نام: _____ تاریخ: _____ نمبر: _____

فشنگ حملے اور سوشل انجینئرنگ

اسپیئر فشنگ، وہیلنگ فراڈ، SPF/DKIM/DMARC پروٹوکولز، بھیجنے والے کی اسپوفنگ، اور ملازمین کی سیکیورٹی تربیت۔

فشنگ حملے سیکھنے کا 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 فشنگ حملوں اور سوشل انجینئرنگ سے متعارف کراتا ہے۔ آپ اسپیئر فشنگ، وہیلنگ، ڈومین اسپوفنگ، SPF/DKIM/DMARC پروٹوکولز، لنک کی حفاظت، اور ملازمین کی آگاہی کی تربیت 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/phishing-attacks/

آپ کی فشنگ سے بچاؤ کا لرننگ روڈ میپ

- عام فشنگ، وشنگ اور سپورٹ پاپ اپ اسکیمز کی نشاندہی کریں۔
- آؤٹ آف بینڈ لین دین کی تصدیق کے طریقہ کار نافذ کریں۔
- جعلی ڈومینز کو بلاک کرنے کے لیے SPF، DKIM اور DMARC کے قواعد ترتیب دیں۔

فشنگ حملے گائیڈ 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 ای میل کی تصدیق پر لاگو کریں۔ اور آخر میں اضافی سرگرمی "تیزی سے سوچیں"۔

فشنگ حملے اور سوشل انجینئرنگ (تعارف)

فشنگ حملے صارفین کی لاگ اِن اسناد حاصل کرنے کے لیے ہدفی پیغامات، وہیلنگ اسکیمز اور ڈومین اسپوفنگ استعمال کرتے ہیں۔ کارپوریٹ سسٹمز کو محفوظ بنانے کے لیے گیٹ وے پر SPF، DKIM اور DMARC قواعد کے ساتھ آؤٹ آف بینڈ منظوری کے مراحل نافذ کرنا ضروری ہے۔

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

چیک پوائنٹ 1: کثیر انتخابی چیلنج

1 1. اسپیئر فشنگ کیا ہے؟

- A. ہدف شدہ فشنگ ای میل جو کسی مخصوص فرد یا ادارے کے مطابق تیار کی گئی ہو
- B. لاکھوں بے ترتیب پتوں کو بھیجی جانے والی وسیع پیمانے کی ای میل
- C. نیٹ ورک حملہ جو ویب سرورز کو ٹریفک سے بھر دیتا ہے
- D. صارف کے ریکارڈز کو نشانہ بنانے والی ڈیٹا بیس نکالنے کی تکنیک

2 2. کون سا پروٹوکول کسی ڈومین کو اسپوفنگ کا مقابلہ کرنے کے لیے DNS میں اپنے مجاز بھیجنے والے IP ایڈریسز درج کرنے دیتا ہے؟

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

3 3. وہیلنگ حملہ کیا ہے؟

- A. فشنگ مہم جو خاص طور پر نمایاں کارپوریٹ ایگزیکٹوز کو نشانہ بناتی ہے
- B. ڈیٹا بیس بیک اپس کو نشانہ بنانے والا SQL انجیکشن حملہ
- C. مقامی ایریا نیٹ ورک راؤٹر کے سازوسامان کی فزیکل چوری
- D. ایک خودکار کریڈینشل اسٹفنگ بروٹ فورس اسکین

4 4. DKIM کیا کرتا ہے؟

- A. بھیجنے والے کی صداقت جانچنے کے لیے ای میلز میں خفیہ کاری پر مبنی دستخط شامل کرتا ہے
- B. فائر وال پر آنے والے نیٹ ورک پیکٹ ٹریفک کو روکتا ہے
- C. ڈیٹا بیس اسٹوریج والیومز کو ساکن حالت میں خفیہ کرتا ہے
- D. دستخط پر مبنی میل ویئر کے لیے ای میل منسلکات کو اسکین کرتا ہے

5 5. DMARC کا کردار کیا ہے؟

- A. وصول کرنے والے ای میل سرورز کو ہدایت دینا کہ ناکام SPF/DKIM جانچ سے کیسے نمٹیں
- B. پہلے سے تیار شدہ رینبو ٹیبلز کے ذریعے سسٹم پاس ورڈز کو ڈی کرپٹ کرنا
- C. ترسیل سے پہلے ای میل اٹیچمنٹس کو کمپریس کرنا
- D. نیٹ ورک روٹنگ رسائی کے استحقاق کی ترتیب

چیک پوائنٹ 2: درست یا غلط چیلنج

6 سوال 6

6. اسپیئر فشنگ لاکھوں بے ترتیب ایڈریسز کو بھیجی جانے والی عام بلک ای میلز پر انحصار کرتی ہے۔

○ درست ○ غلط

7 سوال 7

7. DMARC پالیسیاں میل سرورز کو غیر مجاز جعلی پیغامات مسترد کرنے کی ہدایت دے سکتی ہیں۔

○ درست ○ غلط

8 سوال 8

8. SPF کی تصدیق ای میل کی باڈی کے کرپٹوگرافک سگنیچر کی توثیق سے کام کرتی ہے۔

○ درست ○ غلط

9 سوال 9

9. وہیلنگ حملے ڈیٹا بیس فائلوں تک رسائی کے لیے کارپوریٹ کے نچلی سطح کے منتظمین کو نشانہ بناتے ہیں۔

○ درست ○ غلط

10 سوال 10

10. ادائیگی کی درخواستوں کی آؤٹ آف بینڈ تصدیق مالیاتی وائر ٹرانسفر فراڈ کو روکنے میں مدد دیتی ہے۔

○ 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. ذاتی معلومات کے ساتھ کسی مخصوص ملازم کو نشانہ بنانا _____ فشنگ ہے۔
2. پیغامات کو جائز ظاہر کرنے کے لیے ای میل ہیڈر میں جعل سازی بھیجنے والے کی _____ ہے۔
3. مجاز میل سرور IPs کی DNS ریکارڈ فہرست _____ ہے۔
4. بھیجنے والے کی تصدیق فراہم کرنے والا ای میل دستخطی معیار _____ ہے۔
5. ناکام SPF/DKIM جانچوں کو مسترد کرنے کی پالیسیاں _____ سے قائم کی جاتی ہیں۔
6. سی لیول ایگزیکٹوز کو نشانہ بنانے والی فشنگ مہم _____ کہلاتی ہے۔

الفاظ کا بینک

اسپوفنگ | اسپیئر | اسمشنگ | ایس پی ایف | ڈی کے آئی ایم | ڈی مارک | وشنگ | وہیلنگ

اپنے جوابات یہاں لکھیں:

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

چیک پوائنٹ 4: سیکیورٹی تصورات کا ملان

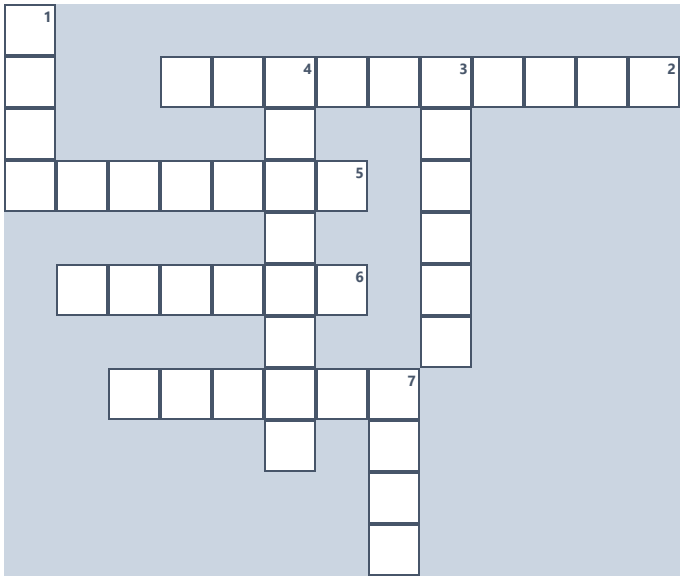
تعریفوں کا ملان

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. اسپیئر	A	آواز پر مبنی دھوکے کی کالز۔
2. اسپوفنگ	B	C-level ایگزیکٹوز کو نشانہ بنانا۔
3. SPF	C	پالیسی مسترد کرنے کی ہدایات۔
4. DKIM	D	DNS کے مجاز بھیجنے والے IPs۔
5. DMARC	E	سوشل انجینئرنگ ای میل۔
6. وہیلنگ	F	ذاتی نوعیت کی ہدفی ای میل۔
7. فشنگ	G	بھیجنے والے کے ای میل ایڈریس کی جعل سازی۔
8. وشنگ	H	ای میل میں کرپٹوگرافک دستخط۔

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. ای میل میں کرپٹوگرافک دستخط (10)

5. بھیجنے والے کا ای میل ایڈریس جعلی بنانا (7)

6. مسترد کرنے کی ہدایات والی پالیسی (6)

7. سی لیول ایگزیکٹوز کو ہدف بنانا (6)

عمودی

1. سوشل انجینئرنگ پر مبنی ای میل (4)

3. ذاتی نوعیت کی ہدف شدہ ای میل (6)

4. DNS میں مجاز بھیجنے والے IPs کی فہرست (8)

7. صوتی کالز پر مبنی فراڈ (4)

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: ای میل میں کرپٹوگرافک دستخط (10 حروف):

5 افقی: بھیجنے والے کا ای میل ایڈریس جعلی بنانا (7 حروف):

6 افقی: مسترد کرنے کی ہدایات والی پالیسی (6 حروف):

7 افقی: سی لیول ایگزیکٹوز کو ہدف بنانا (6 حروف):

عمودی

1 عمودی: سوشل انجینئرنگ پر مبنی ای میل (4 حروف):

3 عمودی: ذاتی نوعیت کی ہدف شدہ ای میل (6 حروف):

4 عمودی: DNS میں مجاز بھیجنے والے IPs کی فہرست (8 حروف):

7 عمودی: صوتی کالز پر مبنی فراڈ (4 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۔

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

الفاظ کی فہرست

اسپیئر
اسپوفنگ
ایسپیایف
ڈیکےائیایم
ڈیمارک
وہیلنگ
فشنگ
وشنگ

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. اسپیئر
B. اسپوفنگ
C. ایسپیایف
D. ڈیکےائیایم
E. ڈیمارک
F. وہیلنگ
G. فشنگ
H. وشنگ

تعریفیں اور ملان کے خانے
1. بھیجنے والے کا ای میل ایڈریس جعلی بنانا۔
2. ذاتی نوعیت کی ہدف شدہ ای میل۔
3. صوتی کالز پر مبنی فراڈ۔
4. DNS میں مجاز بھیجنے والے IPs کی فہرست۔
5. سوشل انجینئرنگ پر مبنی ای میل۔
6. مسترد کرنے کی ہدایات والی پالیسی۔
7. ای میل میں کرپٹوگرافک دستخط۔
8. سی لیول ایگزیکٹوز کو ہدف بنانا۔

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. پ ا ی ئ ر س _____
2. پ ا ف ی ی ا ی س _____
3. ڈ م ا ک ر ی _____
4. گ ن ف ش _____
5. ف گ و پ ا ن س _____
6. ی ا ے ی ا ڈ ی ئ م ک _____
7. ن و ل گ ی ہ _____
8. و 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	وہ ڈیوائسز جنہیں ہیک کیا جا سکتا ہے			
2	فشنگ ای میل کی علامات			
3	کمپیوٹر کے متاثر ہونے کی علامات			
4	وہ الفاظ جو جھوٹی جلد بازی پیدا کرتے ہیں			
5	بھیجنے والے کی تصدیق کرنے کے طریقے			
6	وہ لوگ جن سے آپ آئی ٹی مدد مانگ سکتے ہیں			
7	وہ چیزیں جن کا آپ بیک اپ لیتے ہیں			
8	آپ کی جانی پہچانی مچھلیوں یا سمندری مخلوقات کے نام			
9	وہ کمپنیاں جن کا روپ دھار کر فراڈ کرنے والے دھوکا دیتے ہیں			
10	محفوظ عادات جو آپ آج شروع کر سکتے ہیں			
11	جعلی لنک پر کلک کرنے کے بعد کرنے کے کام			
12	ڈیٹا لیک کے بعد کرنے کے کام			
13	وہ ذرائع جہاں فشنگ ہوتی ہے			
14	وہ چیزیں جو آپ کو کبھی ای میل سے نہیں بھیجنی چاہئیں			
15	اپنے اکاؤنٹس کو محفوظ رکھنے کے طریقے			

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: اعلیٰ ایگزیکٹو کو نشانہ بنانے والے وہیلنگ حملے کا ازالہ



منظرنامہ: ایک چیف فنانشل آفیسر کو نہایت ذاتی نوعیت کی ای میل موصول ہوتی ہے جس میں CEO کی جانب سے ہونے کا دعویٰ کیا گیا ہے اور ایک خفیہ ڈومین خریداری مکمل کرنے کے لیے فوری $50,000 کی وائر ادائیگی کی درخواست ہے۔

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

کیس اسٹڈی 2: SPF/DKIM/DMARC گیٹ وے پالیسیاں نافذ کرنا



منظرنامہ: ایک انٹرپرائز سیکیورٹی آڈٹس میں ناکام ہو رہا ہے کیونکہ آؤٹ باؤنڈ مارکیٹنگ ای میلز اکثر اسپیم قرار دی جاتی ہیں، اور ہیکرز کمپنی کے برانڈ ڈومین کی فعال طور پر نقل کر رہے ہیں۔

بحث کا سوال: ای میل کی صداقت کی تصدیق کے لیے تکنیکی اور انتظامی کنٹرولز قائم 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

29	32	14	39	32	37	7	32	1		30	19	34	18		38	18		5	12	1

33	37	32	1	8	35	3

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: فشنگ کیا ہے؟

فشنگ ایک سوشل انجینئرنگ حملہ ہے جس میں مجرم صارفین کو حساس ڈیٹا شیئر کرنے پر آمادہ کرنے کے لیے جعلی پیغامات بھیجتے ہیں۔

Q2: فشنگ اور اسپیئر فشنگ میں کیا فرق ہے؟

فشنگ عمومی مواد کے ساتھ وسیع گروہوں کو نشانہ بناتی ہے، جبکہ اسپیئر فشنگ حسبِ ضرورت تفصیلات کے ذریعے مخصوص متاثرین کو نشانہ بناتی ہے۔

Q3: وہیلنگ کیا ہے؟

وہیلنگ ایک انتہائی ہدف شدہ فشنگ حملہ ہے جو انتظامی اختیارات رکھنے والے اعلیٰ سطح کے ایگزیکٹوز کو نشانہ بناتا ہے۔

Q4: ای میل اسپوفنگ کیا ہے؟

ای میل اسپوفنگ جعلی بھیجنے والے ایڈریس کے ساتھ ای میل پیغامات بنانا ہے تاکہ وصول کنندہ کو ماخذ پر بھروسا کرنے کے لیے دھوکا دیا جائے۔

Q5: SPF اسپوفنگ کو کیسے روکتا ہے؟

یہ DNS میں مجاز بھیجنے والے IP ایڈریسز کی فہرست شائع کرتا ہے، جس سے وصول کنندہ سرورز میل کے ماخذ کی تصدیق کر سکتے ہیں۔ [1]

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: DKIM کیا ہے؟

DomainKeys Identified Mail ای میل ہیڈرز میں ایک خفیہ کاری دستخط شامل کرتا ہے، جو ثابت کرتا ہے کہ ڈومین نے ذمہ داری لی اور پیغام میں ردوبدل نہیں ہوا۔

Q7: DMARC کا مطلب کیا ہے؟

ڈومین پر مبنی میسج تصدیق، رپورٹنگ، اور مطابقت۔ [2]

Q8: DMARC پالیسی کیا ہے؟

پالیسی جو میل سرورز کو بتاتی ہے کہ SPF/DKIM میں ناکام پیغامات سے کیسے نمٹنا ہے (none، quarantine یا reject)۔ [2]

Q9: وشنگ کیا ہے؟

وائس فشنگ، جس میں حملہ آور جعلی فون کالز کے ذریعے انتظامی یا مالی معلومات حاصل کرتے ہیں۔

Q10: لنک اسکینرز کیسے مدد کرتے ہیں؟

وہ آنے والی ای میلز کے لنکس کو اسکین کر کے دوبارہ لکھتے ہیں تاکہ کلک کے وقت منزل کے ویب صفحات کی سلامتی کی تصدیق ہو سکے۔

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: ہومو گراف حملہ کیسے کام کرتا ہے؟

حملہ آور ملتے جلتے غیر ASCII یونیکوڈ حروف سے ڈومین نام رجسٹر کرتے ہیں تاکہ وہ دیکھنے میں کسی اصل ڈومین نام جیسا لگے۔

Q2: پیونی کوڈ نمائندگی کیا ہے؟

انکوڈنگ جو یونیکوڈ ڈومین ناموں کو 'xn--' سے شروع ہونے والی ASCII سے ہم آہنگ لڑیوں میں بدلتی ہے تاکہ DNS انہیں سنبھال سکے۔

Q3: 'p=reject' سب سے محفوظ DMARC حالت کیوں ہے؟

یہ وصول کنندہ سرورز سے کہتا ہے کہ SMTP سیشن کے دوران DMARC (ہم آہنگ SPF/DKIM) میں ناکام ہونے والی میل مسترد کر دیں، جس سے براہ راست جعل سازی رک جاتی ہے۔ [2]

Q4: حملہ آور SPF اصولوں کو کیسے بائی پاس کرتے ہیں؟

ملتے جلتے ڈومینز (ٹائپو اسکواٹنگ) کا فائدہ اٹھا کر یا جائز تھرڈ پارٹی میل سروسز پر ہیک شدہ اکاؤنٹس استعمال کر کے۔

Q5: بزنس ای میل کمپرومائز (BEC) کیا ہے؟

کارپوریٹ فراڈ جس میں حملہ آور جعلی ادائیگیوں کی منظوری کے لیے کاروباری ای میل اکاؤنٹس ہائی جیک کرتے ہیں یا ان کی نقالی کرتے ہیں۔

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: ملٹی فیکٹر تصدیق فشنگ کو کیسے روکتی ہے؟

اسے ثانوی ٹوکنز (جیسے ہارڈ ویئر کیز) درکار ہوتے ہیں جنہیں صرف ہم شکل لینڈنگ پیجز کے ذریعے چرایا نہیں جا سکتا۔

Q7: اسناد چرانے والا لینڈنگ پیج کیا ہے؟

ہم شکل لاگ اِن پورٹل جو درج کیے گئے یوزر نیمز، پاس ورڈز اور MFA ٹوکنز کو ریئل ٹائم میں حاصل کرنے کے لیے بنایا جاتا ہے۔

Q8: سب ڈومین ہائی جیکنگ کیا ہے؟

حملہ آور غیر استعمال شدہ DNS سب ڈومین پوائنٹر پر قبضہ کر کے قابلِ اعتماد بنیادی ڈومین کے تحت بدنیت فشنگ لینڈنگ صفحات ہوسٹ کرتا ہے۔

Q9: DKIM الائنمنٹ چیک کیسے کام کرتا ہے؟

یہ تصدیق کرتا ہے کہ 'From' ہیڈر میں ڈومین اسی ڈومین سے ملتا ہے جس نے DKIM ہیڈر میں پیغام پر کرپٹوگرافک دستخط کیے تھے۔

Q10: ای میل گیٹ وے کا کردار کیا ہے؟

آنے والی ای میل کی فلٹرنگ، لنکس کا آڈٹ، اٹیچمنٹس کی سینڈ باکسنگ، اور SPF/DKIM/DMARC کی تعمیل کی توثیق۔

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

2025 میں FBI کے IC3 کو رپورٹ ہونے والی سب سے زیادہ جرائم کی قسم فشنگ اور اسپوفنگ تھی، جس کی 191,561 شکایات تھیں۔ [4]

2. سیکیورٹی بصیرت

بزنس ای میل کمپرومائز (BEC) نے 2025 میں FBI کے IC3 کو رپورٹ ہونے والے 3 ارب ڈالر سے زیادہ کے نقصانات کیے۔ [4]

3. سیکیورٹی بصیرت

ہومو گراف حملے براؤزرز میں ایگزیکٹ میچ برانڈ ڈومینز کی بصری نقل بنانے کے لیے Cyrillic کے ہم شکل حروف استعمال کرتے ہیں۔

4. سیکیورٹی بصیرت

'p=reject' کے ساتھ، ڈومین وصول کنندگان سے کہتا ہے کہ ناکام ہونے والی میل کو ڈیلیوری کے دوران مسترد کریں، اسے اسپام کے طور پر فائل نہ کریں۔ [2]

5. سیکیورٹی بصیرت

CEOs کو نشانہ بنانے والے وہیلنگ حملے عموماً خفیہ انضمام یا ڈومین خریداری کے لیے فوری ادائیگیوں کی درخواست کرتے ہیں۔

6. سیکیورٹی بصیرت

کریڈینشل ہارویسٹنگ پورٹلز اصل لاگ اِن صفحات کی نقل کرتے ہیں تاکہ متاثرین اپنے پاس ورڈز براہِ راست حملہ آور کے فارم میں لکھ دیں۔

7. سیکیورٹی کی بصیرت

CISA کی مشترکہ فشنگ رہنمائی DMARC، SPF، DKIM اور فشنگ سے محفوظ MFA کے ساتھ ساتھ صارفین کی تربیت کی سفارش کرتی ہے۔ [3]

8. سیکیورٹی کی بصیرت

SPF کی جانچ DNS کوئری کرنے والی 10 شرائط تک محدود ہے؛ حد سے تجاوز پر 'permerror' نتیجہ ملتا ہے۔ [1]

9. سیکیورٹی کی بصیرت

FIDO2 ہارڈ ویئر سیکیورٹی کیز ریموٹ اسناد کی چوری کے خلاف خفیہ کاری پر مبنی تحفظ فراہم کرتی ہیں۔

10. سیکیورٹی بصیرت

فشنگ حملہ آوروں کے کسی ادارے میں پہلی بار داخل ہونے کے سب سے عام طریقوں میں سے ایک ہے، اسی لیے باقاعدہ آگاہی کی تربیت ایک مؤثر دفاع ہے۔

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] 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

جوابی کلید: چیک پوائنٹ 1 – کثیر انتخابی

1 سوال 1 — درست جواب: A

تدریسی نوٹ

اسپیئر فشنگ کیا ہے؟ → ہدف شدہ فشنگ ای میل جو کسی مخصوص فرد یا ادارے کے مطابق تیار کی گئی ہو

2 سوال 2 — درست جواب: A

تدریسی نوٹ

SPF کسی ڈومین کے مجاز بھیجنے والے ہوسٹس کو DNS میں شائع کرتا ہے تاکہ وصول کنندگان انویلپ بھیجنے والے کی جانچ کر سکیں۔

3 سوال 3 — درست جواب: A

تدریسی نوٹ

وہیلنگ حملہ کیا ہے؟ → فشنگ مہم جو خاص طور پر نمایاں کارپوریٹ ایگزیکٹوز کو نشانہ بناتی ہے

4 سوال 4 — درست جواب: A

تدریسی نوٹ

DKIM کیا کرتا ہے؟ → بھیجنے والے کی صداقت جانچنے کے لیے ای میلز میں خفیہ کاری پر مبنی دستخط شامل کرتا ہے

5 سوال 5 — درست جواب: A

تدریسی نوٹ

DMARC کا کردار کیا ہے؟ → وصول کرنے والے ای میل سرورز کو ہدایت دینا کہ ناکام SPF/DKIM جانچ سے کیسے نمٹیں

جوابی کلید: چیک پوائنٹ 2 – درست یا غلط

6 سوال 6

درست جواب: غلط

تدریسی نوٹ

غلط: اسپیئر فشنگ مخصوص لوگوں کے لیے تیار کی جاتی ہے، عام بلک فشنگ کے برعکس۔

7 سوال 7

درست جواب: درست

تدریسی نوٹ

DMARC پالیسیاں میل سرورز کو غیر مجاز جعلی پیغامات مسترد کرنے کی ہدایت دے سکتی ہیں۔

8 سوال 8

درست جواب: غلط

تدریسی نوٹ

غلط: SPF بھیجنے والے IP کو DNS سے جانچتا ہے؛ کرپٹوگرافک سگنیچر کی تصدیق DKIM کرتا ہے۔

9 سوال 9

درست جواب: غلط

تدریسی نوٹ

غلط: وہیلنگ سینئر ایگزیکٹوز کو نشانہ بناتی ہے، جو ادائیگیوں کی منظوری دے سکتے ہیں اور حساس ڈیٹا تک رسائی رکھتے ہیں۔

10 سوال 10

درست جواب: درست

تدریسی نوٹ

درست: ادائیگی کی درخواستوں کی علیحدہ، معلوم ذریعے سے تصدیق وائر فراڈ کو روکنے میں مدد دیتی ہے۔

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

F 1. اسپیئر	G 2. اسپوفنگ	D 3. SPF	H 4. DKIM
C 5. DMARC	B 6. وہیلنگ	E 7. فشنگ	A 8. وشنگ

چیک پوائنٹ 3: جوابی کلید – اہم اصطلاحات

1 اسپیئر	2 اسپوفنگ	3 ایس پی ایف	4 ڈی کے آئی ایم
5 ڈی مارک	6 وہیلنگ		

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

1 B – اسپوفنگ	2 A – اسپیئر	3 H – وشنگ	4 C – ایسپیایف
5 G – فشنگ	6 E – ڈیمارک	7 D – ڈیکےائیایم	8 F – وہیلنگ

اساتذہ کے لیے بحث کے نوٹس

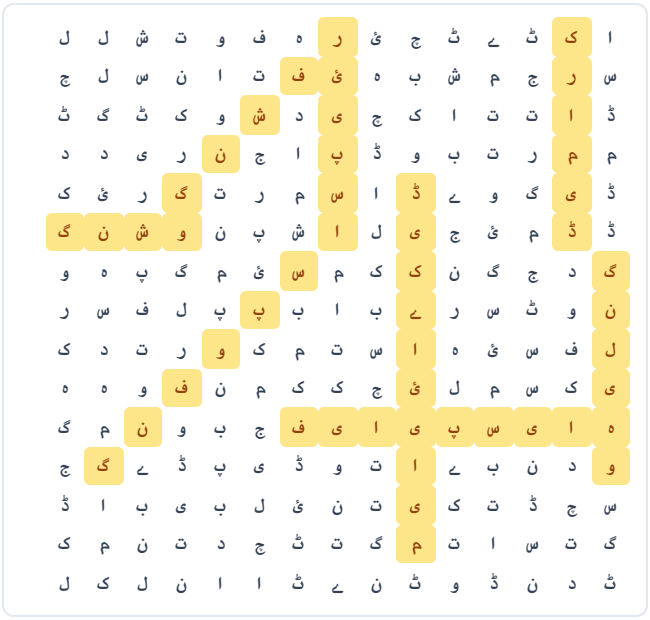
اہم اصطلاحات:
یقینی بنائیں کہ طلبہ اسپیئر، اسپوفنگ اور SPF کو اپنے الفاظ میں سمجھا سکیں اور ہر ایک کی مثال دے سکیں۔

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

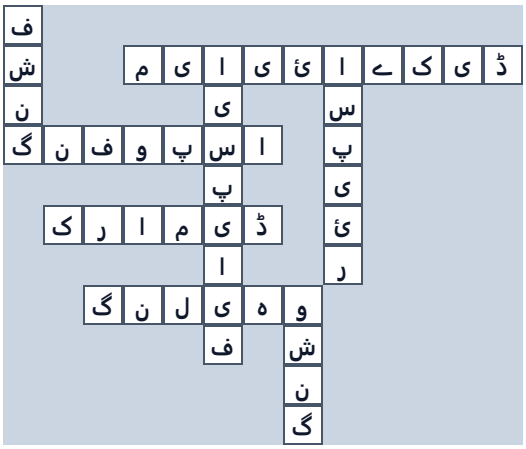
ماخذ کی جانچ:
طلبہ سے کہیں کہ ورک شیٹ کے ماخذ میں کم از کم ایک دعوے کی تصدیق کریں، اور اس پر بات کریں کہ اعداد و شمار، قیمتیں اور قواعد وقت کے ساتھ کیوں بدل سکتے ہیں۔

پہیلیوں کی کلیدیں اور استاد کے نوٹس

الفاظ کی تلاش کا حل



کراس ورڈ کا حل



کراس ورڈ حل کے لیے استاد کی گائیڈ

افقی

2 افقی: ڈیکےائیایم ای میل میں کرپٹوگرافک دستخط (10 حروف)

5 افقی: اسپوفنگ بھیجنے والے کا ای میل ایڈریس جعلی بنانا (7 حروف)

6 افقی: ڈیمارک مسترد کرنے کی ہدایات والی پالیسی (6 حروف)

7 افقی: وہیلنگ سی لیول ایگزیکٹوز کو ہدف بنانا (6 حروف)

عمودی

1 عمودی: فشنگ سوشل انجینئرنگ پر مبنی ای میل (4 حروف)

3 عمودی: اسپیئر ذاتی نوعیت کی ہدف شدہ ای میل (6 حروف)

4 عمودی: ایسپیایف DNS میں مجاز بھیجنے والے IPs کی فہرست (8 حروف)

7 عمودی: وشنگ صوتی کالز پر مبنی فراڈ (4 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. پائرس — اسپیئر
2. پافیپایس — ایسپیایف
3. ڈماکری — ڈیمارک
4. گنفش — فشنگ
5. فگوپانس — اسپوفنگ
6. یاےیاڈیئمک — ڈیکےائیایم
7. نولگیہ — وہیلنگ
8. وگنش — وشنگ

خفیہ سائفر چیلنج کی کلید

"آڈٹ سے سوشل انجینئرنگ پہچانیں"

کیس اسٹڈیز کی جوابی کلید

A کیس اسٹڈی 1: اعلیٰ ایگزیکٹو کو نشانہ بنانے والے وہیلنگ حملے کا ازالہ

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: ایک چیف فنانشل آفیسر کو سی ای او کی طرف سے آنے کا دعویٰ کرنے والی نہایت ذاتی نوعیت کی ای میل ملتی ہے، جس میں خفیہ ڈومین خریداری مکمل کرنے کے لیے فوری طور پر 50,000 ڈالر وائر کرنے کا کہا گیا ہے۔
- تجویز کردہ حکمت عملی اور حل: جعلی بھیجنے والے ڈومینز کو بلاک کرنے کے لیے DMARC کو 'p=reject' پالیسی کے ساتھ ترتیب دیں۔ گیٹ وے پر بیرونی بھیجنے والے کی انتباہی بینرز شامل کریں، اور تمام مالی لین دین کے لیے زبانی، آؤٹ آف بینڈ تصدیق لازمی قرار دیں۔

B کیس اسٹڈی 2: SPF/DKIM/DMARC گیٹ وے پالیسیاں نافذ کرنا

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: ایک انٹرپرائز سیکیورٹی آڈٹس میں ناکام ہو رہی ہے کیونکہ اس کی آؤٹ باؤنڈ مارکیٹنگ ای میلز کو اکثر اسپام قرار دیا جاتا ہے اور ہیکرز کمپنی کے برانڈ ڈومین کی اسپوفنگ کر رہے ہیں۔
- تجویز کردہ حکمت عملی اور حل: مجاز بھیجنے والے IPs کی تفصیل کے ساتھ SPF کے لیے TXT ریکارڈ شائع کریں۔ آؤٹ باؤنڈ میل سرورز پر DKIM سائننگ کیز ترتیب دیں، اور بدسلوکی کی نشاندہی کے لیے آنے والی DMARC XML فیڈ بیک رپورٹس کا تجزیہ کریں۔