نام: _____ تاریخ: _____ نمبر: _____

# آن لائن اسکیمز اور سوشل انجینئرنگ تحفظ کی گائیڈ

ای میل فشنگ، جعلی ڈومینز، وشنگ، سپورٹ فراڈز، آؤٹ آف بینڈ تصدیق، BEC

## آن لائن اسکیمز 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 آن لائن فراڈ سے دفاع سے متعارف کراتا ہے۔ آپ جعلی فشنگ ویب سائٹس، سوشل انجینئرنگ کی چالوں، سپورٹ اسکیمز، وائر فراڈ کے ذرائع، اور ادائیگی کی تصدیق کے طریقوں 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/online-scams/

# آپ کا آن لائن فراڈ سے تحفظ کا لرننگ روڈ میپ

- سپورٹ اسکیمز اور ٹائپو اسکواٹنگ ڈومینز کے عام اشاروں کی نشاندہی کریں۔
- جعل سازی کے خلاف ای میل تصدیقی پروٹوکولز (SPF, DKIM, DMARC) نافذ کریں۔
- کاروباری وائر فراڈ روکنے کے لیے آؤٹ آف بینڈ لین دین کی تصدیق قائم کریں۔

### آن لائن اسکیمز 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 آن لائن فراڈ سے تحفظ پر لاگو کریں۔ اور آخر میں اضافی سرگرمی "تیزی سے سوچیں"۔

### آن لائن اسکیمز اور سوشل انجینئرنگ سے تحفظ (تعارف)

آن لائن اسکیمز فشنگ، سپورٹ پاپ آپس، وشنگ اور وائر فراڈ کے ذریعے انسانی رویے کا فائدہ اٹھاتی ہیں۔ آؤٹ آف بینڈ ٹرانزیکشن تصدیق اور SPF/DKIM/DMARC ڈومین قواعد نافذ کرنے سے سوشل انجینئرنگ کے راستوں کو گیٹ وے پر روکنے میں مدد ملتی ہے۔

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

## چیک پوائنٹ 1: کثیر انتخابی چیلنج

**1** 1. سپورٹ اسکیم کی بنیادی علامت کیا ہے؟

- A. پاپ اپ جو دعویٰ کرتا ہے کہ آپ کا سسٹم متاثر ہے اور فون نمبر پر کال کرنے کا مطالبہ کرتا ہے
- B. سرکاری رجسٹری سے ڈاؤن لوڈ ہونے والی خودکار سیکیورٹی اپ ڈیٹ
- C. پاس ورڈ مینیجر کا کارپوریٹ ڈومین پر اسناد بھرنے سے انکار کرنا
- D. بیرونی ڈرائیو کی ترتیب پر چلنے والا پس منظر کی فائل کا بیک اپ

**2** 2. بینک کی تفصیلات چرانے کے لیے کون سی تکنیک جعلی بھیجنے والے ڈومینز استعمال کرتی ہے؟

- A. ای میل فشنگ
- B. پورٹ اسکیننگ
- C. میموری انجیکشن
- D. کرپٹوگرافک شریڈنگ

**3** 3. وائر ٹرانسفر فراڈ کی نمائندگی کیا کرتا ہے؟

- A. سوشل انجینئرنگ کے ذریعے متاثرین کو جعلی کارپوریٹ اکاؤنٹس میں رقم بھیجنے پر بہکانا
- B. رینسم ویئر پے لوڈز کے ذریعے سسٹم ڈیٹا بیس کو خفیہ کرنا
- C. SQL انجیکشن کمانڈز کے ذریعے ڈیٹا بیس سے کوئری کرنا
- D. سسٹم فائلوں کا آف لائن اسٹوریج ڈسکس پر بیک اپ لینا

**4** 4. دھوکے باز جعلی شاپنگ ویب سائٹس کیوں بناتے ہیں؟

- A. خریداروں کے کریڈٹ کارڈ کی تفصیلات اور ادائیگی کی اسناد چرانا
- B. سینڈ باکس میں میل ویئر تجزیے کے ڈیٹا بیس ٹیبلز ہوسٹ کرنے کے لیے
- C. آن لائن آرڈرز کی ترسیل تیز کرنے کے لیے
- D. ویب سائٹ کے نئے ڈیزائنز کو مفت ٹیسٹ کرنے کے لیے

**5** 5. وشنگ کا کیا مطلب ہے؟

- A. فون نیٹ ورکس پر اسناد چرانے کے لیے وائس فشنگ فراڈ
- B. غیر محفوظ سسٹم ڈیوائسز کے لیے مقامی نیٹ ورکس کی اسکیننگ
- C. غیر مجاز خلاف ورزی کے بعد سسٹم ڈیٹا بیسز بحال کرنا
- D. غیر معتبر کوڈ کو محفوظ ورچوئل کنٹینرز کے اندر چلانا

## چیک پوائنٹ 2: درست یا غلط چیلنج

**6 سوال 6**

6. فشنگ اسکیمز صرف اینڈ یوزرز کو نشانہ بناتے ہیں، کبھی ایگزیکٹو وہیلنگ اہداف کو نہیں۔

درست غلط

**7 سوال 7**

7. جعلی ڈومینز اکثر معتبر برانڈز کی نقل کرنے کے لیے معمولی ٹائپو (جیسے amaz0n.com) استعمال کرتے ہیں۔

درست غلط

**8 سوال 8**

8. سپورٹ اسکیمز کو کال کرنے والے کو ریموٹ رسائی دے کر حل کیا جا سکتا ہے۔

درست غلط

**9 سوال 9**

9. سوشل انجینئرنگ خوف اور عجلت جیسی انسانی نفسیات کا فائدہ اٹھا کر سیکیورٹی اصولوں کو بائی پاس کرتی ہے۔

درست غلط

**10 سوال 10**

10. وائر ٹرانسفر کی درخواستوں کی تصدیق ہمیشہ آؤٹ آف بینڈ مواصلاتی چینلز کے ذریعے کی جانی چاہیے۔

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. صارفین کو دھوکہ دینے والی جعلی ای میلز _____ کہلاتی ہیں۔
2. قابل اعتماد برانڈز کی نقل کرنے والے ویب ایڈریس _____ ہوتے ہیں۔
3. بینک تفصیلات کو نشانہ بنانے والے صوتی فراڈ _____ کہلاتے ہیں۔
4. وائرس ہٹانے کے لیے رقم مانگنے والا پاپ اپ سپورٹ _____ ہے۔
5. ادائیگی کی درخواست کو یقینی بنانے کے لیے آؤٹ آف بینڈ _____ درکار ہوتی ہے۔
6. کاروباری لین دین کو چوروں کے اکاؤنٹس پر موڑنا _____ فراڈ ہے۔

**الفاظ کا بینک**

اسکیم　اسمشنگ　تصدیق　جعلی　فشنگ　وائر　وشنگ　وہیلنگ

**اپنے جوابات یہاں لکھیں:**

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

# چیک پوائنٹ 4: سیکیورٹی تصورات کا ملان

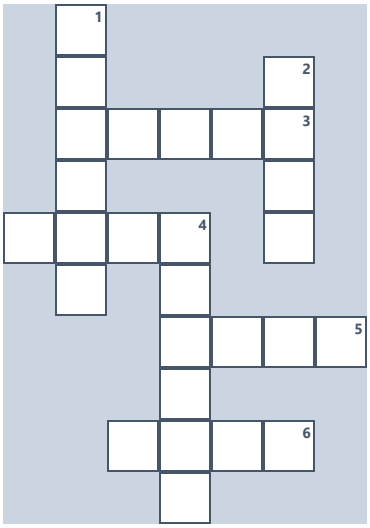
**تعریفوں کا ملان**

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. فشنگ | A | بینک ٹرانزیکشنز کی مجرمانہ اکاؤنٹس میں جعلی ری ڈائریکشن۔ |
| 2. اسپوفڈ | B | متاثرین سے رقم یا اسناد تک رسائی چرانے کے لیے بنائی گئی دھوکا دہی کی اسکیم۔ |
| 3. وشنگ | C | موبائل اکاؤنٹ کی اسناد چرانے کے لیے دھوکا دہی کے ٹیکسٹ پیغامات بھیجنا۔ |
| 4. اسکیم | D | اسناد اور اکاؤنٹ کی تفصیلات چرانے کے لیے بنائی گئی جعلی صوتی کالز۔ |
| 5. تصدیق | E | ہدف شدہ فشنگ حملے جن کا مقصد C-level ایگزیکٹوز کی اسناد چرانا ہے۔ |
| 6. تار | F | نقل کیا گیا ای میل بھیجنے والا یا ویب سائٹ ایڈریس جو جائز دکھائی دینے کے لیے بنایا گیا ہو۔ |
| 7. وہیلنگ | G | لاگ اِن اسناد اور پاس ورڈز چرانے کے لیے بنائی گئی جعلی ای میل مہمات۔ |
| 8. اسمشنگ | H | قابلِ اعتماد ثانوی رابطے کے طریقے سے ادائیگی کی تفصیلات کی تصدیق کرنا۔ |

# 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

**3. فریب پر مبنی منصوبہ جو متاثرین سے رقم یا اسناد تک رسائی چرانے کے لیے بنایا گیا ہو (5)**

**4. فریب پر مبنی صوتی کالز جو اسناد اور اکاؤنٹ کی تفصیلات چرانے کے لیے کی جاتی ہیں (4)**

**5. نقل کیا گیا ای میل بھیجنے والا یا ویب سائٹ ایڈریس جو جائز دکھائی دینے کے لیے بنایا گیا ہو (4)**

**6. جعلی ای میل مہمات جو لاگ اِن اسناد اور پاس ورڈز چرانے کے لیے بنائی جاتی ہیں (4)**

## عمودی

**1. موبائل اکاؤنٹ کی اسناد چرانے کے لیے اسکیم ٹیکسٹ میسجز بھیجنا (6)**

**2. بینک لین دین کو مجرمانہ اکاؤنٹس کی طرف فریب سے موڑ دینا (4)**

**4. سی لیول ایگزیکٹوز کی اسناد چرانے کے لیے کیے جانے والے ہدف شدہ فشنگ حملے (6)**

# 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

**3 افقی: فریب پر مبنی منصوبہ جو متاثرین سے رقم یا اسناد تک رسائی چرانے کے لیے بنایا گیا ہو (5 حروف):**

**4 افقی: فریب پر مبنی صوتی کالز جو اسناد اور اکاؤنٹ کی تفصیلات چرانے کے لیے کی جاتی ہیں (4 حروف):**

**5 افقی: نقل کیا گیا ای میل بھیجنے والا یا ویب سائٹ ایڈریس جو جائز دکھائی دینے کے لیے بنایا گیا ہو (4 حروف):**

**6 افقی: جعلی ای میل مہمات جو لاگ اِن اسناد اور پاس ورڈز چرانے کے لیے بنائی جاتی ہیں (4 حروف):**

## عمودی

**1 عمودی: موبائل اکاؤنٹ کی اسناد چرانے کے لیے اسکیم ٹیکسٹ میسجز بھیجنا (6 حروف):**

**2 عمودی: بینک لین دین کو مجرمانہ اکاؤنٹس کی طرف فریب سے موڑ دینا (4 حروف):**

**4 عمودی: سی لیول ایگزیکٹوز کی اسناد چرانے کے لیے کیے جانے والے ہدف شدہ فشنگ حملے (6 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 | ج | ع | ٹ | د | ع | ی | ق | ی | ت | ک | م | م | ش | چ |
| ن | ق | ک | ب | ی | ت | ا | ہ | ج | ش | م | چ | ئ | ت | ٹ |
| ب | ی | گ | چ | ر | ی | گ | ج | ل | ع | ٹ | ن | س | ت | ب |
| ہ | د | ئ | ا | چ | س | ے | ر | د | ئ | ل | ل | ہ | ع | ا |
| و | ص | س | ٹ | س | و | ص | گ | ق | ن | ص | ی | ج | ن | ک |
| پ | ت | ہ | ر | ج | ہ | ل | ا | و | ک | ن | و | ا | ئ | ر |
| ص | ن | ل | پ | ے | ی | ہ | ی | س | ٹ | ش | س | ب | ا | ب |
| پ | م | ص | ش | س | ل | ق | ش | ص | ک | ے | ش | ت | و | گ |
| گ | س | ت | ر | گ | ن | گ | ش | ن | م | ی | ج | گ | گ | ن |
| ن | و | ہ | ے | ی | گ | ج | پ | ہ | ن | ل | م | د | ہ | ب |
| ش | ا | س | م | ش | ن | گ | ع | ت | ی | ئ | ف | پ | ئ | و |
| ف | ع | ج | ش | د | ئ | ت | گ | ت | و | ص | م | پ | ش | ے |
| ب | ا | ئ | ل | ت | ش | ا | ت | ل | ت | ج | چ | ن | ر | ت |
| و | ن | گ | ٹ | ر | ہ | ئ | ی | ج | و | ف | گ | ٹ | ا | ا |
| و | م | گ | ن | ے | ص | ن | س | ہ | ے | ہ | پ | گ | ق | ب |

### الفاظ کی فہرست

فشنگ جعلی وشنگ اسکیم تصدیق وائر وہیلنگ اسمشنگ

## 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. فشنگ** |
| **B. جعلی** |
| **C. وشنگ** |
| **D. اسکیم** |
| **E. تصدیق** |
| **F. وائر** |
| **G. وہیلنگ** |
| **H. اسمشنگ** |

| تعریفیں اور ملان کے خانے |
| --- |
| 1. نقل کیا گیا ای میل بھیجنے والا یا ویب سائٹ ایڈریس جو جائز دکھائی دینے کے لیے بنایا گیا ہو۔ |
| 2. کسی قابل اعتماد ثانوی رابطے کے طریقے سے ادائیگی کی تفصیلات کی توثیق۔ |
| 3. بینک لین دین کو مجرمانہ اکاؤنٹس کی طرف فریب سے موڑ دینا۔ |
| 4. موبائل اکاؤنٹ کی اسناد چرانے کے لیے اسکیم ٹیکسٹ میسجز بھیجنا۔ |
| 5. سی لیول ایگزیکٹوز کی اسناد چرانے کے لیے کیے جانے والے ہدف شدہ فشنگ حملے۔ |
| 6. فریب پر مبنی صوتی کالز جو اسناد اور اکاؤنٹ کی تفصیلات چرانے کے لیے کی جاتی ہیں۔ |
| 7. جعلی ای میل مہمات جو لاگ اِن اسناد اور پاس ورڈز چرانے کے لیے بنائی جاتی ہیں۔ |
| 8. فریب پر مبنی منصوبہ جو متاثرین سے رقم یا اسناد تک رسائی چرانے کے لیے بنایا گیا ہو۔ |

## 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. ن ف گ ش
2. و ن گ ش
3. د ت ق ی ص
4. گ ل ی ن و ہ
5. ی ج ل ع
6. ی ا ک م س
7. ئ و ر ا
8. م گ ا ن ش س

# 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. وہ جملے جو فراڈ کرنے والے اکثر استعمال کرتے ہیں
3. ادائیگی کے وہ طریقے جو فراڈ کرنے والے مانگتے ہیں
4. آن لائن فراڈ کی اقسام
5. وہ پیشکشیں جو حد سے زیادہ اچھی لگتی ہیں
6. فراڈ کی رپورٹ کرنے کے مقامات
7. سائبر سیکیورٹی سے متعلق الفاظ
8. وہ لوگ جنہیں آپ فراڈ سے خبردار کر سکتے ہیں
9. وہ چیزیں جن کا آپ بیک اپ لیتے ہیں
10. ای میل میں انتباہی علامات
11. کمپیوٹر کے متاثر ہونے کی علامات
12. آن لائن دکان کی جانچ کرنے کے طریقے
13. اپنے اکاؤنٹس کو محفوظ رکھنے کے طریقے
14. فراڈ کا شکار ہونے پر کرنے کے کام
15. ڈیٹا لیک کے بعد کرنے کے کام

# 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: کارپوریٹ وائر ٹرانسفر فراڈ کی روک تھام



**منظرنامہ:** ایک فنانس ڈیپارٹمنٹ کو جعلی وینڈر ایڈریس سے ایک فوری ای میل موصول ہوتی ہے، جس میں درخواست کی گئی ہے کہ آئندہ انوائس کی وائر ادائیگیاں ایک نئے روٹنگ نمبر پر بھیجی جائیں۔

**بحث کا سوال:** وائر فراڈ کی تصدیق کی پالیسی کا خاکہ بیان کریں، اور ای میل کی تصدیق کے بلاکس بیان کریں۔

### کیس اسٹڈی 2: ایگزیکٹو کو نشانہ بنانے والے وہیلنگ فشنگ کا واقعہ



**منظرنامہ:** ایک ایگزیکٹو ایک فشنگ لنک پر کلک کرتا ہے جس میں بورڈ میٹنگ کی محفوظ دستاویز ہونے کا دعویٰ تھا، اور جعلی پورٹل پر اپنی بنیادی کارپوریٹ کریڈینشلز درج کر دیتا ہے۔

**بحث کا سوال:** واقعے کے ردعمل کے اقدامات تفصیل سے بیان کریں، اور وضاحت کریں کہ ایگزیکٹو کے لاگ انز کا آڈٹ کیسے کیا جائے۔

## 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

| 38 | 22 | 2 | 1 | 14 | | 29 | 32 | 19 | 26 | | 38 | 18 | | 27 | 37 | 11 | 20 | 4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | |

| 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: آن لائن اسکیم کیا ہے؟

ڈیجیٹل ذرائع استعمال کرنے والی دھوکہ دہی کی اسکیم جو متاثرین کو رقم بھیجنے یا ذاتی اسناد دینے پر آمادہ کرتی ہے۔

### Q2: ای میل فشنگ کی بنیادی علامت کیا ہے؟

ایسا پیغام جو فوری کارروائی کا دعویٰ کرتا ہے (جیسے اکاؤنٹ کی معطلی) اور آپ کو ایسے لنک کی طرف لے جاتا ہے جو سرکاری ڈومین سے مماثل نہیں ہوتا۔

### Q3: ٹائپو اسکویٹنگ کیا ہے؟

مقبول برانڈز کی عام ٹائپنگ غلطیوں والے ڈومینز (جیسے amaz0n.com) رجسٹر کر کے جعلی فشنگ سائٹس چلانا۔

### Q4: سپورٹ اسکیم کیا ہے؟

پاپ اپ جو دعویٰ کرتا ہے کہ آپ کا پی سی متاثر ہے اور آپ کو نمبر پر کال کرنے اور جعلی صفائی سافٹ ویئر یا ریموٹ رسائی سروسز کے لیے ادائیگی کرنے کی طرف لے جاتا ہے۔ [1]

### Q5: وشنگ کیا ہے؟

وائس فون کالز استعمال کرنے والے فشنگ حملے جن میں متاثرین کو بینک اکاؤنٹ یا لاگ اِن کی تفصیلات دینے پر آمادہ کیا جاتا 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: وائر فراڈ کا کیا مطلب ہے؟**

وینڈرز یا ایگزیکٹوز کا روپ دھار کر ادائیگی کے لین دین کو دھوکے باز اکاؤنٹس کی طرف موڑنا۔

**Q7: وہیلنگ کیا ہے؟**

اسپیئر فشنگ کی انتہائی ہدف شدہ قسم جو براہِ راست سی لیول کارپوریٹ ایگزیکٹوز جیسے اعلیٰ قدر والے اہداف کو نشانہ بناتی ہے۔

**Q8: اسمشنگ کیا ہے؟**

موبائل ڈیوائسز پر بھیجے گئے اسکیم ٹیکسٹ پیغامات جن میں جعلی پورٹلز یا ٹریکنگ اپ ڈیٹس کے لنک ہوتے ہیں۔

**Q9: آؤٹ آف بینڈ تصدیق انتہائی اہم کیوں ہے؟**

یہ متاثرہ ای میل تھریڈز سے بچتے ہوئے علیحدہ مواصلاتی چینل (جیسے فون کال) کے ذریعے لین دین کی تفصیلات کی تصدیق کرتا ہے۔

**Q10: جعلی ایسکرو اکاؤنٹ اسکیم کیسے کام کرتی ہے؟**

اسکیمرز جعلی ایسکرو سائٹ بناتے ہیں اور دعویٰ کرتے ہیں کہ رقم محفوظ رکھی گئی ہے، پھر خریدار کا وائر ڈپازٹ چرا لیتے ہیں۔

# 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: اسکیمرز BEC (Business Email Compromise) کے ذریعے وائر فراڈ کیسے کرتے ہیں؟**

وہ کسی جائز ملازم کا ای میل اکاؤنٹ ہائی جیک کرتے ہیں، انوائس تھریڈز کی نگرانی کرتے ہیں، اور جعلی بینک اکاؤنٹس کے ساتھ اپ ڈیٹ شدہ بلنگ تفصیلات بھیج دیتے ہیں۔

**Q2: آن لائن اسکیمز میں IDN ہومو گراف حملوں کا کیا خطرہ ہے؟**

عام حروف جیسے دکھائی دینے والے غیر ASCII حروف (مثلاً سیریلک 'а') کا استعمال کر کے اصل برانڈز کی نقل کرنے والے جعلی ڈومینز رجسٹر کرنا۔

**Q3: اسکیم کی شناخت میں ای میل ہیڈر کا معائنہ کیوں اہم ہے؟**

یہ اصل ماخذ سرور کا IP اور SPF/DKIM کی توثیق کی حالت ظاہر کرتا ہے، جس سے پتا چلتا ہے کہ بھیجنے والا ڈومین جعلی ہے یا نہیں۔

**Q4: سپورٹ اسکیمرز ریموٹ ڈیسک ٹاپ سافٹ ویئر کا کیسے استحصال کرتے ہیں؟**

وہ AnyDesk یا TeamViewer جیسی یوٹیلیٹیز کے ذریعے متاثرہ کی ڈیوائس سے جڑتے ہیں، میل ویئر لگاتے ہیں اور محفوظ شدہ پاس ورڈز چرا لیتے ہیں۔

**Q5: ایڈوانس فیس اسکیمز کا مقصد کیا ہوتا ہے؟**

متاثرین کو ایک ایسے بڑے مالی انعام کے بدلے پیشگی پروسیسنگ فیس ادا کرنے پر ورغلانا جو وجود ہی نہیں رکھتا۔

# 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: اسکیمرز ہدفی فشنگ کے لیے سوشل میڈیا پروفائلنگ کیسے استعمال کرتے ہیں؟

وہ قائل کرنے والی اسپیئر فشنگ ای میلز تیار کرنے کے لیے کارپوریٹ تنظیمی ڈھانچے اور ملازمین کے نام جمع کرتے ہیں۔

### Q7: جعلی ویب شاپس بھاری رعایتیں کیوں پیش کرتی ہیں؟

خریداروں کو کریڈٹ کارڈ کی تفصیلات درج کرنے پر آمادہ کرنے کے لیے، اور اسناد حاصل کر کے کارڈنگ فورمز پر دوبارہ استعمال یا فروخت کرنے کے لیے۔

### Q8: DMARC ریکارڈز فشنگ اسکیمز کو کیسے بلاک کرتے ہیں؟

DMARC ڈومین مالکان کو یہ کہنے دیتا ہے کہ جو میل منسلک SPF اور DKIM جانچ میں ناکام ہو، وصول کنندگان اسے قرنطینہ کریں یا مسترد کر دیں، جس سے براہِ راست اسپوفنگ رکتی ہے۔ [5]

### Q9: اسناد چرانے والے پورٹلز کا کیا خطرہ ہے؟

جعلی لینڈنگ صفحات جو بالکل Microsoft 365 یا Google ورک اسپیسز جیسے نظر آتے ہیں، اور لاگ اِن کی اسناد درج ہوتے ہی چرا لیتے ہیں۔

### Q10: سیکیورٹی ٹیمیں اسکیم ڈومینز کی رپورٹ اور انہیں غیر فعال کیسے کرتی ہیں؟

رجسٹرار کی ابیوز ای میل، ہوسٹنگ فراہم کنندہ اور Google Safe Browsing رجسٹری کو فراڈ کا ثبوت جمع کرا کر۔

# 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۔ [2]

### 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۔ [2]

### 3. سیکیورٹی بصیرت

ٹائپو اسکوئیٹڈ ڈومینز اصل برانڈ ناموں سے ایک یا دو حرف کے فرق سے مختلف ہوتے ہیں، اس لیے سرسری نظر میں یہ نظر انداز ہو سکتے ہیں۔

### 4. سیکیورٹی بصیرت

ٹیک سپورٹ اسکیمز کی وجہ سے 2025 میں FBI کے IC3 کو رپورٹ ہونے والے نقصانات $2.1 بلین سے زیادہ رہے۔ [2]

### 5. سیکیورٹی بصیرت

ہومو گراف حملے براؤزر ایڈریس بارز میں بالکل ایک جیسے نظر آتے ہیں، جب تک براؤزر punycode کنفیگریشنز ظاہر نہ کرے۔

### 6. سیکیورٹی بصیرت

SMS ٹیکسٹ اسکیمز (اسمشنگ) لنکس کے ساتھ مختصر، فوری پیغامات استعمال کرتے ہیں، جس سے متاثرین کے پاس فراڈ پہچاننے کے لیے بہت کم سیاق و سباق ہوتا ہے۔

### 7. سیکیورٹی کی بصیرت

وہیلنگ حملے ایگزیکٹو ای میلز کو نشانہ بناتے ہیں کیونکہ وہ بڑی وائر ٹرانسفر ادائیگیوں تک رسائی کنٹرول کرتے ہیں۔

### 8. سیکیورٹی کی بصیرت

ادائیگی کی تبدیلیوں کی تصدیق کسی معلوم، محفوظ شدہ فون نمبر پر کال کر کے کرنا BEC وائر فراڈ کے خلاف ایک اہم دفاع ہے۔

### 9. سیکیورٹی کی بصیرت

جعلی ایسکرو ویب سائٹس آن لائن مارکیٹ پلیسز میں عام فراڈ ہیں: یہ محفوظ ادائیگی کی سروس جیسی نظر آتی ہیں لیکن خریدار کا وائر ٹرانسفر چرا لیتی ہیں۔

### 10. سیکیورٹی بصیرت

Google Safe Browsing صارفین کو ان سائٹس کھولنے سے پہلے خبردار کرتا ہے جنہیں اس نے فشنگ یا میل ویئر کے لیے نشان زد کیا ہو۔

# 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.). 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

## جوابی کلید: چیک پوائنٹ 1 – کثیر انتخابی

**1 سوال 1** — درست جواب: A

**تدریسی نوٹ**

سپورٹ اسکیم کی بنیادی علامت کیا ہے؟ → پاپ اپ جو دعویٰ کرتا ہے کہ آپ کا سسٹم متاثر ہے اور فون نمبر پر کال کرنے کا مطالبہ کرتا ہے

**2 سوال 2** — درست جواب: A

**تدریسی نوٹ**

بینک کی تفصیلات چرانے کے لیے کون سی تکنیک جعلی بھیجنے والے ڈومینز استعمال کرتی ہے؟ → ای میل فشنگ

**3 سوال 3** — درست جواب: A

**تدریسی نوٹ**

وائر ٹرانسفر فراڈ کی نمائندگی کیا کرتا ہے؟ → سوشل انجینئرنگ کے ذریعے متاثرین کو جعلی کارپوریٹ اکاؤنٹس میں رقم بھیجنے پر بہکانا

**4 سوال 4** — درست جواب: A

**تدریسی نوٹ**

دھوکے باز جعلی شاپنگ ویب سائٹس کیوں بناتے ہیں؟ → خریداروں کے کریڈٹ کارڈ کی تفصیلات اور ادائیگی کی اسناد چرانا

**5 سوال 5** — درست جواب: A

**تدریسی نوٹ**

وشنگ کا کیا مطلب ہے؟ → فون نیٹ ورکس پر اسناد چرانے کے لیے وائس فشنگ فراڈ

## جوابی کلید: چیک پوائنٹ 2 – درست یا غلط

**6 سوال 6**

درست جواب: غلط

**تدریسی نوٹ**

غلط: فشنگ ایگزیکٹوز کو بھی نشانہ بناتی ہے؛ وہیلنگ سینئر قیادت کو ہدف بنانے والی فشنگ ہے۔

**7 سوال 7**

درست جواب: درست

**تدریسی نوٹ**

جعلی ڈومینز اکثر معتبر برانڈز کی نقل کرنے کے لیے معمولی ٹائپو (جیسے amaz0n.com) استعمال کرتے ہیں۔

**8 سوال 8**

درست جواب: غلط

**تدریسی نوٹ**

غلط: سپورٹ فراڈ کرنے والے کو ریموٹ رسائی دینے سے وہ میل ویئر لگا سکتا ہے اور ڈیٹا چرا سکتا ہے۔

**9 سوال 9**

درست جواب: درست

**تدریسی نوٹ**

سوشل انجینئرنگ خوف اور عجلت جیسی انسانی نفسیات کا فائدہ اٹھا کر سیکیورٹی اصولوں کو بائی پاس کرتی ہے۔

**10 سوال 10**

درست جواب: درست

**تدریسی نوٹ**

وائر ٹرانسفر کی درخواستوں کی تصدیق ہمیشہ آؤٹ آف بینڈ مواصلاتی چینلز کے ذریعے کی جانی چاہیے۔

# 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

| | | | |
|---|---|---|---|
| G 1. فشنگ | F 2. اسپوفڈ | D 3. وشنگ | B 4. اسکیم |
| H 5. تصدیق | A 6. تار | E 7. وہیلنگ | C 8. اسمشنگ |

## چیک پوائنٹ 3: جوابی کلید – اہم اصطلاحات

| | | | |
|---|---|---|---|
| 1 فشنگ | 2 جعلی | 3 وشنگ | 4 اسکیم |
| 5 تصدیق | 6 وائر | | |

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

| | | | |
|---|---|---|---|
| 1 B – جعلی | 2 E – تصدیق | 3 F – وائر | 4 H – اسمشنگ |
| 5 G – وہیلنگ | 6 C – وشنگ | 7 A – فشنگ | 8 D – اسکیم |

### اساتذہ کے لیے بحث کے نوٹس

**اہم اصطلاحات:**
یقینی بنائیں کہ طلبہ فشنگ، اسپوفڈ اور وشنگ 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

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ا | ج | ع | ٹ | د | ے | ی | ق | ی | ت | ک | م | ش | ج | چ |
| ن | ق | ک | ب | ی | ت | ہ | ج | ش | م | چ | ئ | ت | ٹ | ٹ |
| ب | ی | گ | چ | ر | ی | گ | چ | ل | ع | ٹ | ن | س | ت | ب |
| ہ | د | ئ | ا | چ | س | ے | ر | د | ئ | ل | ل | ہ | ع | ا |
| و | س | ٹ | س | و | ص | گ | ن | ق | ص | ی | چ | ن | ک | ک |
| پ | ت | ہ | ر | چ | ہ | ل | ک | و | ن | و | ا | ئ | ر | ر |
| ص | ن | ل | پ | ے | ی | ہ | ٹ | ش | س | ب | ا | ب | ی | ب |
| پ | م | ص | ش | س | ل | ق | ش | ص | ک | ے | ش | ت | و | گ |
| گ | س | ت | ر | گ | ن | گ | ش | م | ی | ج | گ | گ | ن | ن |
| ن | و | ہ | ے | ی | گ | چ | پ | ن | ل | م | د | ہ | ب | ب |
| ش | ا | س | م | ش | ن | گ | ع | ت | ی | ف | پ | ئ | و | و |
| ف | ع | چ | ش | د | ئ | ت | گ | و | ص | م | پ | ش | ے | ے |
| ب | ا | ئ | ل | ت | ش | ا | ت | ل | چ | چ | ن | ر | ت | ت |
| و | ن | گ | ٹ | ر | ہ | ئ | ی | و | ف | گ | ٹ | ا | ا | ا |
| و | م | گ | ن | ے | ص | ن | س | ہ | ے | ہ | پ | گ | ق | ب |

## کراس ورڈ کا حل




## کراس ورڈ حل کے لیے استاد کی گائیڈ

### افقی

**3 افقی: اسکیم** فریب پر مبنی منصوبہ جو متاثرین سے رقم یا اسناد تک رسائی چرانے کے لیے بنایا گیا ہو (5 حروف)

**4 افقی: وشنگ** فریب پر مبنی صوتی کالز جو اسناد اور اکاؤنٹ کی تفصیلات چرانے کے لیے کی جاتی ہیں (4 حروف)

**5 افقی: جعلی** نقل کیا گیا ای میل بھیجنے والا یا ویب سائٹ ایڈریس جو جائز دکھائی دینے کے لیے بنایا گیا ہو (4 حروف)

**6 افقی: فشنگ** جعلی ای میل مہمات جو لاگ اِن اسناد اور پاس ورڈز چرانے کے لیے بنائی جاتی ہیں (4 حروف)

### عمودی

**1 عمودی: اسمشنگ** موبائل اکاؤنٹ کی اسناد چرانے کے لیے اسکیم ٹیکسٹ میسجز بھیجنا (6 حروف)

**2 عمودی: وائر** بینک لین دین کو مجرمانہ اکاؤنٹس کی طرف فریب سے موڑ دینا (4 حروف)

**4 عمودی: وہیلنگ** سی لیول ایگزیکٹوز کی اسناد چرانے کے لیے کیے جانے والے ہدف شدہ فشنگ حملے (6 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. نفگش → فشنگ
2. ونگش → وشنگ
3. دتقیص → تصدیق
4. گلینوہ → وہیلنگ
5. یجلع → جعلی
6. یاکمس → اسکیم
7. ئورا → وائر
8. مگانشس → اسمشنگ

### خفیہ سائفر چیلنج کی کلید

**"تصدیق سے فشنگ رابطے پہچانیں"**

# کیس اسٹڈیز کی جوابی کلید

## A کیس اسٹڈی 1: کارپوریٹ وائر ٹرانسفر فراڈ کی روک تھام

استاد کا حل

### گریڈنگ کی ہدایت

**طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:**

- منظرنامے کا تجزیہ: ایک مالیاتی شعبے کو جعلی وینڈر ایڈریس سے فوری ای میل ملتی ہے، جس میں درخواست کی گئی ہے کہ آئندہ انوائسز کی وائرز ایک نئے روٹنگ نمبر پر بھیجی جائیں۔
- تجویز کردہ حکمت عملی اور حل: تمام ادائیگیوں کے لیے دوہری منظوری کی پالیسی نافذ کریں۔ پہلے سے محفوظ شدہ فون نمبر کے ذریعے آؤٹ آف بینڈ تصدیق کریں، اور جعلی ڈومین والی ای میلز کو گیٹ وے پر بلاک کریں۔

## B کیس اسٹڈی 2: ایگزیکٹو کو نشانہ بنانے والے وہیلنگ فشنگ کا واقعہ

استاد کا حل

### گریڈنگ کی ہدایت

**طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:**

- منظرنامے کا تجزیہ: ایک ایگزیکٹو نے ایسے فشنگ لنک پر کلک کیا جس میں بورڈ میٹنگ کی محفوظ دستاویز ہونے کا دعویٰ کیا گیا تھا، اور جعلی پورٹل پر اپنی بنیادی کارپوریٹ اسناد درج کر دیں۔
- تجویز کردہ حکمت عملی اور حل: ایگزیکٹو کی ڈیوائس کو الگ کریں۔ کارپوریٹ سیشن ٹوکنز اور اسناد سب ری سیٹ کریں۔ ڈیٹا کے اخراج کے لیے ایکسیس لاگز کا جائزہ لیں، اور تمام لاگ اِنز پر ہارڈ ویئر MFA نافذ کریں۔