نام: _____ تاریخ: _____ نمبر: _____

# رینسم ویئر حملے اور کاروبار بحالی

پے لوڈ کا نفاذ، کرپٹوگرافک فائل انکرپشن، آف لائن بیک اپس، روک تھام کے طریقۂ کار اور ڈیزاسٹر ریکوری۔

## رینسم ویئر حملوں کا 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 رینسم ویئر حملوں اور کاروباری بحالی سے متعارف کراتا ہے۔ آپ پے لوڈ کے نفاذ، فائل کی خفیہ کاری، آف لائن بیک اپس، خطرے کی روک تھام، کرپٹو کرنسی ادائیگیوں، اور ڈیزاسٹر ریکوری پلانز 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/ransomware-attack/

# آپ کا رینسم ویئر بحالی کا لرننگ روڈ میپ

- ٹروجن، رینسم ویئر اور اسپائی ویئر پے لوڈز میں فرق واضح کریں۔
- محفوظ سینڈ باکس ماحول کے اندر بدنیت فائلوں کا تجزیہ کریں۔
- نیٹ ورک کو فوری طور پر الگ کرنے اور محدود کرنے کے طریقہ کار تیار کریں۔

### رینسم ویئر حملوں کی 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 رینسم ویئر سے بحالی پر لاگو کریں۔ اور آخر میں اضافی سرگرمی "تیزی سے سوچیں"۔

### رینسم ویئر حملے اور آفت سے بحالی (تعارف)

رینسم ویئر پے لوڈز سسٹم اسٹوریج کو کرپٹوگرافی کے ذریعے لاک کر دیتے ہیں اور ڈی کرپشن کیز کے لیے کرپٹو کرنسی کی ادائیگی کا مطالبہ کرتے ہیں۔ اس خطرے کو کم کرنے میں نیٹ ورک آئسولیشن اصول، سینڈ باکس میں میل ویئر کا تجزیہ، اور مضبوط ایئر گیپڈ کولڈ بیک اپس شامل ہیں۔

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

## چیک پوائنٹ 1: کثیر انتخابی چیلنج

**1. رینسم ویئر حملے کا بنیادی طریقہ کار کیا ہے؟**

- A. سسٹم تک رسائی روکنے کے لیے صارف کی فائلوں کی خفیہ کاری
- B. فارم کے خانوں میں نقصان دہ SQL کمانڈز ڈالنا
- C. عوامی Wi-Fi کنکشن پر نیٹ ورک پیکٹس کی جاسوسی کرنا
- D. SPF توثیق کو عبور کرنے کے لیے ای میل ہیڈرز کی جعل سازی کرنا

**2. آف لائن (کولڈ) بیک اپ کیا ہے؟**

- A. اسٹوریج کاپی جو میل ویئر کے پھیلاؤ سے بچانے کے لیے نیٹ ورک سے منقطع ہو
- B. بیک اپ جو بنیادی ویب سرور کی ہارڈ ڈرائیو پر محفوظ ہو
- C. سسٹم رجسٹری لاگز کا عارضی کیش
- D. ایک ایڈمنسٹریٹو ٹول جو صارف کے پاس ورڈز ری سیٹ کرنے کے لیے استعمال ہوتا ہے

**3. رینسم ویئر حملے کے دوران سیکیورٹی ٹیموں کو متاثرہ سسٹمز کو کیسے الگ کرنا چاہیے؟**

- A. نیٹ ورک کیبلز فوراً منقطع کریں اور وائرلیس انٹرفیسز بند کر دیں
- B. اینٹی وائرس سگنیچرز کا ڈیٹا بیس اپ گریڈ کرنا
- C. بنیادی DNS سرور بند کر دیں
- D. متاثرہ فائلوں کی ایکسٹینشنز کا نام تبدیل کریں

**4. سیکیورٹی ایجنسیاں رینسم ویئر کے مطالبات ادا کرنے کے خلاف مشورہ کیوں دیتی ہیں؟**

- A. رقم ادا کرنا حملہ آوروں کی حوصلہ افزائی کرتا ہے اور ڈی کرپشن کلید ملنے کی ضمانت نہیں دیتا
- B. یہ تمام کارپوریٹ انشورنس پالیسیوں کو خودکار طور پر کالعدم کر دیتا ہے
- C. یہ ہر کسٹمر کو ای میل کے ذریعے خودکار طور پر مطلع کرتا ہے
- D. یہ باقی سسٹم بیک اپ فائلوں کو خراب کر دیتا ہے

**5. ڈیزاسٹر ریکوری پلان (DRP) کیا ہے؟**

- A. سسٹم سمجھوتے کے بعد آپریشنز اور ڈیٹا بحال کرنے کا منظم عمل
- B. فائر وال کنفیگریشن جو آنے والے نیٹ ورک پورٹس کی نقشہ بندی کرتی ہے
- C. صارف کی انتظامی مراعات کی فہرست والا ڈیٹا بیس اسکیما
- D. ایک ای میل توثیقی پروٹوکول جو جعلی ڈومینز کو مسترد کرتا ہے

## چیک پوائنٹ 2: درست یا غلط چیلنج

**6 سوال 6**

6. رینسم ویئر پے لوڈز نیٹ ورک سے جڑے آن لائن بیک اپس تک آسانی سے پھیل سکتے ہیں۔

درست غلط

**7 سوال 7**

7. کرپٹو کرنسی تاوان ادا کرنے سے ضمانت ملتی ہے کہ فائلیں کامیابی سے ڈیکرپٹ ہو جائیں گی۔

درست غلط

**8 سوال 8**

8. متاثرہ سسٹمز کو نیٹ ورک سے منقطع کرنا رینسم ویئر کو ملحقہ سسٹمز تک پھیلنے سے روکنے میں مدد دیتا ہے۔

درست غلط

**9 سوال 9**

9. رینسم ویئر سسٹم اسٹوریج کو خفیہ کرنے کے لیے سمیٹرک کرپٹوگرافی کبھی استعمال نہیں کرتا۔

درست غلط

**10 سوال 10**

10. ڈیٹا بحالی کے طریقہ کار کی باقاعدہ جانچ ڈیزاسٹر ریکوری کا ایک اہم حصہ 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. مقامی فائلوں تک رسائی روکنا کرپٹوگرافک _____ کے ذریعے ہوتا ہے۔
2. سسٹم پر چلنے والا فعال نقصان دہ کوڈ _____ ہوتا ہے۔
3. منقطع آف سائٹ اسٹوریج کاپیاں ایک محفوظ _____ کی نمائندگی کرتی ہیں۔
4. میل ویئر کو پھیلنے سے روکنے کے لیے اینڈ پوائنٹ نیٹ ورک _____ ضروری ہے۔
5. سائبر مجرموں کی طرف سے مانگی گئی کرپٹو کرنسی ادائیگی _____ ہے۔
6. آپریشنل ڈیٹا فائلوں کی واپسی ڈیزاسٹر _____ کہلاتی ہے۔

### الفاظ کا بینک

بحالی | پے لوڈ | تاوان | تباہی | ٹروجن | خفیہ کاری | علیحدگی | کولڈ بیکاپ

**اپنے جوابات یہاں لکھیں:**

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

# چیک پوائنٹ 4: سیکیورٹی تصورات کا ملان

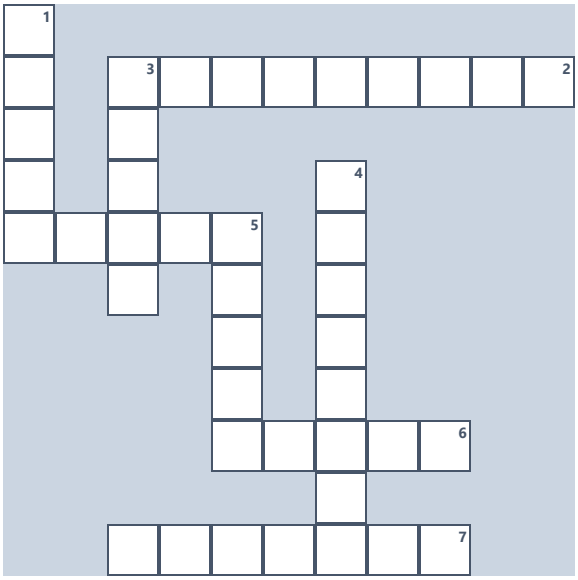
### تعریفوں کا ملان

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. خفیہ کاری | A | متاثرہ نیٹ ورک سسٹمز کو منقطع کرنا۔ |
| 2. پے لوڈ | B | نقصان دہ فائل جو صاف فائل کی طرح ظاہر کی گئی ہو۔ |
| 3. کولڈ بیک اپ | C | فائلوں کو کرپٹوگرافک طریقے سے لاک کرنا۔ |
| 4. علیحدگی | D | سسٹم میں بڑی خرابی کا واقعہ۔ |
| 5. تاوان | E | نقصان دہ سافٹ ویئر چلانا۔ |
| 6. بحالی | F | منقطع آف لائن کاپی۔ |
| 7. آفت | G | بیک اپ سے ڈیٹا بیس بحال کرنا۔ |
| 8. ٹروجن | H | کرپٹوگرافک کی کی ادائیگی کی درخواست۔ |

# 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. منقطع آف لائن کاپی (9)**

**5. کرپٹوگرافک کلید کے بدلے ادائیگی کی درخواست (5)**

**6. بیک اپ سے ڈیٹابیس کو بحال کرنا (5)**

**7. متاثرہ نیٹ ورک سسٹمز کو منقطع کرنا (7)**

## عمودی

**1. صاف فائل کے بھیس میں نقصان دہ فائل (5)**

**3. نقصان دہ سافٹ ویئر چلانا (5)**

**4. فائلوں کو کرپٹوگرافی کے ذریعے مقفل کرنا (8)**

**5. نظام میں بڑی رکاوٹ کا واقعہ (5)**

# 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: منقطع آف لائن کاپی (9 حروف):**

**5 افقی: کرپٹوگرافک کلید کے بدلے ادائیگی کی درخواست (5 حروف):**

**6 افقی: بیک اپ سے ڈیٹابیس کو بحال کرنا (5 حروف):**

**7 افقی: متاثرہ نیٹ ورک سسٹمز کو منقطع کرنا (7 حروف):**

## عمودی

**1 عمودی: صاف فائل کے بھیس میں نقصان دہ فائل (5 حروف):**

**3 عمودی: نقصان دہ سافٹ ویئر چلانا (5 حروف):**

**4 عمودی: فائلوں کو کرپٹوگرافی کے ذریعے مقفل کرنا (8 حروف):**

**5 عمودی: نظام میں بڑی رکاوٹ کا واقعہ (5 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 | ح | ہ | ب | ت | س | ن | ٹ | ٹ | ل | ج | گ | ی | ر | چ |
| س | و | ا | ف | ہ | ل | ب | ر | ح | د | ر | ے | س | ڈ | چ |
| ہ | پ | ک | ن | چ | ح | ڈ | و | ن | ع | گ | ڈ | س | و | ٹ |
| ہ | ے | پ | ل | ا | ن | ڈ | ج | ن | ک | و | ل | ج | ل | ر |
| ڈ | ت | م | ل | پ | ب | ا | ن | ب | ک | س | ش | ٹ | ے | ی |
| گ | ب | ی | و | ت | ش | ے | ع | ڈ | و | ش | ع | س | پ | ش |
| ن | ا | گ | گ | چ | م | ل | ن | ش | ل | گ | گ | ر | ت | س |
| ہ | ہ | د | ل | ن | ی | ہ | پ | چ | ڈ | ی | ے | ہ | و | ن |
| ش | ی | چ | ف | ح | ح | پ | خ | ح | ب | ی | ت | ف | ب | ا |
| ا | ب | ے | د | پ | م | ڈ | و | ت | ی | گ | ت | ح | د | و |
| ا | ش | گ | ت | ل | ح | ی | ر | ا | ک | ہ | ی | ف | خ | ا |
| ر | ی | ٹ | گ | ن | و | ت | ر | چ | ا | ج | ت | ل | ت | ت |
| ے | ن | گ | م | و | ا | ٹ | خ | پ | و | ج | ی | ح | ہ | |
| ر | ف | ڈ | ہ | چ | ب | ع | گ | پ | ہ | ے | ہ | س | ن | ڈ |
| م | ی | ک | ک | س | و | گ | ر | چ | ش | ع | ع | ح | و | ا |

### الفاظ کی فہرست

خفیہکاری
پےلوڈ
کولڈبیکاپ
علیحدگی
تاوان
بحالی
تباہی
ٹروجن

## 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.** خفیہکاری |
| **B.** پےلوڈ |
| **C.** کولڈبیکاپ |
| **D.** علیحدگی |
| **E.** تاوان |
| **F.** بحالی |
| **G.** تباہی |
| **H.** ٹروجن |

| تعریفیں اور ملان کے خانے | |
| --- | --- |
| 1. منقطع آف لائن کاپی۔ | |
| 2. صاف فائل کے بھیس میں نقصان دہ فائل۔ | |
| 3. فائلوں کو کرپٹوگرافی کے ذریعے مقفل کرنا۔ | |
| 4. کرپٹوگرافک کلید کے بدلے ادائیگی کی درخواست۔ | |
| 5. متاثرہ نیٹ ورک سسٹمز کو منقطع کرنا۔ | |
| 6. نظام میں بڑی رکاوٹ کا واقعہ۔ | |
| 7. نقصان دہ سافٹ ویئر چلانا۔ | |
| 8. بیک اپ سے ڈیٹابیس کو بحال کرنا۔ | |

## 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. ر ہ ک خ ا ف ی ی
2. پ ک ا ڈ و ی ک ب ل
3. و ت ن ا ا
4. ا ی ہ ت ب
5. ل ڈ پ و ے
6. گ ی د ع ح ی ل
7. ل ی ب ا ح
8. ن ٹ و ج ر

# اضافی سرگرمی: تیزی سے سوچیں

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

| | | | |
|---|---|---|---|
| 1 | وہ معلومات جو آپ کو کبھی شیئر نہیں کرنی چاہئیں | | |
| 2 | وہ ڈیوائسز جنہیں ہیک کیا جا سکتا ہے | | |
| 3 | تاوان ادا نہ کرنے کی وجوہات | | |
| 4 | محفوظ عادات جو آپ آج شروع کر سکتے ہیں | | |
| 5 | آپ کے جانے پہچانے سیکیورٹی ٹولز کے نام | | |
| 6 | اپنے اکاؤنٹس کو محفوظ رکھنے کے طریقے | | |
| 7 | کمپیوٹر کے متاثر ہونے کی علامات | | |
| 8 | بیک اپ رکھنے کے مقامات | | |
| 9 | وہ فائلیں جنہیں آپ کبھی کھونا نہیں چاہتے | | |
| 10 | رینسم ویئر کے پھیلنے کے طریقے | | |
| 11 | حملے کے پہلے گھنٹے میں کرنے کے کام | | |
| 12 | حملے کے دوران رابطہ کرنے والے لوگ | | |
| 13 | وہ چیزیں جنہیں رینسم ویئر لاک کر سکتا ہے | | |
| 14 | سائبر سیکیورٹی سے متعلق الفاظ | | |
| 15 | وہ ادارے جنہیں اکثر نشانہ بنایا جاتا ہے | | |

# 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: انٹرپرائز رینسم ویئر پے لوڈ کی روک تھام



**منظرنامہ: ایک کارپوریٹ لوکل ایریا نیٹ ورک فعال رینسم ویئر کی زد میں آ گیا ہے۔** اہم فائل سرورز پر .locked کے ساتھ فائل ایکسٹینشنز نظر آنے لگی ہیں۔

**بحث کا سوال:** کنٹینمنٹ کے اقدامات تفصیل سے بیان کریں، اور ڈیٹا ریکوری کا پروٹوکول بیان کریں۔

### کیس اسٹڈی 2: آف لائن بیک اپ آرکیٹیکچرز کا جائزہ



**منظرنامہ:** ایک انٹرپرائز ڈیٹا بیک اپ کی ایسی حکمت عملی ڈیزائن کرنا چاہتا ہے جو بیک اپس کے سمجھوتے کا شکار ہونے کا خطرہ کم کرے، چاہے بنیادی لوکل نیٹ ورک پر رینسم ویئر مکمل طور پر قبضہ کر لے۔

**بحث کا سوال: ایک محفوظ آف لائن بیک اپ اسٹوریج والٹ سسٹم ڈیزائن 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

| 1 | 5 | 37 | 12 | | 38 | 18 | | 3 | 1 | 28 | 37 | 2 | | 12 | 30 | 34 | 28 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | |

| 33 | 37 | 14 | 28 | | 30 | 1 | 9 | 2 |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |

**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: رینسم ویئر کیا ہے؟

رینسم ویئر ایک نقصان دہ سافٹ ویئر ہے جو کمپیوٹر سسٹمز یا فائلوں تک رسائی اس وقت تک بلاک کرنے کے لیے بنایا گیا ہے جب تک تاوان کی رقم ادا نہ کی جائے۔

### Q2: رینسم ویئر کیسے پھیلتا ہے؟

ای میل فشنگ اٹیچمنٹس، بغیر پیچ والی سافٹ ویئر کمزوریوں اور متاثرہ ریموٹ رسائی کے سسٹمز کے ذریعے۔ [1]

### Q3: ادائیگی کرپٹو کرنسی میں کیوں مانگی جاتی ہے؟

Bitcoin جیسی کرپٹو کرنسیاں نسبتاً گمنامی فراہم کرتی ہیں، جس سے قانون نافذ کرنے والے اداروں کے لیے رقم کا سراغ لگانا مشکل ہو جاتا ہے۔

### Q4: کیا اینٹی وائرس رینسم ویئر کو بلاک کرتا ہے؟

جی ہاں، لیکن دستخط پر مبنی اینٹی وائرس نئے بنائے گئے زیرو ڈے رینسم ویئر پے لوڈز کے خلاف ناکام ہو سکتا ہے۔

### Q5: ایئر گیپڈ بیک اپ کیا ہے؟

بیک اپ کی ایسی کاپی جس کا بنیادی نیٹ ورک سے کوئی فزیکل یا منطقی تعلق نہ ہو، تاکہ وہ پھیلاؤ سے محفوظ رہے۔

# 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: ڈبل ایکسٹورشن کیا ہے؟

جب حملہ آور نہ صرف فائلیں خفیہ کرتے ہیں بلکہ حساس ڈیٹا بھی چرا لیتے ہیں تاکہ ادائیگی نہ ہونے پر عوامی طور پر لیک کرنے کی دھمکی دے سکیں۔

### Q7: ڈیکرپٹر کیا ہے؟

سافٹ ویئر یوٹیلیٹی جس میں لاک شدہ فائلوں کو سادہ متن میں بحال کرنے کے لیے درکار خفیہ کاری کلید ہوتی ہے۔

### Q8: آپ رینسم ویئر کا جلد پتا کیسے لگاتے ہیں؟

اچانک بڑے پیمانے پر فائلوں میں ترمیم اور نام تبدیل کرنے کی سرگرمی کے لیے فائل سسٹمز کی نگرانی کر کے۔

### Q9: انشورنس کا کیا کردار ہے؟

سائبر انشورنس بحالی کے اخراجات پورے کرنے میں مدد دے سکتی ہے، لیکن کوریج کی شرائط اور تاوان کی ادائیگی کے قواعد پالیسی کے لحاظ سے مختلف ہوتے ہیں۔

### Q10: کیا مجھے متاثرہ سسٹم کو ری بوٹ کرنا چاہیے؟

نہیں، ری بوٹ کرنے سے عارضی میموری کے شواہد ضائع ہو سکتے ہیں؛ اس کے بجائے اسے نیٹ ورک سے الگ کر دیں۔ [1]

# 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: رینسم ویئر غیر متناسب خفیہ کاری کیسے استعمال کرتا ہے؟**

یہ فائلوں کو خفیہ کرنے کے لیے میل ویئر میں شامل عوامی کلید استعمال کرتا ہے، اور انہیں ڈی کرپٹ کرنے کے لیے حملہ آور کی نجی کلید درکار ہوتی ہے۔

**Q2: سمیٹرک خفیہ کاری بھی کیوں استعمال کی جاتی ہے؟**

سمیٹرک خفیہ کاری (جیسے AES) تیز ہے اور بڑے ڈیٹا بیسز کو منٹوں میں مقفل کر سکتی ہے، جبکہ ایسمیٹرک کیز AES کلید کو محفوظ بناتی ہیں۔

**Q3: منطقی تقسیم کیا ہے؟**

نیٹ ورکس کو الگ تھلگ زونز میں تقسیم کرنا، جس سے میل ویئر ورک اسٹیشن نوڈز سے مرکزی سرورز تک پہلو بہ پہلو نہیں پھیلتا۔

**Q4: WORM اسٹوریج کیا ہے؟**

ایک بار لکھیں، بار بار پڑھیں (Write-Once, Read-Many) میڈیا، جو بیک اپ ڈیٹا کو رینسم ویئر پے لوڈز کے ذریعے ایڈٹ، اوور رائٹ یا حذف ہونے سے روکتا ہے۔

**Q5: شیڈو کاپیاں کیا ہیں؟**

Windows کے بنائے ہوئے مقامی بیک اپ اسنیپ شاٹس؛ رینسم ویئر عموماً ایڈمنسٹریٹو ٹولز کے ذریعے سب سے پہلے انہیں حذف کرتا 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: اسناد کی چوری رینسم ویئر کو کیسے ممکن بناتی ہے؟**

حملہ آور لیک شدہ ایڈمن لاگ اِنز خرید کر ریموٹ ڈیسک ٹاپس کے ذریعے سائن اِن کرتے ہیں اور پورے نیٹ ورک میں دستی طور پر رینسم ویئر چلاتے ہیں۔

**Q7: ڈرائی رن بحالی ٹیسٹنگ کیا ہے؟**

بیک اپ ڈیٹا بیسز کو باقاعدگی سے الگ تھلگ ٹیسٹ ماحول میں بحال کرنا تاکہ تصدیق ہو کہ بحالی کی رفتار اور ڈیٹا کی سالمیت ڈیزاسٹر کے معیارات پر پوری اترتی ہے۔

**Q8: اینڈ پوائنٹ ڈیٹیکشن (EDR) رینسم ویئر کو کیسے روکتی ہے؟**

پروسیس کے رویے (مثلاً تیز خفیہ کاری) کا تجزیہ کر کے اور سرکش ایپلی کیشن کو فوراً معطل کر کے۔

**Q9: رینسم ویئر-ایز-اے-سروس (RaaS) ماڈل کیا ہے؟**

فرنچائز ماڈل جس میں میل ویئر ڈیولپرز ادائیگیوں کے ایک فیصد کے بدلے رینسم ویئر بلڈرز ملحقہ افراد کو کرائے پر دیتے ہیں۔

**Q10: غیر پیچ شدہ RDP رینسم ویئر کو کیسے متحرک کرتا ہے؟**

کھلے ہوئے، بغیر پیچ والے Remote Desktop Protocol گیٹ ویز حملہ آوروں کو لاگ اِنز پر بروٹ فورس کرنے اور دستی طور پر میل ویئر چلانے کی اجازت دیتے ہیں۔

# 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

رینسم ویئر کے عناصر اکثر Windows شیڈو کاپیاں مٹانے اور مقامی بحالی کو روکنے کے لیے vssadmin.exe جیسے ٹولز استعمال کرتے ہیں۔ [1]

### 2. سیکیورٹی بصیرت

سمیٹرک AES-256 کیز عموماً فائل پے لوڈز کو خفیہ کرنے کے لیے استعمال ہوتی ہیں، جنہیں پھر پبلک RSA کیز سے مقفل کیا جاتا ہے۔

### 3. سیکیورٹی بصیرت

کامیاب رینسم ویئر حملے سے بحالی میں ہفتے لگ سکتے ہیں، اسی لیے آزمائے ہوئے آف لائن بیک اپس اہم ہیں۔

### 4. سیکیورٹی بصیرت

FBI تاوان ادا کرنے کی حمایت نہیں کرتا اور خبردار کرتا ہے کہ ادائیگی اس بات کی ضمانت نہیں دیتی کہ آپ کا ڈیٹا واپس مل جائے گا۔ [2]

### 5. سیکیورٹی بصیرت

ڈیزاسٹر ریکوری پلانز (DRP) میں ریکوری ٹائم آبجیکٹو (RTO) اور ریکوری پوائنٹ آبجیکٹو (RPO) متعین ہونے چاہییں۔

### 6. سیکیورٹی بصیرت

FBI ایسے بیک اپس کی سفارش کرتا ہے جو خفیہ کردہ اور ناقابلِ تغیر ہوں، یعنی انہیں تبدیل یا حذف نہ کیا جا سکے۔ [3]

### 7. سیکیورٹی کی بصیرت

رینسم ویئر ڈویلپرز روایتی سگنیچر پر مبنی اینٹی وائرس اسکینرز کو بائی پاس کرنے کے لیے جدید اوبفسکیشن تکنیکیں استعمال کرتے ہیں۔

### 8. سیکیورٹی کی بصیرت

نیٹ ورک سیگمنٹیشن پہلو بہ پہلو حرکت کو محدود کرتی ہے، جس سے رینسم ویئر کو پہلے متاثرہ ہوسٹ سے آگے پھیلنے سے روکنے میں مدد ملتی ہے۔ [3]

### 9. سیکیورٹی کی بصیرت

کھلی ہوئی، کمزور طور پر محفوظ ریموٹ سروسز جیسے Remote Desktop Protocol (RDP) رینسم ویئر کے داخلے کا عام راستہ ہیں۔ [1]

### 10. سیکیورٹی بصیرت

CISA مشورہ دیتا ہے کہ خفیہ شدہ بیک اپس کو آف لائن رکھا جائے، کیونکہ رینسم ویئر کی کئی اقسام قابلِ رسائی بیک اپس کو تلاش کر کے حذف کر دیتی ہیں۔ [1]

# 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] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[2] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/Ransomware

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[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

## جوابی کلید: چیک پوائنٹ 1 – کثیر انتخابی

**1 سوال 1**

درست جواب: A

**تدریسی نوٹ**

رینسم ویئر حملے کا بنیادی طریقہ کار کیا ہے؟ → سسٹم تک رسائی روکنے کے لیے صارف کی فائلوں کی خفیہ کاری

**2 سوال 2**

درست جواب: A

**تدریسی نوٹ**

آف لائن (کولڈ) بیک اپ کیا ہے؟ → اسٹوریج کاپی جو میل ویئر کے پھیلاؤ سے بچانے کے لیے نیٹ ورک سے منقطع ہو

**3 سوال 3**

درست جواب: A

**تدریسی نوٹ**

رینسم ویئر حملے کے دوران سیکیورٹی ٹیموں کو متاثرہ سسٹمز کو کیسے الگ کرنا چاہیے؟ → نیٹ ورک کیبلز فوراً منقطع کریں اور وائرلیس انٹرفیسز بند کر دیں

**4 سوال 4**

درست جواب: A

**تدریسی نوٹ**

سیکیورٹی ایجنسیاں رینسم ویئر کے مطالبات ادا کرنے کے خلاف مشورہ کیوں دیتی ہیں؟ → رقم ادا کرنا حملہ آوروں کی حوصلہ افزائی کرتا ہے اور ڈی کرپشن کلید ملنے کی ضمانت نہیں دیتا

**5 سوال 5**

درست جواب: A

**تدریسی نوٹ**

ڈیزاسٹر ریکوری پلان (DRP) کیا ہے؟ → سسٹم سمجھوتے کے بعد آپریشنز اور ڈیٹا بحال کرنے کا منظم عمل

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

**6 سوال 6**

درست جواب: درست

### تدریسی نوٹ

رینسم ویئر پے لوڈز نیٹ ورک سے جڑے آن لائن بیک اپس تک آسانی سے پھیل سکتے ہیں۔

**7 سوال 7**

درست جواب: غلط

### تدریسی نوٹ

غلط: FBI خبردار کرتا ہے کہ ادائیگی کرنے سے آپ کو کوئی ڈیٹا واپس ملنے کی ضمانت نہیں ملتی۔

**8 سوال 8**

درست جواب: درست

### تدریسی نوٹ

درست: CISA متاثرہ ہوسٹس کو ان پلگ کرنے یا نیٹ ورک کو آف لائن کرنے کا مشورہ دیتا ہے تاکہ پھیلاؤ پر قابو پایا جا سکے۔

**9 سوال 9**

درست جواب: غلط

### تدریسی نوٹ

غلط: رینسم ویئر عموماً فائلوں کو AES جیسے تیز سیمیٹرک سائفرز سے خفیہ کرتا ہے۔

**10 سوال 10**

درست جواب: درست

### تدریسی نوٹ

ڈیٹا بحالی کے طریقہ کار کی باقاعدہ جانچ ڈیزاسٹر ریکوری کا ایک اہم حصہ 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

| | | | |
|---|---|---|---|
| C 1. خفیہ کاری | E 2. پے لوڈ | F 3. کولڈ بیک اپ | A 4. علیحدگی |
| H 5. تاوان | G 6. بحالی | D 7. آفت | B 8. ٹروجن |

## چیک پوائنٹ 3: جوابی کلید – اہم اصطلاحات

| | | | |
|---|---|---|---|
| 1 خفیہ کاری | 2 پے لوڈ | 3 کولڈ بیکاپ | 4 علیحدگی |
| 5 تاوان | 6 بحالی | | |

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

| | | | |
|---|---|---|---|
| 1 C – کولڈبیکاپ | 2 H – ٹروجن | 3 A – خفیہکاری | 4 E – تاوان |
| 5 D – علیحدگی | 6 G – تباہی | 7 B – پےلوڈ | 8 F – بحالی |

### اساتذہ کے لیے بحث کے نوٹس

**اہم اصطلاحات:**
یقینی بنائیں کہ طلبہ خفیہ کاری، پے لوڈ اور کولڈ بیک اپ 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۔

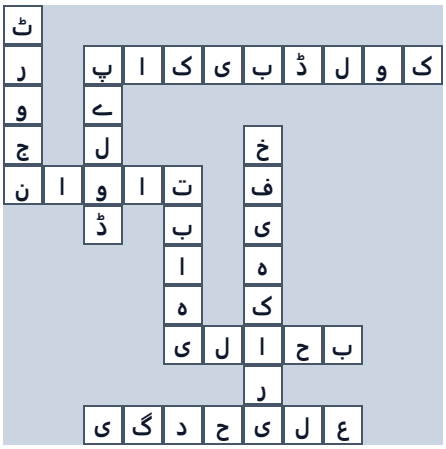
**ماخذ کی جانچ:**
طلبہ سے کہیں کہ ورک شیٹ کے ماخذ میں کم از کم ایک دعوے کی تصدیق کریں، اور اس پر بات کریں کہ اعداد و شمار، قیمتیں اور قواعد وقت کے ساتھ کیوں بدل سکتے ہیں۔

# پہیلیوں کی کلیدیں اور استاد کے نوٹس

## الفاظ کی تلاش کا حل

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ا | ح | ہ | ب | ت | س | ن | ٹ | ٹ | ل | چ | گ | ی | ر | چ |
| س | و | ا | ف | ہ | ل | ب | ر | ح | د | ر | ے | س | ڈ | چ |
| ہ | پ | ک | ن | چ | ح | ڈ | و | ن | ع | گ | ڈ | س | و | ٹ |
| ہ | ے | پ | ل | ا | ن | ڈ | چ | ن | ک | و | ل | چ | ل | ر |
| ڈ | ت | م | ل | پ | ب | ا | ن | ب | ک | س | ش | ٹ | ے | ی |
| گ | ب | ی | و | ت | ش | ے | ع | ڈ | و | ش | ع | س | پ | ش |
| ن | ا | گ | گ | چ | م | ل | ن | ش | ل | گ | گ | ر | ت | س |
| ہ | ہ | د | ل | ن | ی | ہ | پ | چ | ڈ | ی | ے | ہ | و | ن |
| ش | ی | چ | ف | ح | ح | پ | خ | ح | ب | ی | ت | ف | ب | ا |
| ا | ب | ے | د | پ | م | ڈ | و | ت | ی | گ | ت | ح | د | و |
| ا | ش | گ | ت | ل | ح | ی | ر | ا | ک | ہ | ی | ف | خ | ا |
| ر | ی | ت | گ | ن | و | ت | ر | چ | ا | چ | ت | ل | ت | ت |
| ے | ن | گ | م | ا | ا | و | ٹ | خ | پ | و | چ | ی | ح | ہ |
| ر | ف | ڈ | ہ | چ | ب | ع | گ | پ | ہ | ے | ہ | س | ن | ڈ |
| م | ی | ک | ک | س | و | گ | ر | چ | ش | ع | ع | ح | و | ا |

## کراس ورڈ کا حل




## کراس ورڈ حل کے لیے استاد کی گائیڈ

### افقی

**2 افقی: کولڈبیکاپ** منقطع آف لائن کاپی (9 حروف)

**5 افقی: تاوان** کرپٹوگرافک کلید کے بدلے ادائیگی کی درخواست (5 حروف)

**6 افقی: بحالی** بیک اپ سے ڈیٹابیس کو بحال کرنا (5 حروف)

**7 افقی: علیحدگی** متاثرہ نیٹ ورک سسٹمز کو منقطع کرنا (7 حروف)

### عمودی

**1 عمودی: ٹروجن** صاف فائل کے بھیس میں نقصان دہ فائل (5 حروف)

**3 عمودی: پےلوڈ** نقصان دہ سافٹ ویئر چلانا (5 حروف)

**4 عمودی: خفیہکاری** فائلوں کو کرپٹوگرافی کے ذریعے مقفل کرنا (8 حروف)

**5 عمودی: تباہی** نظام میں بڑی رکاوٹ کا واقعہ (5 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. رہکخافیی → خفیہکاری
2. پکاڈویکبل → کولڈبیکاپ
3. وتناا → تاوان
4. ایہتب → تباہی
5. لڈپوے → پےلوڈ
6. گیدعحیل → علیحدگی
7. لیباح → بحالی
8. نٹوجر → ٹروجن

### خفیہ سائفر چیلنج کی کلید

**"کولڈ بیکاپ سے ڈیٹا بحال کریں"**

# کیس اسٹڈیز کی جوابی کلید

## A کیس اسٹڈی 1: انٹرپرائز رینسم ویئر پے لوڈ کی روک تھام

استاد کا حل

### گریڈنگ کی ہدایت

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

- منظرنامے کا تجزیہ: ایک کارپوریٹ لوکل ایریا نیٹ ورک میں فعال رینسم ویئر داخل ہو گیا ہے۔ اہم فائل سرورز پر فائل ایکسٹینشنز .locked کے ساتھ دکھائی دینے لگی ہیں۔
- تجویز کردہ حکمت عملی اور حل: تمام متاثرہ سرورز کو لوکل ایریا نیٹ ورک سے منقطع کریں۔ فعال انتظامی سیشنز ختم کریں۔ غیر متاثرہ فائلیں محفوظ، رائٹ لاکڈ آف لائن بیک اپ سسٹم سے بحال کریں۔

## B کیس اسٹڈی 2: آف لائن بیک اپ آرکیٹیکچرز کا جائزہ

استاد کا حل

### گریڈنگ کی ہدایت

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

- منظرنامے کا تجزیہ: ایک انٹرپرائز ڈیٹا بیک اپ کی ایسی حکمت عملی بنانا چاہتی ہے جو اس خطرے کو کم کرے کہ اگر بنیادی مقامی نیٹ ورک مکمل طور پر رینسم ویئر کے قبضے میں آ جائے تب بھی بیک اپس متاثر نہ ہوں۔
- تجویز کردہ حکمت عملی اور حل: ایک بار لکھیں، بار بار پڑھیں (WORM) اسٹوریج نافذ کریں۔ بیک اپ سسٹم کو تمام نیٹ ورکس سے منقطع کر کے منطقی ایئر گیپ بنائیں، اور روزانہ فزیکل میڈیا کی تبدیلی نافذ کریں۔