بینک اکاؤنٹ کی لین دین کی ہسٹری حذف کرنا
- C. اسکینرز پر کریڈٹ کارڈ کے میگنیٹک سوائپ ریڈرز کو بند کرنا
- D. مقامی ڈیٹا بیس ہارڈ ڈرائیوز کو ایٹ ریسٹ خفیہ کرنا

4 4. ڈارک ویب مانیٹرنگ کیوں مفید ہے؟

- A. اگر صارفین کی لیک شدہ اسناد غیر قانونی ڈیٹا بیسز میں ظاہر ہوں تو یہ انہیں خبردار کرتا ہے
- B. یہ فعال میل ویئر کو ورچوئل سینڈ باکسز میں چلنے سے روکتا ہے
- C. یہ ورچوئل نیٹ ورکس پر براؤزر روٹنگ کی رفتار بڑھاتا ہے
- D. یہ بیک اینڈ ڈیٹا بیس SQL انجیکشن رسائی کی کوششوں کو بلاک کرتا ہے

5 5. سوشل انجینئرنگ کا کیا مطلب ہے؟

- A. لوگوں کو بہلا کر ان سے رضاکارانہ طور پر خفیہ اسناد ظاہر کروانا
- B. فعال سیکیورٹی کمزوریوں کے لیے کارپوریٹ سرور پورٹس کی اسکیننگ
- C. سسٹم ڈیٹا بیس فائلوں کا آف لائن ہارڈ ڈرائیوز پر بیک اپ بنانا
- D. نیٹ ورک پیکٹس کو تین خفیہ onion نوڈز سے گزارنا

چیک پوائنٹ 2: درست یا غلط چیلنج

6 سوال 6

6. شناخت کی چوری صرف آن لائن ڈیجیٹل اکاؤنٹس کو متاثر کرتی ہے، فزیکل ڈاک کو نہیں۔

○ درست ○ غلط

7 سوال 7

7. تمام ذاتی اکاؤنٹس پر MFA نافذ کرنا زیادہ تر کریڈینشل اسٹفنگ بوٹ حملوں کو روکتا ہے۔

○ درست ○ غلط

8 سوال 8

8. کریڈٹ فریز کریڈٹ چیکس کو بلاک کرتا ہے لیکن آپ کو اپنے بینک اکاؤنٹ تک رسائی سے روکتا ہے۔

○ درست ○ غلط

9 سوال 9

9. پاس ورڈ مینیجر جعلی ڈومینز پر پاس ورڈز خود بخود بھرنے سے انکار کر کے صارفین کو فشنگ سے بچاتے ہیں۔

○ درست ○ غلط

10 سوال 10

10. فشنگ ای میلز اکثر جذباتی اور جلد بازی والے ردعمل کو ابھارنے کے لیے فوری نوعیت کی زبان استعمال کرتی ہیں۔

○ درست ○ غلط

چیک پوائنٹ 3: کلیدی اصطلاح شامل کرنا

ذیل میں ہر جملہ پڑھیں اور خالی جگہ کو ورڈ بینک سے درست اصطلاح کے ساتھ پُر کریں۔

1. شناخت چوری کرنے والے ذاتی پاس ورڈز اور صارف کی _____ کو نشانہ بناتے ہیں۔
2. ڈیٹابیس خلاف ورزیوں سے صارفین کو خبردار کرنا نجی اکاؤنٹ _____ کی نشاندہی کرتا ہے۔
3. سائن اِن کے لیے عارضی کوڈ طلب کرنا _____ کہلاتا ہے۔
4. چوری شدہ ڈیٹا کے لیے ہیکر فورمز کی اسکیننگ ڈارک ویب _____ ہے۔
5. غیر مجاز کریڈٹ چیکس کو روکنے کے لیے کریڈٹ _____ درکار ہوتا ہے۔
6. ملازمین کو فشنگ سے آگاہی کی تربیت دینا ایک فعال سیکیورٹی _____ تشکیل دیتا ہے۔

الفاظ کا بینک

اسپوفنگ　اسناد　ایم ایف اے　دفاع　فریز　فشنگ　لیکس　نگرانی

اپنے جوابات یہاں لکھیں:

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

چیک پوائنٹ 4: سیکیورٹی تصورات کا ملان

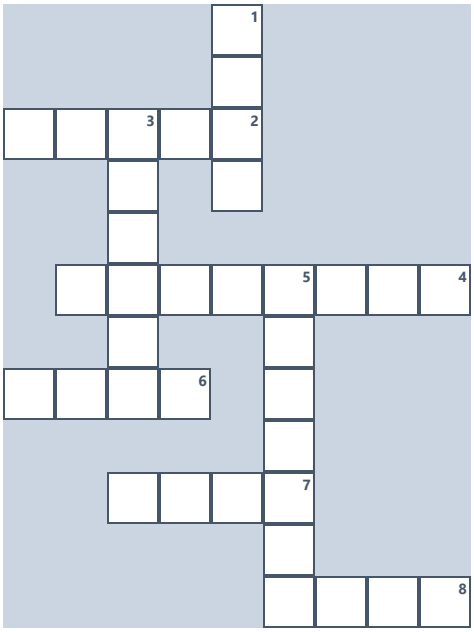
تعریفوں کا ملان

دائیں جانب کی ہر اصطلاح کو بائیں جانب کی درست تعریف سے ملائیں اور بھرے جانے والے ان پٹ باکس میں متعلقہ حرف (A-H) لکھیں۔

1. کریڈینشلز	A	اکاؤنٹ لاگ اِن کی حفاظت کرنے والا ثانوی تصدیقی مرحلہ (جیسے ہارڈ ویئر کیز)۔
2. لیکس	B	کسی جائز ادارے کی نقل کرنے کے لیے جعلی ویب سائٹ یا ای میل بنانا۔
3. MFA	C	جعلی قرض درخواستوں کو روکنے کے لیے کریڈٹ فائلوں تک رسائی محدود کرنا۔
4. نگرانی	D	ذاتی صارف ریکارڈز پر مشتمل نجی ڈیٹا بیسز کا غیر مجاز افشا۔
5. منجمد کرنا	E	شناخت کی چوری سے بچاؤ کے لیے استعمال ہونے والی تربیت اور تکنیکی کنٹرولز۔
6. دفاع	F	صارفین کو اسناد دینے پر آمادہ کرنے کے لیے جعلی پیغامات بھیجنا۔
7. اسپوفنگ	G	چوری شدہ کارپوریٹ ڈیٹا کے لیے آن لائن فورمز اور ہیکر چینلز کی اسکیننگ۔
8. فشنگ	H	ڈیجیٹل شناختوں کی تصدیق کے لیے استعمال ہونے والے یوزر نیم، پاس ورڈز اور نجی ٹوکنز۔

چیک پوائنٹ 5: کراس ورڈ پہیلی

فعال سفید خانوں میں حروف ٹائپ کر کے کراس ورڈ پہیلی حل کریں۔ نمبر نیچے دیے گئے سراغوں سے مطابقت رکھتے ہیں۔



افقی

2. ڈیجیٹل شناخت کی توثیق کے لیے استعمال ہونے والے صارف نام، پاس ورڈز اور نجی ٹوکنز (5)

4. اکاؤنٹ لاگ اِن کو تحفظ دینے والا اضافی تصدیقی مرحلہ (مثلاً ہارڈ ویئر کیز) (8)

6. ذاتی صارف ریکارڈز پر مشتمل نجی ڈیٹابیسز کا غیر مجاز انکشاف (4)

7. جعلی قرض درخواستوں کو روکنے کے لیے کریڈٹ فائلوں تک رسائی محدود کرنا (4)

8. صارفین کو دھوکے سے اسناد حاصل کرنے کے لیے جعلی پیغامات بھیجنا (4)

عمودی

1. شناخت کی چوری سے بچاؤ کے لیے استعمال ہونے والی تربیت اور تکنیکی کنٹرولز (4)

3. چوری شدہ کارپوریٹ ڈیٹا کے لیے آن لائن فورمز اور ہیکر چینلز کی اسکیننگ (6)

5. جائز ادارے کی نقل کرنے کے لیے جعلی ویب سائٹ یا ای میل بنانا (7)

چیک پوائنٹ 5 – متبادل سرگرمی: قابلِ رسائی کراس ورڈ سراغ

اسکرین ریڈر اور کی بورڈ استعمال کرنے والے صارفین نیچے دیے گئے ٹیکسٹ فیلڈز میں کراس ورڈ کے جوابات براہ راست ٹائپ کر سکتے ہیں۔

افقی

2 افقی: ڈیجیٹل شناخت کی توثیق کے لیے استعمال ہونے والے صارف نام، پاس ورڈز اور نجی ٹوکنز (5 حروف):

4 افقی: اکاؤنٹ لاگ اِن کو تحفظ دینے والا اضافی تصدیقی مرحلہ (مثلاً ہارڈ ویئر کیز) (8 حروف):

6 افقی: ذاتی صارف ریکارڈز پر مشتمل نجی ڈیٹابیسز کا غیر مجاز انکشاف (4 حروف):

7 افقی: جعلی قرض درخواستوں کو روکنے کے لیے کریڈٹ فائلوں تک رسائی محدود کرنا (4 حروف):

8 افقی: صارفین کو دھوکے سے اسناد حاصل کرنے کے لیے جعلی پیغامات بھیجنا (4 حروف):

عمودی

1 عمودی: شناخت کی چوری سے بچاؤ کے لیے استعمال ہونے والی تربیت اور تکنیکی کنٹرولز (4 حروف):

3 عمودی: چوری شدہ کارپوریٹ ڈیٹا کے لیے آن لائن فورمز اور ہیکر چینلز کی اسکیننگ (6 حروف):

5 عمودی: جائز ادارے کی نقل کرنے کے لیے جعلی ویب سائٹ یا ای میل بنانا (7 حروف):

چیک پوائنٹ 6: پوشیدہ الفاظ کی تلاش

نیچے گرڈ میں چھپی 8 اہم اصطلاحات تلاش کریں۔ الفاظ افقی، عمودی یا ترچھے ہو سکتے ہیں۔

ع	و	ب	ت	ر	م	ٹ	ف	گ	ٹ	ک	و	د	ی	چ
م	ا	ے	و	گ	ع	ل	ش	د	د	ی	ر	ج	ن	ا
پ	ش	ل	ج	ف	ی	م	ن	ع	ک	ف	ر	ت	ا	ر
ہ	پ	گ	م	ک	ف	م	گ	ک	ن	گ	ج	د	ر	ن
س	ز	ل	س	پ	ب	ا	ب	ر	ا	س	ٹ	و	گ	و
ز	ی	ر	ف	م	ت	س	ا	ہ	ی	ف	س	ز	ن	ر
ل	م	س	ک	ک	د	س	ت	ر	م	ک	د	ف	ا	ع
م	و	ب	ج	ہ	پ	ہ	و	ن	ا	م	ک	ک	چ	د
ے	ع	پ	ی	و	ع	و	ت	ے	ی	ب	ن	د	گ	ا
ی	ب	ل	ف	ف	ن	ت	ک	ت	ف	ع	ج	س	ج	ن
چ	ٹ	ن	ت	گ	ت	ا	س	ت	ا	گ	ع	ا	ب	س
ن	گ	ٹ	و	ع	ن	د	ٹ	ک	ے	م	ن	ت	د	ا
و	ہ	ن	ر	م	ف	ہ	ل	ک	ل	ن	ا	ا	ٹ	ے
ش	ز	ز	ع	ن	ا	ر	ف	ف	ن	ج	ب	ز	ک	پ
ا	ع	چ	م	م	چ	ل	ہ	ش	ش	ر	ن	ک	د	چ

الفاظ کی فہرست

اسناد
لیکس
ایمایفاے
نگرانی
فریز
دفاع
اسپوفنگ
فشنگ

چیک پوائنٹ 6 – متبادل سرگرمی: قابلِ رسائی الفاظ کا ملان

ورڈ سرچ کی 8 اصطلاحات میں سے ہر ایک کو اس کی درست تعریف سے ملائیں اور خالی جگہ میں حرف (A-H) لکھیں۔

اصطلاحات
A. اسناد
B. لیکس
C. ایمایفاے
D. نگرانی
E. فریز
F. دفاع
G. اسپوفنگ
H. فشنگ

تعریفیں اور ملان کے خانے	
1. صارفین کو دھوکے سے اسناد حاصل کرنے کے لیے جعلی پیغامات بھیجنا۔	
2. ڈیجیٹل شناخت کی توثیق کے لیے استعمال ہونے والے صارف نام، پاس ورڈز اور نجی ٹوکنز۔	
3. جائز ادارے کی نقل کرنے کے لیے جعلی ویب سائٹ یا ای میل بنانا۔	
4. شناخت کی چوری سے بچاؤ کے لیے استعمال ہونے والی تربیت اور تکنیکی کنٹرولز۔	
5. چوری شدہ کارپوریٹ ڈیٹا کے لیے آن لائن فورمز اور ہیکر چینلز کی اسکیننگ۔	
6. جعلی قرض درخواستوں کو روکنے کے لیے کریڈٹ فائلوں تک رسائی محدود کرنا۔	
7. ذاتی صارف ریکارڈز پر مشتمل نجی ڈیٹابیسز کا غیر مجاز انکشاف۔	
8. اکاؤنٹ لاگ اِن کو تحفظ دینے والا اضافی تصدیقی مرحلہ (مثلاً ہارڈ ویئر کیز)۔	

چیک پوائنٹ 7: الجھے الفاظ کا چیلنج

سائبر سیکیورٹی کے اہم تصورات اور اصطلاحات ظاہر کرنے کے لیے نیچے دیے گئے حروف کو درست ترتیب میں لائیں۔ اپنے جوابات دیے گئے ان پٹ باکسز میں لکھیں۔

1. ا ن ا د س
2. ا ا ے ی ا ف ی م
3. ز ف ی ر
4. گ س ف و ن ا پ
5. س ل ک ی
6. ن ا ن ر ی گ
7. ا د ع ف
8. ف گ ن ش

اضافی سرگرمی: تیزی سے سوچیں

ہر زمرے کے لیے 3 جوابات لکھیں۔ جو سب سے پہلے فہرست مکمل کرے وہ جیتتا ہے۔

1. شناخت چوری ہونے پر کرنے کے کام
2. وہ چیزیں جو سوشل میڈیا پر شیئر نہیں کرنی چاہئیں
3. وہ چیزیں جن کا آپ بیک اپ لیتے ہیں
4. آپ کے بٹوے میں موجود کارڈز یا شناختی دستاویزات کے نام
5. وہ دستاویزات جن کی حفاظت آپ کو کرنی چاہیے
6. ڈیٹا لیک کے بعد کرنے کے کام
7. سافٹ ویئر اپ ڈیٹ کرنے کی وجوہات
8. وہ معلومات جو شناخت چور چاہتا ہے
9. وہ ڈیوائسز جنہیں ہیک کیا جا سکتا ہے
10. وہ مقامات جہاں سے آپ کا ڈیٹا لیک ہو سکتا ہے
11. محفوظ عادات جو آپ آج شروع کر سکتے ہیں
12. کمپیوٹر کے متاثر ہونے کی علامات
13. اپنی شناخت ثابت کرنے کے طریقے
14. شناخت کی چوری کی علامات
15. ای میل میں انتباہی علامات

چیک پوائنٹ 8: سائبر سیکیورٹی کیس اسٹڈیز

جو تصورات آپ نے سیکھے ہیں انہیں نیچے دیے گئے حقیقی منظرناموں کو حل کرنے میں استعمال کریں۔

کیس اسٹڈی 1: ایگزیکٹو کی شناخت کی نقالی سے تحفظ



منظرنامہ: ایک اعلیٰ سطح کے C-suite ایگزیکٹو کو ایسے ٹائپو اسکواٹڈ ڈومین ناموں کا نشانہ بنایا گیا ہے جو کلائنٹس کو دھوکا دینے کے لیے اس کی ذاتی ای میل کی نقل کرتے ہیں۔ برانڈ پروٹیکشن پلان ڈیزائن کریں۔

بحث کا سوال: برانڈ اسپوفنگ کے خطرات کا تجزیہ کریں، اور SPF/DKIM/DMARC اور تصدیقی کنٹرولز تفصیل سے بیان کریں۔

کیس اسٹڈی 2: ڈارک ویب پر کارپوریٹ کریڈینشلز کا انکشاف



منظرنامہ: ڈارک ویب کے ڈیٹا بیس ڈمپ میں ایک انٹرپرائز کے سسٹم ایڈمنسٹریٹرز کے کئی سو کارپوریٹ کریڈینشلز موجود ہیں۔ خطرے میں کمی کی حکمت عملی ڈیزائن کریں۔

بحث کا سوال: کریڈینشلز کی صفائی کا عمل بیان کریں، اور پاس ورڈ مینیجر کے رول آؤٹ کی منصوبہ بندی کریں۔

چیک پوائنٹ 9: سائفر حل کریں

سائبر سیکیورٹی پیشہ ور نیٹ ورک اثاثوں کو آن لائن خطرات پیدا کرنے والوں سے بچاتا ہے۔ نیچے دی گئی حرف سے عدد کی کلید استعمال کر کے خالی جگہوں میں متعلقہ حروف لکھ کر پیغام ڈی کرپٹ کریں۔

حرف سے عدد خفیہ کاری کی کلید

ا=1 ب=2 پ=3 ت=4 ٹ=5 ث=6 ج=7 چ=8 ح=9 خ=10 د=11 ڈ=12 ذ=13

ر=14 ڑ=15 ز=16 ژ=17 س=18 ش=19 ص=20 ض=21 ط=22 ظ=23 ع=24 غ=25 ف=26

ق=27 ک=28 گ=29 ل=30 م=31 ن=32 ں=33 و=34 ہ=35 ھ=36 ی=37 ے=38 ئ=39

14	5	28	37	26		37	5	30	31		4	10	1	32	19
23	34	26	9	31		38	18		27	37	11	20	4		

ڈی کوڈ شدہ پیغام:

ٹپ: ہر نمبر اوپر دی گئی کلید کے ایک اردو حرف کو ظاہر کرتا ہے۔

چیک پوائنٹ 10: سائبر سیکیورٹی عمومی سوالات – بنیادی (حصہ A)

آن لائن خطرات کی روک تھام کے بارے میں عام سوالات اور جوابات کا جائزہ لیں۔

Q1: شناختی چوری کیا ہے؟

جرم جس میں حملہ آور مالی فائدے کے لیے کسی اور کی نقالی کرنے کے واسطے ذاتی ریکارڈ (جیسے پاس ورڈز یا SSNs) چراتا ہے۔

Q2: شناختی چوری کی سب سے عام وجہ کیا ہے؟

فشنگ پاس ورڈز چرانے کا ایک نمایاں طریقہ ہے، جس میں صارفین کو جعلی، اسپوف شدہ ویب سائٹس پر لے جایا جاتا ہے۔

Q3: ملٹی فیکٹر تصدیق (MFA) شناختوں کا تحفظ کیسے کرتی ہے؟

MFA لاگ اِن کے لیے ایک اضافی ثبوت (جیسے ہارڈ ویئر کی) مانگتا ہے، جو آپ کا پاس ورڈ چرانے کے باوجود حملہ آوروں کو روکتا ہے۔

Q4: کریڈٹ فریز کیا ہے؟

مفت سروس جو کریڈٹ بیورو کو آپ کی کریڈٹ فائل شیئر کرنے سے روکتی ہے اور چوروں کو آپ کے نام پر نئے قرضے لینے سے باز رکھتی ہے۔ [2]

Q5: ڈارک ویب مانیٹرنگ کیا ہے؟

ایسا سافٹ ویئر جو ہیکر فورمز میں لیک ہونے والی ای میلز، پاس ورڈز اور ذاتی ریکارڈز کو چیک کرتا ہے، اور آپ کا ڈیٹا ظاہر ہونے پر آپ کو الرٹ کرتا ہے۔

چیک پوائنٹ 10: سائبر سیکیورٹی عمومی سوالات – بنیادی (حصہ B)

آن لائن خطرات کی روک تھام کے بارے میں عام سوالات اور جوابات کا جائزہ لیں۔

Q6: کریڈینشل اسٹفنگ کا کیا مطلب ہے؟

خودکار بوٹس جو لیک شدہ پاس ورڈ فہرستوں کو سینکڑوں ویب سائٹس پر آزما کر فعال اکاؤنٹس پر قبضہ کر لیتے ہیں۔

Q7: ای میل اسپوفنگ خطرناک کیوں ہے؟

یہ حملہ آوروں کو ای میلز میں بھیجنے والے کا نام جعلی بنانے دیتا ہے، جس سے فشنگ پیغامات قابل اعتماد ساتھیوں کی طرف سے آئے ہوئے لگتے ہیں۔

Q8: پاس ورڈ مینیجرز شناخت کی چوری کو کیسے روکتے ہیں؟

وہ ہر اکاؤنٹ کے لیے پیچیدہ، منفرد پاس ورڈز محفوظ کرتے ہیں اور جعلی فشنگ ڈومینز پر اسناد خود بخود بھرنے سے انکار کرتے ہیں۔

Q9: اسپیئر فشنگ کیا ہے؟

انتہائی ہدف شدہ فشنگ حملہ جو دھوکے کا امکان بڑھانے کے لیے شکار کے نام اور تفصیلات کے مطابق تیار کیا جاتا ہے۔

Q10: کریڈٹ الرٹ فریز سے کیسے مختلف ہے؟

الرٹ قرض دہندگان کو اکاؤنٹ کھولنے سے پہلے آپ کی شناخت کی تصدیق کا کہتا ہے، جبکہ فریز آپ کی کریڈٹ فائل تک رسائی مکمل طور پر بلاک کر دیتا ہے۔ [2]

چیک پوائنٹ 10: سیکیورٹی عمومی سوالات – اعلیٰ (حصہ C)

سیکیورٹی فریم ورکس، میل ویئر تجزیے اور ڈیٹا کمپلائنس کے جدید تکنیکی پہلوؤں کا جائزہ لیں۔

Q1: SIM سوئپنگ شناختی چوری تک کیسے لے جاتی ہے؟

حملہ آور کیریئر کے عملے کو قائل کر کے شکار کا فون نمبر نئے SIM کارڈ پر منتقل کرا لیتے ہیں اور SMS پر مبنی 2FA کوڈز ہتھیا لیتے ہیں۔

Q2: شناختی چوری روکنے میں DMARC کا کیا کردار ہے؟

DMARC ڈومین مالکان کو جعلی ای میلز کو ان باکس تک پہنچنے سے روکنے کی سہولت دیتا ہے، جس سے کارپوریٹ ڈومینز کی نقل کرنے والی جعلی ای میلز رک جاتی ہیں۔

Q3: مصنوعی شناخت کی چوری کا پتا لگانا مشکل کیوں ہے؟

چور اصلی SSNs کو جعلی ناموں اور تاریخِ پیدائش کے ساتھ ملا کر بالکل نئے کریڈٹ پروفائلز بناتے ہیں، جس سے بنیادی فراڈ الرٹس بائی پاس ہو جاتے ہیں۔

Q4: ڈیٹا بروکرز ذاتی شناختوں کا کیسے استحصال کرتے ہیں؟

بروکرز عوامی ریکارڈز، ویب رویے اور خریداری کی ہسٹری جمع کر کے پروفائل ڈوزیئر بناتے ہیں، جو لیک یا فروخت ہو سکتے ہیں۔

Q5: SMS پر مبنی MFA کو کمزور کیوں سمجھا جاتا ہے؟

SMS ٹریفک مداخلت، فشنگ، اور کیریئر سطح کے SIM سوپنگ ایکسپلائٹس کے لیے کمزور ہوتا ہے۔

چیک پوائنٹ 10: سیکیورٹی عمومی سوالات – اعلیٰ (حصہ D)

سیکیورٹی فریم ورکس، میل ویئر تجزیے اور ڈیٹا کمپلائنس کے جدید تکنیکی پہلوؤں کا جائزہ لیں۔

Q6: کریڈٹ فائل لاک کیا ہے؟

فریز سے ملتی جلتی تجارتی سروس جو صارفین کو موبائل ایپ کے ذریعے اپنی کریڈٹ فائل فوراً کھولنے یا لاک کرنے دیتی ہے۔

Q7: کارپوریٹ ڈیٹا کی خلاف ورزیاں شناخت کی چوری کو کیسے ہوا دیتی ہیں؟

لیک شدہ ڈیٹابیس لاکھوں سادہ اسناد ظاہر کر دیتے ہیں، جس سے چوروں کو ہدفی شناختی فراڈ کے لیے درکار خام ڈیٹا مل جاتا ہے۔

Q8: سوشل میڈیا پر حد سے زیادہ معلومات شیئر کرنے کا کیا خطرہ ہے؟

پالتو جانوروں کے نام، جائے پیدائش اور والدہ کا پیدائشی خاندانی نام عوامی طور پر شیئر کرنا چوروں کو اکاؤنٹ ریکوری کے عام سوالات کے جوابات دے دیتا ہے۔

Q9: بائیو میٹرک لاگ ان شناختی پروفائلز کا تحفظ کیسے کرتے ہیں؟

بایومیٹرکس لاگ اِن کو انگلیوں کے نشان یا چہرے جیسی خصوصیات سے جوڑتے ہیں؛ ڈیوائس پر رکھے جائیں تو انہیں چرانا مشکل ہوتا ہے، لیکن محفوظ شدہ بایومیٹرک ڈیٹا لیک ہو سکتا ہے۔

Q10: Red Flags Rule شناختی چوری کا مقابلہ کیسے کرتا ہے؟

وفاقی ضابطہ جو مالیاتی اداروں سے شناخت کی چوری کی انتباہی علامات کا پتا لگانے اور ان کا جواب دینے کے لیے تحریری پروگرام بنانے کا تقاضا کرتا ہے۔

حصہ 11: 10 حقیقی دنیا کے سائبر سیکیورٹی حقائق اور بصیرتیں

سیکیورٹی خلاف ورزیوں، دفاعی نظاموں اور تعمیل کے معیارات کے بارے میں حقیقی دنیا کے حقائق کا جائزہ لیں۔

1. سیکیورٹی بصیرت

FTC کی چلائی جانے والی IdentityTheft.gov امریکی متاثرین کو شناخت کی چوری کی اطلاع دینے اور ذاتی بحالی کا منصوبہ حاصل کرنے کی سہولت دیتی ہے۔ [1]

2. سیکیورٹی بصیرت

ہارڈ ویئر سیکیورٹی کیز فشنگ کے خلاف مزاحم MFA ہیں، جو CISA کی تاکید کردہ MFA کی سب سے مضبوط قسم ہے۔ [4]

3. سیکیورٹی بصیرت

سمجھوتا شدہ پاس ورڈز ڈیٹا کی خلاف ورزیوں میں داخلے کا عام راستہ ہیں، جو بعد میں شناخت کے فراڈ کو ہوا دیتے ہیں۔

4. سیکیورٹی بصیرت

وفاقی قانون کے تحت کریڈٹ فریز مفت ہے، اور کھولنے تک قرض دہندگان کو کریڈٹ فائلیں دیکھنے سے روکتا ہے۔ [2]

5. سیکیورٹی بصیرت

DMARC ڈومین مالکان کو میل سرورز سے یہ کہنے دیتا ہے کہ جانچ میں ناکام جعلی ای میل کو مسترد یا قرنطینہ کریں۔ [7]

6. سیکیورٹی بصیرت

SIM سویپنگ ہیکرز کو بینکنگ پورٹلز پر SMS پر مبنی دو مرحلہ تصدیق بائی پاس کرنے کی اجازت دیتی ہے۔

7. سیکیورٹی کی بصیرت

مصنوعی شناخت کا فراڈ اصلی اور جعلی تفصیلات کو ملاتا ہے، جس سے قرض دہندگان کے لیے اس کا پتا لگانا مشکل ہو جاتا ہے۔

8. سیکیورٹی کی بصیرت

بہت سے لوگ آن لائن اکاؤنٹس میں ایک ہی پاس ورڈ دوبارہ استعمال کرتے ہیں، اس لیے ایک خلاف ورزی کئی اکاؤنٹس کو بے نقاب کر سکتی ہے۔

9. سیکیورٹی کی بصیرت

ڈیٹا بروکرز بڑی تعداد میں صارفین کے تفصیلی ریکارڈ مرتب کرتے ہیں، جس سے رازداری کا مرتکز خطرہ پیدا ہوتا ہے۔

10. سیکیورٹی بصیرت

شناخت کی چوری سے بحالی میں مہینوں کا کام لگ سکتا ہے، جیسے ادائیگیوں پر اعتراض اور کریڈٹ رپورٹس کی درستگی۔

تکنیکی حوالہ جات اور ماخذ

مطالعاتی گائیڈ اور انٹرایکٹو پہیلیاں عالمی NIST، OWASP اور ڈیٹا پرائیویسی کمپلائنس معیارات سے مرتب کی گئی ہیں۔

علمی اور صنعتی حوالہ جات

[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

جوابی کلید: چیک پوائنٹ 1 – کثیر انتخابی

1 سوال 1

درست جواب: A

تدریسی نوٹ

شناخت چور لاگ اِن اسناد چرانے کے لیے کون سا بنیادی طریقہ استعمال کرتے ہیں؟ → جعلی ای میل الرٹس بھیجنا جو صارفین کو جعلی پورٹلز پر پاس ورڈ درج کرنے پر بہکاتے ہیں

2 سوال 2

درست جواب: A

تدریسی نوٹ

کون سا سیکیورٹی کنٹرول اسناد کے لیکس کے خلاف سب سے مضبوط دفاع فراہم کرتا ہے؟ → ہارڈ ویئر کیز کے ساتھ ملٹی فیکٹر تصدیق

3 سوال 3

درست جواب: A

تدریسی نوٹ

کریڈٹ فریزنگ کی نمائندگی کیا کرتا ہے؟ → غیر مجاز قرضے لینے سے چوروں کو روکنے کے لیے کریڈٹ رپورٹس کو لاک کرنا

4 سوال 4

درست جواب: A

تدریسی نوٹ

ڈارک ویب مانیٹرنگ کیوں مفید ہے؟ → اگر صارفین کی لیک شدہ اسناد غیر قانونی ڈیٹا بیسز میں ظاہر ہوں تو یہ انہیں خبردار کرتا ہے

5 سوال 5

درست جواب: A

تدریسی نوٹ

سوشل انجینئرنگ کا کیا مطلب ہے؟ → لوگوں کو بہلا کر ان سے رضاکارانہ طور پر خفیہ اسناد ظاہر کروانا

جوابی کلید: چیک پوائنٹ 2 – درست یا غلط

6 سوال 6

درست جواب: غلط

تدریسی نوٹ

شناخت کی چوری آف لائن بھی شروع ہو سکتی ہے، جیسے چوری شدہ ڈاک یا دستاویزات۔

7 سوال 7

درست جواب: درست

تدریسی نوٹ

تمام ذاتی اکاؤنٹس پر MFA نافذ کرنا زیادہ تر کریڈینشل اسٹفنگ بوٹ حملوں کو روکتا ہے۔

8 سوال 8

درست جواب: غلط

تدریسی نوٹ

کریڈٹ فریز نئی کریڈٹ جانچ کو روکتا ہے لیکن آپ کے موجودہ اکاؤنٹس پر اثر نہیں ڈالتا۔

9 سوال 9

درست جواب: درست

تدریسی نوٹ

پاس ورڈ مینیجر جعلی ڈومینز پر پاس ورڈز خود بخود بھرنے سے انکار کر کے صارفین کو فشنگ سے بچاتے ہیں۔

10 سوال 10

درست جواب: درست

تدریسی نوٹ

فشنگ ای میلز اکثر جذباتی اور جلد بازی والے ردعمل کو ابھارنے کے لیے فوری نوعیت کی زبان استعمال کرتی ہیں۔

الفاظ کی کلید اور درجہ بندی کا معیار

استاد کی گریڈنگ روبرک: ہر درست ملان (کل 8 نمبر) اور سیاقی اصطلاح (کل 6 نمبر) کے لیے 1 نمبر دیں۔

چیک پوائنٹ 4: جوابی کلید – تصورات کا ملان

H 1. کریڈینشلز	D 2. لیکس	A 3. MFA	G 4. نگرانی
C 5. منجمد کرنا	E 6. دفاع	B 7. اسپوفنگ	F 8. فشنگ

چیک پوائنٹ 3: جوابی کلید – اہم اصطلاحات

1 اسناد	2 لیکس	3 ایم ایف اے	4 نگرانی
5 فریز	6 دفاع		

چیک پوائنٹ 6 – متبادل سرگرمی: جوابی کلید – الفاظ کا ملان

1 H – فشنگ	2 A – اسناد	3 G – اسپوفنگ	4 F – دفاع
5 D – نگرانی	6 E – فریز	7 B – لیکس	8 C – ایمایفاے

اساتذہ کے لیے بحث کے نوٹس

اہم اصطلاحات:
یقینی بنائیں کہ طلبہ کریڈینشلز، لیکس اور MFA کو اپنے الفاظ میں سمجھا سکیں اور ہر ایک کی مثال دے سکیں۔

کیس اسٹڈیز:
طلبہ سے کہیں کہ اپنی سفارشات کو ورک شیٹ کے حقائق پر مبنی رکھیں، ذاتی رائے پر نہیں۔

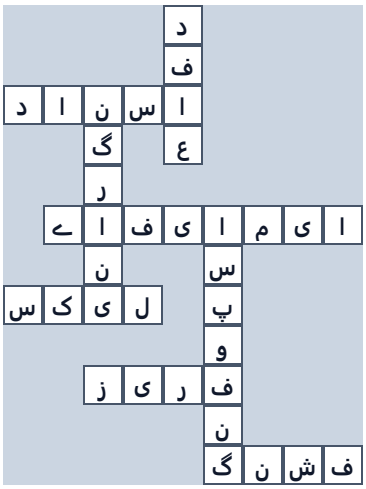
ماخذ کی جانچ:
طلبہ سے کہیں کہ ورک شیٹ کے ماخذ میں کم از کم ایک دعوے کی تصدیق کریں، اور اس پر بات کریں کہ اعداد و شمار، قیمتیں اور قواعد وقت کے ساتھ کیوں بدل سکتے ہیں۔

پہیلیوں کی کلیدیں اور استاد کے نوٹس

الفاظ کی تلاش کا حل

چ	ی	د	و	ک	ٹ	گ	ف	ٹ	م	ر	ت	ب	و	ع
ا	ن	چ	ر	ی	د	د	ش	ل	ع	گ	و	ے	ا	م
ر	ا	ت	ر	ف	ک	ع	ن	ی	م	ف	چ	ل	ش	پ
ن	ر	د	چ	گ	ن	ک	گ	م	ف	ک	م	گ	پ	ہ
و	گ	و	ٹ	س	ا	ر	ب	ا	پ	س	ل	ز	س	
ر	ن	ز	س	ف	ی	ہ	ا	س	ت	م	ف	ر	ی	ز
ع	ا	ف	د	ک	م	ر	ت	س	د	ک	ک	س	م	ل
د	چ	ک	ک	م	ا	ن	و	ہ	پ	ہ	چ	ب	و	م
ا	گ	د	ن	ب	ی	ے	و	ع	ت	و	ی	پ	ع	ے
ن	چ	س	ج	ع	ف	ت	ک	ت	ن	ف	ف	ل	ب	ی
س	ب	ا	ع	گ	ا	ت	س	ا	گ	ت	ن	ٹ	چ	
ا	د	ت	ن	م	ے	ک	ٹ	د	ن	ع	و	ٹ	گ	ن
ے	ٹ	ا	ن	ل	ک	ل	ہ	ف	م	ر	ن	ہ	و	
پ	ک	ز	ب	چ	ن	ف	ف	ر	ا	ن	ع	ز	ز	ش
چ	د	ک	ن	ر	ش	ش	ہ	ل	ج	م	م	ع	ج	ا

کراس ورڈ کا حل



کراس ورڈ حل کے لیے استاد کی گائیڈ

افقی

2 افقی: اسناد ڈیجیٹل شناخت کی توثیق کے لیے استعمال ہونے والے صارف نام، پاس ورڈز اور نجی ٹوکنز (5 حروف)

4 افقی: ایمایفاے اکاؤنٹ لاگ اِن کو تحفظ دینے والا اضافی تصدیقی مرحلہ (مثلاً ہارڈ ویئر کیز) (8 حروف)

6 افقی: لیکس ذاتی صارف ریکارڈز پر مشتمل نجی ڈیٹابیسز کا غیر مجاز انکشاف (4 حروف)

7 افقی: فریز جعلی قرض درخواستوں کو روکنے کے لیے کریڈٹ فائلوں تک رسائی محدود کرنا (4 حروف)

8 افقی: فشنگ صارفین کو دھوکے سے اسناد حاصل کرنے کے لیے جعلی پیغامات بھیجنا (4 حروف)

عمودی

1 عمودی: دفاع شناخت کی چوری سے بچاؤ کے لیے استعمال ہونے والی تربیت اور تکنیکی کنٹرولز (4 حروف)

3 عمودی: نگرانی چوری شدہ کارپوریٹ ڈیٹا کے لیے آن لائن فورمز اور پیکر چینلز کی اسکیننگ (6 حروف)

5 عمودی: اسپوفنگ جائز ادارے کی نقل کرنے کے لیے جعلی ویب سائٹ یا ای میل بنانا (7 حروف)

الفاظ کی ترتیب اور سائفر حل کی کلید

الفاظ کی ترتیب درست کرنے کی سرگرمی اور Secret Cipher Challenge کی گریڈنگ کلید۔

الفاظ کی ترتیب درست کرنے کی کلید

1. انادس — اسناد
2. االےیافیم — ایمایفاے
3. زفیر — فریز
4. گسفوناپ — اسپوفنگ
5. سلکی — لیکس
6. نانریگ — نگرانی
7. ادعف — دفاع
8. فگنش — فشنگ

خفیہ سائفر چیلنج کی کلید

"شناخت ملٹی فیکٹر تصدیق سے محفوظ"

کیس اسٹڈیز کی جوابی کلید

A کیس اسٹڈی 1: ایگزیکٹو کی شناخت کی نقالی سے تحفظ

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: ایک اعلیٰ سطح کے سی-سویٹ ایگزیکٹو کو ٹائپو اسکواٹڈ ڈومین ناموں سے نشانہ بنایا گیا ہے جو کلائنٹس کو دھوکہ دینے کے لیے اس کی ذاتی ای میل کی نقل کرتے ہیں۔ برانڈ تحفظ کا منصوبہ ڈیزائن کریں۔
- تجویز کردہ حکمت عملی اور حل: ایگزیکٹو کے نام کے تمام عام ہجے والے مختلف روپ رجسٹر کریں۔ ڈومین اسپوفنگ روکنے کے لیے ای میل تصدیقی پروٹوکولز (DMARC, DKIM, SPF) نافذ کریں۔ تمام سی-سویٹ کارپوریٹ لاگ اِنز پر ہارڈ ویئر MFA لازمی کریں۔

B کیس اسٹڈی 2: ڈارک ویب پر کارپوریٹ کریڈینشلز کا انکشاف

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: ڈارک ویب ڈیٹا بیس ڈمپ میں ایک انٹرپرائز کے سسٹم ایڈمنسٹریٹرز کی کئی سو کارپوریٹ اسناد شامل ہیں۔ تدارک کی حکمت عملی ڈیزائن کریں۔
- تجویز کردہ حکمت عملی اور حل: پوری کمپنی کے پاس ورڈز ری سیٹ کریں۔ انٹرپرائز پاس ورڈ مینیجر کا استعمال لازمی قرار دیں۔ تمام سسٹم پورٹلز پر MFA نافذ کریں اور مسلسل خودکار ڈارک ویب مانیٹرنگ الرٹس ترتیب دیں۔