نام: _____ تاریخ: _____ نمره: _____

# مبانی امنیت سایبری و تهدیدهای آنلاین پیشگیری

تهدیدهای امنیت سایبری، دیوارهای آتش شبکه، احراز هویت چندعاملی، چارچوب‌های امنیتی

## مرور آموزشی مبانی امنیت سایبری

**خوش آمدید!** این بستهٔ فعالیت شما را در آشنایی با اصول بنیادین مبانی امنیت سایبری و پیشگیری از تهدیدهای آنلاین راهنمایی می‌کند. با تهدیدهای بدافزار، احراز هویت چندعاملی، دیوارهای آتش شبکه و چارچوب‌های واکنش به رخداد آشنا می‌شوید.

**ایستگاه‌های بررسی کاربرگ**

- [ ] **بخش 1-4: بر امنیت سایبری و پیشگیری از تهدید مسلط شوید.**
- [ ] **بخش 5-7: جدول‌های متقاطع و جدول‌های جست‌وجوی کلمه را حل کنید.**
- [ ] **بخش 8-9: مطالعات موردی و چالش رمز را حل کنید.**
- [ ] **بخش 10: صفحه‌های پرسش‌های متداول مقدماتی و پیشرفته را مرور کنید.**
- [ ] **بخش 11: 10 واقعیت جالب دنیای واقعی را کاوش کنید.**
- [ ] **تکمیلی: چالش سریع فکر کن**

**ایمن‌شده**
رمزگذاری داده
استاندارد AES 256 بیتی

**منطبق**
استانداردهای جهانی
چارچوب‌های GDPR و CCPA

**اعتماد صفر**
سیاست دسترسی
احراز هویت چندعاملی

باز کردن راهنمای امنیت سایبری VPN.com

URL: https://www.vpn.com/cybersecurity/

# نقشهٔ راه یادگیری مبانی امنیت سایبری شما

- بردارهای رایج بدافزار، فیشینگ و نفوذ به شبکهٔ سازمانی را شناسایی کنید.
- کنترل‌های استاندارد امنیت سایبری، از جمله MFA، دیوارهای آتش و دفاع نقطه پایانی را پیاده‌سازی کنید.
- رویه‌های پاسخ به رخداد را برای کاهش تأثیر نقض داده ارزیابی کنید.
- عوامل ریسک سازمانی و هم‌راستایی امنیتی را تحت رهنمودهای NIST تحلیل کنید.
- روش‌های بهداشت امنیتی را برای کاهش پر کردن خودکار اعتبارنامه پیکربندی کنید.

### دستورالعمل‌های راهنمای امنیت سایبری

به پرسش‌های چندگزینه‌ای و درست/نادرست پاسخ دهید، جمله‌های جای‌خالی را با استفاده از بانک واژه‌ها کامل کنید، تعاریف را تطبیق دهید و جدول‌های کلمات متقاطع و جست‌وجوی کلمه را حل کنید. دانسته‌های خود را درباره پیشگیری از تهدیدها به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

### مبانی امنیت سایبری و پیشگیری از تهدید (مقدمه)

امنیت سایبری از شبکه‌ها، سیستم‌ها و داده‌ها در برابر حملات دیجیتال غیرمجاز محافظت می‌کند. ایجاد عادت‌های امنیتی قوی، پیکربندی دیوارهای آتش، الزام احراز هویت چندعاملی و آموزش کارکنان در شناخت تهدیدها از اجزای ضروری دفاع از شبکهٔ سازمانی هستند.

**هر ایستگاه بررسی را با دقت بخوانید و پاسخ درست را انتخاب کنید یا بنویسید.**

# ایستگاه بررسی 1: چالش چندگزینه‌ای

**1. هدف اصلی حملهٔ فیشینگ چیست؟**

- A. سرقت اعتبارنامه‌ها و داده‌های حساس کاربر
- B. بهبود دیده‌شدن وب‌سایت در موتورهای جست‌وجو
- C. افزایش ظرفیت پهنای باند شبکه
- D. مدیریت تکثیر مرکز دادهٔ پشتیبان

**2. کدام سازوکار قوی‌ترین حفاظت از حساب را فراهم می‌کند؟**

- A. احراز هویت چندعاملی با کلیدهای سخت‌افزاری
- B. گذرواژه‌های پیچیده که هر سی روز به‌روزرسانی می‌شوند
- C. محدود کردن ورود به حساب به ساعات کاری
- D. پنهان کردن نام کاربری حساب از فهرست‌های عمومی

**3. چه چیزی بار آلوده‌کنندهٔ باج‌افزار را تعریف می‌کند؟**

- A. رمزگذاری فایل‌های سیستم و مطالبهٔ پول
- B. ثبت پنهانی ضربه‌های صفحه‌کلید روی سرورهای راه دور
- C. تزریق تبلیغات غیرمجاز به مرورگرها
- D. استفاده از منابع CPU محلی برای استخراج رمزارز

**4. یک اکسپلویت روز-صفر چگونه بر دفاع‌های امنیتی تأثیر می‌گذارد؟**

- A. آسیب‌پذیری‌های وصله‌نشده و ناشناخته را هدف می‌گیرد
- B. دیوار آتش سازمانی را به‌طور خودکار غیرفعال می‌کند
- C. سیستم را وادار به راه‌اندازی مجدد اجباری می‌کند
- D. برای رفع آن به بودجهٔ صفر نیاز است

**5. کدام چارچوب بر کنترل‌های امنیتی سازمانی حاکم است؟**

- A. رهنمودهای چارچوب امنیت سایبری NIST
- B. مشخصات طرحوارهٔ سند W3C HTML5
- C. دفترچه‌های راهنمای نصب درایور چاپگر
- D. تعریف‌های پروتکل مسیریابی IETF

# ایستگاه بررسی 2: چالش درست یا نادرست

### 6 پرسش درست/نادرست 6

6. حملات فیشینگ فقط حساب‌های ایمیل شخصی را هدف می‌گیرند.

○ درست ○ نادرست

### 7 پرسش درست/نادرست 7

7. احراز هویت چندعاملی (MFA) به مسدود کردن حملات credential stuffing کمک می‌کند.

○ درست ○ نادرست

### 8 پرسش درست/نادرست 8

8. دیوار آتش ترافیک شبکه را بررسی می‌کند تا دسترسی غیرمجاز به درگاه‌ها را مسدود کند.

○ درست ○ نادرست

### 9 پرسش درست/نادرست 9

9. رفع بهره‌برداری‌های روز صفر به به‌روزرسانی‌های استاندارد تعریف‌های آنتی‌ویروس نیاز دارد.

○ درست ○ نادرست

### 10 پرسش درست/نادرست 10

10. honeypot سرور طعمه‌ای است که برای فریب مجرمان سایبری به کار می‌رود.

○ درست ○ نادرست

# ایستگاه بررسی 3: درج اصطلاح کلیدی

هر جملهٔ زیر را بخوانید و جای خالی را با واژهٔ درست از بانک واژگان پر کنید.

1. مدیران شبکه برای پالایش ترافیک ورودی یک _____ نصب می‌کنند.
2. مهاجم از یک _____ روز صفر برای دور زدن وصله‌های سیستم استفاده می‌کند.
3. مهاجمان ایمیل‌های جعلی می‌فرستند تا علیه کارکنان کارزارهای _____ اجرا کنند.
4. باج‌افزار شکلی مخرب از _____ است که داده‌های کاربر را قفل می‌کند.
5. برقراری _____ قوی گذرواژه خطر سرقت اعتبارنامه را کاهش می‌دهد.
6. برای محافظت از ارتباطات حساس، کاربران پروتکل‌های _____ را به کار می‌گیرند.

**بانک واژگان**

بدافزار | بهداشت | بهره‌برداری | چارچوب | چندعاملی | دیوار آتش | رمزگذاری | فیشینگ

**پاسخ‌های خود را اینجا بنویسید:**

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

# ایستگاه بررسی 4: تطبیق مفاهیم امنیت

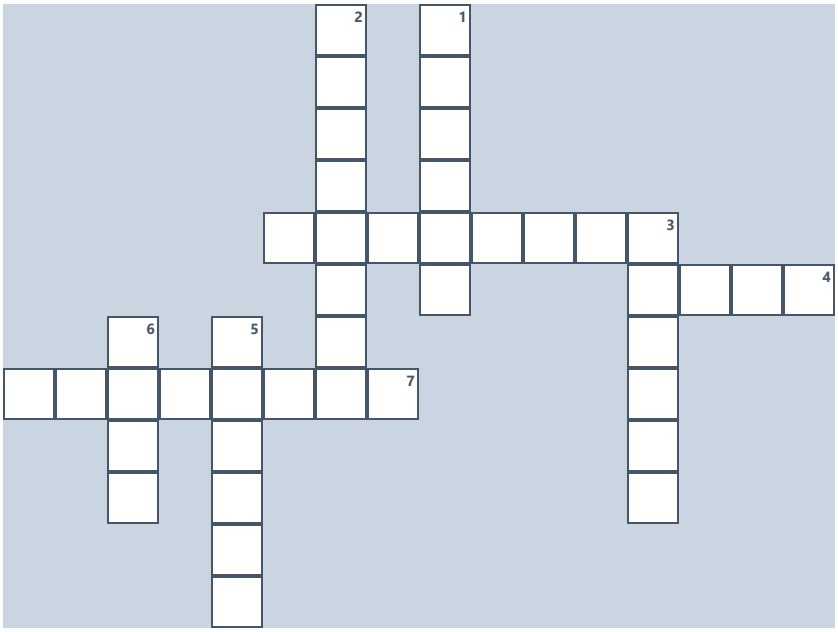
**تطبیق تعاریف**

هر اصطلاح واژگان در سمت راست را با نوشتن حرف متناظر (A-H) در کادر ورودی قابل‌پرکردن به تعریف درست آن در سمت چپ وصل کنید.

| | | |
|---|---|---|
| 1. تهدید باج‌افزار | A | رهنمودهای ساختاریافته مانند NIST که برای مدیریت خطرهای سایبری به کار می‌روند. |
| 2. احراز هویت چندعاملی | B | برنامهٔ ساختاریافته برای مدیریت و کاهش نقض‌های امنیتی. |
| 3. بهره‌برداری روز صفرم | C | مانع شبکه‌ای که ترافیک را بر اساس قواعد امنیتی فیلتر می‌کند. |
| 4. هانی‌پات فریب | D | بدافزاری که داده‌ها را رمزگذاری می‌کند و برای رمزگشایی پرداخت مالی می‌خواهد. |
| 5. دیوار آتش نفوذ | E | سوءاستفاده از آسیب‌پذیری پیش از انتشار وصلهٔ فروشنده. |
| 6. پاسخ به رخداد | F | بهترین روش‌ها برای مدیریت اعتبارنامه‌ها و کلیدهای احراز هویت. |
| 7. بهداشت گذرواژه | G | اعتبارسنجی امنیتی که دو یا چند عامل احراز هویت را الزامی می‌کند. |
| 8. چارچوب امنیتی | H | سیستم فریبی که برای جذب و تحلیل عوامل مخرب راه‌اندازی می‌شود. |

# ایستگاه بررسی 5: جدول‌کلمات

جدول کلمات متقاطع را با تایپ حروف در خانه‌های سفید فعال حل کنید. شماره‌ها با سرنخ‌های زیر مطابقت دارند.




## افقی

**3. بدافزاری که داده را رمزگذاری می‌کند و برای رمزگشایی پرداخت مالی می‌خواهد (8)**

**4. سیستم فریبی که برای جذب و تحلیل عوامل مخرب برپا می‌شود (4)**

**7. سد شبکه‌ای که ترافیک را بر اساس قواعد امنیتی پالایش می‌کند (8)**

## عمودی

**1. بهره‌برداری از آسیب‌پذیری پیش از انتشار وصلهٔ فروشنده (6)**

**2. اعتبارسنجی امنیتی که دو یا چند عامل احراز هویت می‌خواهد (8)**

**3. بهترین روش‌ها برای مدیریت اعتبارنامه‌ها و کلیدهای احراز هویت (6)**

**5. رهنمودهای ساختاریافته مانند NIST برای مدیریت خطرهای سایبری (6)**

**6. طرح ساختاریافته برای مدیریت و کاهش اثر رخنه‌های امنیتی (4)**

# ایستگاه بررسی 5 – فعالیت جایگزین: سرنخ‌های دسترس‌پذیر جدول‌کلمات

کاربران صفحه‌خوان و صفحه‌کلید می‌توانند پاسخ‌های جدول کلمات متقاطع را مستقیماً در فیلدهای متنی زیر تایپ کنند.

## افقی

**3 افقی: بدافزاری که داده را رمزگذاری می‌کند و برای رمزگشایی پرداخت مالی می‌خواهد (8 حرف):**

**4 افقی: سیستم فریبی که برای جذب و تحلیل عوامل مخرب برپا می‌شود (4 حرف):**

**7 افقی: سد شبکه‌ای که ترافیک را بر اساس قواعد امنیتی پالایش می‌کند (8 حرف):**

## عمودی

**1 عمودی: بهره‌برداری از آسیب‌پذیری پیش از انتشار وصلهٔ فروشنده (6 حرف):**

**2 عمودی: اعتبارسنجی امنیتی که دو یا چند عامل احراز هویت می‌خواهد (8 حرف):**

**3 عمودی: بهترین روش‌ها برای مدیریت اعتبارنامه‌ها و کلیدهای احراز هویت (6 حرف):**

**5 عمودی: رهنمودهای ساختاریافته مانند NIST برای مدیریت خطرهای سایبری (6 حرف):**

**6 عمودی: طرح ساختاریافته برای مدیریت و کاهش اثر رخنه‌های امنیتی (4 حرف):**

## ایستگاه بررسی 6: جدول کلمات پنهان

8 اصطلاح کلیدی واژگان را که در جدول زیر پنهان شده‌اند پیدا کنید. کلمات می‌توانند افقی، عمودی یا مورب باشند.

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ص | ر | ج | ض | چ | ظ | ز | ط | ث | پ | ف | ی | ا | خ | ر |
| گ | ف | ذ | ذ | ی | ض | ف | ع | چ | م | ب | ع | ز | چ | ز |
| ن | ص | ش | ه | ظ | و | ح | م | ظ | ا | س | ت | غ | ذ | ح |
| ص | ز | غ | ش | ظ | ن | ع | ه | ض | ت | ر | ک | ف | ق | چ |
| ژ | و | ر | پ | ا | ب | ب | پ | ط | و | پ | چ | ژ | ز | و |
| ژ | ر | ن | ک | ز | ا | ث | د | ع | ش | ر | ا | و | ث | ذ |
| ت | ص | ص | ژ | ع | چ | ظ | خ | ی | ش | ش | ع | س | ب | غ |
| ش | ف | ک | ک | خ | ا | پ | ف | ظ | و | ض | د | ف | خ | پ |
| ا | م | ث | ق | ه | ف | گ | ت | ی | م | ا | ح | ز | خ | ی |
| د | ث | ص | ث | ع | ز | ن | ظ | پ | گ | ب | ر | ا | ی | ض |
| ه | چ | ن | د | ع | ا | م | ل | ی | ث | ژ | ا | ا | ث | ض |
| ب | ث | چ | خ | ذ | ر | ث | غ | ع | ش | ج | ذ | ف | ت | ی |
| ق | چ | ع | ل | چ | ا | ا | ع | ط | ص | ظ | ک | و | ع | ش |
| ز | غ | ک | ف | ت | ص | ه | پ | ح | ف | ن | م | ر | ا | غ |
| ی | ه | ه | ژ | ح | ذ | ش | غ | ز | س | س | ق | ط | خ | ظ |

### فهرست واژگان

باجافزار چندعاملی روزصفر طعمه دیواراتش پاسخ بهداشت چارچوب

# ایستگاه بررسی 6 – فعالیت جایگزین: تطبیق دسترس‌پذیر واژگان

هر یک از 8 اصطلاح واژگان موجود در جدول کلمات پنهان را با نوشتن حرف (A-H) در جای خالی به تعریف درست آن وصل کنید.

| اصطلاحات واژگان |
|---|
| **A.** باجافزار |
| **B.** چندعاملی |
| **C.** روزصفر |
| **D.** طعمه |
| **E.** دیواراتش |
| **F.** پاسخ |
| **G.** بهداشت |
| **H.** چارچوب |

| | تعاریف و فیلدهای تطبیق |
|---|---|
| | 1. سد شبکه‌ای که ترافیک را بر اساس قواعد امنیتی پالایش می‌کند. |
| | 2. طرح ساختاریافته برای مدیریت و کاهش اثر رخنه‌های امنیتی. |
| | 3. بدافزاری که داده را رمزگذاری می‌کند و برای رمزگشایی پرداخت مالی می‌خواهد. |
| | 4. اعتبارسنجی امنیتی که دو یا چند عامل احراز هویت می‌خواهد. |
| | 5. بهترین روش‌ها برای مدیریت اعتبارنامه‌ها و کلیدهای احراز هویت. |
| | 6. رهنمودهای ساختاریافته مانند NIST برای مدیریت خطرهای سایبری. |
| | 7. بهره‌برداری از آسیب‌پذیری پیش از انتشار وصلهٔ فروشنده. |
| | 8. سیستم فریبی که برای جذب و تحلیل عوامل مخرب برپا می‌شود. |

## ایستگاه بررسی 7: چالش کلمات درهم‌ریخته

حروف زیر را مرتب کنید تا مفاهیم و اصطلاحات کلیدی امنیت سایبری آشکار شوند. پاسخ‌هایتان را در کادرهای ورودی ارائه‌شده بنویسید.

1. ا ا ف ب ز ا ر ج
2. ر ر ز ف ص و
3. ا ی د ر ا ش ت و
4. ت ا د ش ب ه
5. ا م ن ی ع چ ل د
6. م ه ط ع
7. س پ خ ا
8. ر ب چ و چ ا

# فعالیت تکمیلی: سریع فکر کن

برای هر دسته 3 پاسخ بنویسید. هر کس زودتر فهرست را کامل کند برنده است.

| | | | |
|---|---|---|---|
| 1 | شغل‌ها در امنیت سایبری | | |
| 2 | دلایل به‌روزرسانی نرم‌افزار | | |
| 3 | چیزهایی که یک دیوار آتش می‌تواند مسدود کند | | |
| 4 | نشانه‌های هشدار در یک ایمیل | | |
| 5 | چیزهایی که پشتیبان می‌گیرید | | |
| 6 | انواع شناخته‌شدهٔ حملهٔ سایبری | | |
| 7 | چیزهایی که یک **honeypot** می‌تواند جذب کند | | |
| 8 | اطلاعاتی که هرگز نباید به اشتراک بگذارید | | |
| 9 | نشانه‌های آلوده بودن رایانه | | |
| 10 | فیلم‌ها یا سریال‌هایی دربارهٔ هکرها | | |
| 11 | لایه‌های امنیتی که می‌توانید بسازید | | |
| 12 | چیزهایی که در یک رزمایش امنیتی تمرین می‌شوند | | |
| 13 | ابزارهای امنیتی که می‌شناسید | | |
| 14 | افرادی که می‌توانید برای کمک فناوری اطلاعات از آن‌ها بپرسید | | |
| 15 | واژه‌هایی که با «سایبر» شروع می‌شوند | | |

# ایستگاه بررسی 8: مطالعات موردی امنیت سایبری

مفاهیمی را که آموخته‌اید برای حل سناریوهای واقعی زیر به کار ببرید.

### مطالعهٔ موردی 1: راهبرد بازیابی از باج‌افزار



**سناریو:** یک شبکهٔ شرکتی به باج‌افزار آلوده می‌شود و پایگاه‌های دادهٔ حیاتی قفل می‌شوند. مهاجمان پرداخت $100,000 به ارز دیجیتال را طلب می‌کنند. شرکت پشتیبان‌های آفلاین مربوط به 24 ساعت پیش را دارد.

**پرسش برای بحث: خطرهای پرداخت را تحلیل کنید و راهبرد بازیابی را ارزیابی کنید.**

### مطالعهٔ موردی 2: دفاع در برابر پر کردن اعتبارنامه



**سناریو:** یک سرویس آنلاین دچار حملهٔ credential stuffing می‌شود و هکرها میلیون‌ها جفت نام کاربری/گذرواژهٔ دزدیده‌شده از سایت‌های دیگر را آزمایش می‌کنند.

**پرسش برای بحث:** سازوکار این حمله را شرح دهید و دو سامانهٔ دفاعی را بیان کنید.

# ایستگاه بررسی 9: رمزگشایی

متخصص امنیت سایبری از دارایی‌های شبکه در برابر عوامل تهدید آنلاین محافظت می‌کند. از کلید حرف-به-عدد زیر استفاده کنید و با نوشتن حرف‌های متناظر در جاهای خالی، پیام را رمزگشایی کنید.

**کلید رمزگذاری حرف به عدد**

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

ر=12 ز=13 ژ=14 س=15 ش=16 ص=17 ض=18 ط=19 ظ=20 ع=21 غ=22

ف=23 ق=24 ک=25 گ=26 ل=27 م=28 ن=29 و=30 ه=31 ی=32

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 10 | 30 | 12 | 30 | 1 | 2 | 28 | 4 | 15 | 32 | 15 |
| | | | | | | | | | | |
| 29 | 28 | 32 | 1 | 32 | 27 | 28 | 1 | 21 | 10 | 29 | 7 |
| | | | | | | | | | | | |

**پیام رمزگشایی‌شده:**

نکته: هر عدد نشان‌دهندهٔ یک حرف فارسی از کلید بالا است.

# ایستگاه بررسی 10: پرسش‌های متداول امنیت سایبری – مقدماتی (بخش A)

پرسش‌ها و پاسخ‌های رایج دربارهٔ کاهش تهدیدهای آنلاین را مرور کنید.

### Q1: هدف اصلی امنیت سایبری چیست؟

هدف اصلی محافظت از شبکه‌ها، دستگاه‌ها و داده‌ها در برابر دسترسی غیرمجاز، حملات و آسیب تصادفی است.

### Q2: فیشینگ چه تفاوتی با فیشینگ هدفمند دارد؟

فیشینگ یک کمپین ایمیلی گسترده است که کاربران تصادفی را هدف می‌گیرد، در حالی که فیشینگ هدفمند با استفاده از داده‌های شخصی‌سازی‌شده افراد مشخصی را هدف می‌گیرد.

### Q3: دیوار آتش شبکه چیست؟

دیوار آتش سامانهٔ امنیت شبکه است که ترافیک ورودی و خروجی را بر پایهٔ قواعد امنیتی از پیش تعریف‌شده پایش و فیلتر می‌کند.

### Q4: چرا احراز هویت چندعاملی (MFA) ضروری است؟

MFA لایهٔ دفاعی حیاتی اضافه می‌کند و حتی اگر مهاجمان اعتبارنامه‌های گذرواژهٔ اصلی را بدزدند یا بشکنند، مانع دسترسی می‌شود.

### Q5: ویروس رایانه‌ای را چه چیزی تعریف می‌کند؟

ویروس بدافزار خودتکثیرشونده‌ای است که خود را به فایل‌های سالم می‌چسباند و پس از اجرا در سیستم‌ها پخش می‌شود.

# ایستگاه بررسی 10: پرسش‌های متداول امنیت سایبری – مقدماتی (بخش B)

پرسش‌ها و پاسخ‌های رایج دربارهٔ کاهش تهدیدهای آنلاین را مرور کنید.

**Q6: باج‌افزار چگونه داده‌های محلی را قفل می‌کند؟**

باج‌افزار از الگوریتم‌های رمزنگاری برای رمزگذاری فایل‌های کاربر استفاده می‌کند و آن‌ها را تا زمان اعمال کلید رمزگشایی ناخوانا می‌سازد.

**Q7: آسیب‌پذیری روز صفر چیست؟**

zero-day نقص امنیتی در نرم‌افزار است که فروشنده از آن بی‌خبر است و پیش از سوءاستفاده زمانی برای تهیهٔ وصله باقی نمی‌گذارد.

**Q8: نقش چارچوب NIST چیست؟**

چارچوب NIST رهنمودها و استانداردهای داوطلبانه‌ای ارائه می‌دهد تا به سازمان‌ها در مدیریت و کاهش خطرهای امنیت سایبری کمک کند.

**Q9: طرح پاسخ به حوادث امنیتی چیست؟**

مجموعه‌ای مستند از رویه‌ها برای شناسایی، مهار و بازیابی از نقض‌های امنیتی و نفوذ به شبکه است.

**Q10: مهندسی اجتماعی چگونه از کاربران سوءاستفاده می‌کند؟**

مهندسی اجتماعی از دستکاری روانی استفاده می‌کند تا کارکنان را فریب دهد که گذرواژه‌ها را فاش کنند یا فایل‌های مخرب دانلود کنند.

# ایستگاه بررسی 10: پرسش‌های متداول امنیت – پیشرفته (بخش C)

جنبه‌های فنی پیشرفتهٔ چارچوب‌های امنیتی، تحلیل بدافزار و انطباق داده را بررسی کنید.

### Q1: حملهٔ DDoS چگونه سرورهای وب را از کار می‌اندازد؟

حملهٔ DDoS میلیون‌ها دستگاه آلوده در یک بات‌نت را هماهنگ می‌کند تا سرور را با ترافیک غرق کند و پهنای باند و محدودیت‌های CPU را تمام کند.

### Q2: تفاوت رمزگذاری متقارن و نامتقارن چیست؟

رمزگذاری متقارن از یک کلید واحد برای رمزگذاری و رمزگشایی استفاده می‌کند، در حالی که رمزگذاری نامتقارن از جفت‌کلید عمومی و خصوصی استفاده می‌کند.

### Q3: هکرها چگونه حملات تزریق SQL را اجرا می‌کنند؟

مهاجمان دستورهای SQL مخرب را در فیلدهای فرم وارد می‌کنند و پایگاه دادهٔ پشتیبان را فریب می‌دهند تا رکوردهای غیرمجاز کاربران را افشا کند.

### Q4: حرکت جانبی در نفوذ به شبکه چیست؟

تکنیکی است که در آن مهاجمان از دسترسی اولیه به سرور برای نفوذ به سایر سامانه‌های به‌هم‌پیوستهٔ شبکهٔ داخلی سوءاستفاده می‌کنند.

### Q5: جعل DNS چگونه ترافیک وب را منحرف می‌کند؟

جعل DNS رکوردهای حافظهٔ پنهان سرور نام را تغییر می‌دهد و کاربران قانونی را به‌جای دامنه‌های مقصد، به وب‌سایت‌های مخرب مشابه هدایت می‌کند.

# ایستگاه بررسی 10: پرسش‌های متداول امنیت – پیشرفته (بخش D)

جنبه‌های فنی پیشرفتهٔ چارچوب‌های امنیتی، تحلیل بدافزار و انطباق داده را بررسی کنید.

### Q6: توکن امنیتی سخت‌افزاری چیست؟

دستگاهی فیزیکی (مانند YubiKey) است که اثبات‌های احراز هویت رمزنگاری‌شده تولید می‌کند و حداکثر دفاع را در برابر فیشینگ از راه دور ارائه می‌دهد.

### Q7: تیم‌های امنیتی چگونه از هانی‌پات‌های فریب استفاده می‌کنند؟

تیم‌ها سرورهای طعمهٔ غیرتولیدی مستقر می‌کنند تا نفوذها را زود شناسایی و الگوهای حملهٔ عوامل غیرمجاز را تحلیل کنند.

### Q8: اصل کمترین امتیاز دسترسی چیست؟

استاندارد امنیتی محدود کردن حقوق دسترسی کاربر به حداقل مطلق لازم برای انجام نقش‌های کاری اوست.

### Q9: حملهٔ مرد میانی (Man-in-the-Middle) چگونه از اتصال‌ها سوءاستفاده می‌کند؟

مهاجم ارتباطات میان دو دستگاه را در شبکه‌های رمزگذاری‌نشده رهگیری و تغییر می‌دهد و توکن‌های نشست و اعتبارنامه‌ها را می‌دزدد.

### Q10: شاخص‌های نفوذ (IOC) چیست؟

IOCها سرنخ‌های دادهٔ قانونی (forensic) هستند، مانند تغییرات غیرعادی رجیستری یا ترافیک IP مخرب، که نشان می‌دهند سامانه نقض شده است.

# بخش 11: 10 واقعیت و بینش دنیای واقعی دربارهٔ امنیت سایبری

واقعیت‌های دنیای واقعی دربارهٔ نقض‌های امنیتی، سازوکارهای دفاعی و استانداردهای انطباق را مرور کنید.

**1. بینش امنیت**

مهاجمان پیوسته اینترنت را برای یافتن سرورهای آسیب‌پذیر اسکن می‌کنند و ایمیل‌های فیشینگ به صندوق ورودی کارکنان می‌فرستند.

**2. بینش امنیت**

خطای انسانی، مانند کلیک روی پیوندهای فیشینگ، عاملی رایج در نقض داده‌هاست و به همین دلیل آموزش اهمیت دارد.

**3. بینش امنیت**

هزینه‌های نقض داده شامل جریمه‌های حقوقی، ازدست‌رفتن مشتریان، بررسی و ترمیم است و می‌تواند به میلیون‌ها دلار برسد.

**4. بینش امنیت**

MFA مقاوم در برابر فیشینگ، مانند کلیدهای امنیتی سخت‌افزاری، قوی‌ترین نوع MFA و استانداردی است که CISA توصیه می‌کند. [2]

**5. بینش امنیت**

باج‌افزار همچنان تهدیدی عمده برای شبکه‌های سازمانی است و CISA پشتیبان‌های آفلاین و رمزگذاری‌شده را به‌عنوان دفاعی کلیدی توصیه می‌کند. [4]

**6. بینش امنیت**

چارچوب امنیت سایبری NIST نسخهٔ 2.0 (2024) شش کارکرد اصلی دارد: Govern، Identify، Protect، Detect، Respond، Recover. [1]

**7. بینش امنیت**

ربات‌های پر کردن اعتبارنامه جفت‌های نام کاربری و گذرواژهٔ لو رفته را در مقیاس بالا روی درگاه‌های ورود بانکی و تجارت الکترونیک آزمایش می‌کنند.

**8. بینش امنیت**

بازارهای اکسپلویت روز صفر در سراسر جهان وجود دارند که در آن‌ها آسیب‌پذیری‌های با شدت بالا می‌توانند پیش از وصله شدن به مبالغ زیادی فروخته شوند.

**9. بینش امنیت**

سامانهٔ طعمهٔ honeypot هشدارهای نفوذ را بلافاصله گزارش می‌کند، زیرا کاربران قانونی دلیلی برای دسترسی به آن ندارند.

**10. بینش امنیت**

Transport Layer Security (TLS) نشست‌های مرورگر را رمزگذاری می‌کند و از شنود بسته در شبکه‌های Wi-Fi عمومی جلوگیری می‌کند.

# منابع و مراجع فنی

راهنمای مطالعه و پازل‌های تعاملی از استانداردهای جهانی NIST، OWASP و انطباق با حریم خصوصی داده گردآوری شده‌اند.

## منابع علمی و صنعتی

[1] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

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

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

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

[6] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

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

[8] OWASP. (n.d.). SQL Injection.
https://owasp.org/www-community/attacks/SQL_Injection

## کلید پاسخ: ایستگاه بررسی 1 – چندگزینه‌ای

**1 حملات فیشینگ** فیشینگ — پاسخ درست: A

**نکتهٔ آموزشی**

کمپین‌های فیشینگ تلاش می‌کنند با ایمیل‌های جعلی اعتبارنامه‌ها و داده‌های حساس کاربران را بدزدند. منبع: OWASP Secure Configuration.

**2 حفاظت از حساب** کلید MFA — پاسخ درست: A

**نکتهٔ آموزشی**

احراز هویت چندعاملی (MFA) با توکن‌های سخت‌افزاری قوی‌ترین دفاع دسترسی به حساب را فراهم می‌کند. منبع: NIST Digital Identity.

**3 تهدید باج‌افزار** باج‌افزار — پاسخ درست: A

**نکتهٔ آموزشی**

باج‌افزار سیستم‌ها و داده‌های حیاتی را رمزگذاری می‌کند و برای کلیدهای رمزگشایی پرداخت رمزارزی طلب می‌کند. منبع: Center for Internet Security (CIS).

**4 آسیب‌پذیری روز صفر** روز صفر — پاسخ درست: A

**نکتهٔ آموزشی**

تهدیدهای روز صفر پیش از ارائهٔ وصلهٔ فروشنده، از نقص‌های امنیتی وصله‌نشده و ناشناخته سوءاستفاده می‌کنند. منبع: OWASP Secure Configuration.

**5 چارچوب‌های امنیتی** چارچوب‌ها — پاسخ درست: A

**نکتهٔ آموزشی**

چارچوب‌هایی مانند NIST رهنمودهای ساختاریافته‌ای ارائه می‌دهند که به سازمان‌ها در مدیریت و کاهش خطرهای سایبری کمک می‌کند. منبع: NIST Digital Identity.

## کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

**6 فیشینگ هدفمند** — فیشینگ — پاسخ درست: نادرست

### نکتهٔ آموزشی

حملات فیشینگ هم شبکه‌های شرکتی و هم حساب‌های شخصی را هدف می‌گیرند تا بردارهای بهره‌برداری را گسترش دهند. منبع: OWASP Secure Configuration.

**7 پرسش 7** — پاسخ درست: درست

### نکتهٔ آموزشی

MFA عامل دومی می‌خواهد، بنابراین گذرواژهٔ دزدیده‌شده به‌تنهایی معمولاً برای ورود کافی نیست.

**8 دیوار آتش ترافیک** — دیوار آتش — پاسخ درست: درست

### نکتهٔ آموزشی

دیوار آتش ترافیک را روی درگاه‌های مشخص شبکه بررسی و مسدود می‌کند تا اتصال‌های غیرمجاز را فیلتر کند. منبع: Center for Internet Security (CIS).

**9 واکنش به روز صفر** — روز صفر — پاسخ درست: نادرست

### نکتهٔ آموزشی

رفع حفره‌های روز صفر به وصله‌های کد و فیلتر WAF نیاز دارد، چون هنوز امضایی وجود ندارد. منبع: OWASP Secure Configuration.

**10 هانی‌پات‌های فریب** — هانی‌پات — پاسخ درست: درست

### نکتهٔ آموزشی

هانی‌پات‌ها سرورهای فریبنده‌ای هستند که تیم‌های امنیتی برای جذب، هشدار و مطالعهٔ عوامل مخرب از آنها استفاده می‌کنند. منبع: Center for Internet Security (CIS).

# کلیدهای واژگان و معیار نمره‌دهی

بارم‌بندی معلم: برای هر تطبیق درست (در مجموع 8 امتیاز) و اصطلاح بافتی (در مجموع 6 امتیاز) 1 امتیاز بدهید.

## ایستگاه بررسی 4: کلید پاسخ – تطبیق مفاهیم

| | | | |
|---|---|---|---|
| D 1. تهدید باج‌افزار | G 2. احراز هویت چندعاملی | E 3. بهره‌برداری روز صفرم | H 4. هانی‌پات فریب |
| C 5. دیوار آتش نفوذ | B 6. پاسخ به رخداد | F 7. بهداشت گذرواژه | A 8. چارچوب امنیتی |

## ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

| | | | |
|---|---|---|---|
| 1 دیوار آتش | 2 بهره‌برداری | 3 فیشینگ | 4 بدافزار |
| 5 بهداشت | 6 رمزگذاری | | |

## ایستگاه بررسی 6 – فعالیت جایگزین: کلید پاسخ – تطبیق واژگان

| | | | |
|---|---|---|---|
| 1 E – دیواراتش | 2 F – پاسخ | 3 A – باجافزار | 4 B – چندعاملی |
| 5 G – بهداشت | 6 H – چارچوب | 7 C – روزصفر | 8 D – طعمه |

### یادداشت‌های بحث برای مدرسان

**اصطلاحات کلیدی:**
بررسی کنید که دانش‌آموزان بتوانند تهدید باج‌افزار، احراز هویت چندعاملی و بهره‌برداری روز صفرم را با کلمات خودشان توضیح دهند و برای هر کدام مثالی بزنند.

**مطالعات موردی:**
از دانش‌آموزان بخواهید پیشنهادهای خود را بر پایهٔ واقعیت‌های کاربرگ ارائه کنند، نه نظر شخصی.

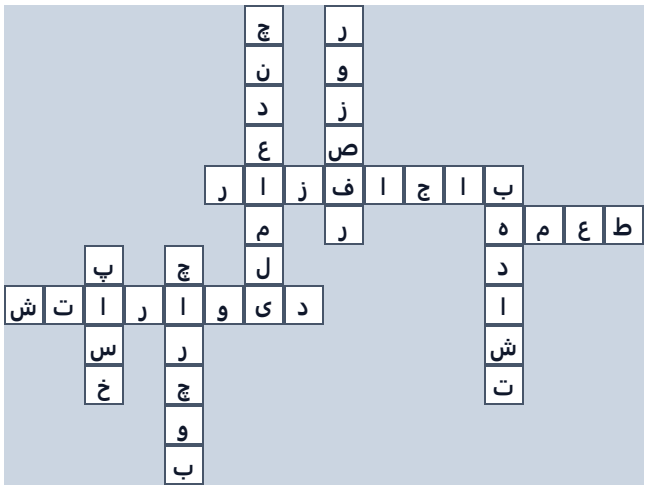
**ارزیابی منابع:**
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

# کلیدهای معما و یادداشت‌های معلم

## پاسخ جدول کلمات

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ر | ر | ج | ض | ج | ظ | ز | ط | ث | پ | ف | ی | ا | خ | ر |
| گ | ف | ذ | ذ | ی | ض | ف | ع | ج | م | ب | ع | ز | ج | ز |
| ن | س | ش | ه | ظ | و | ح | م | ظ | ا | س | ت | غ | ذ | ح |
| س | ز | غ | ش | ظ | ن | ع | ه | ض | ت | ر | ک | ف | ق | چ |
| ژ | و | ر | پ | ا | ب | ب | پ | ط | و | چ | ژ | ز | ز | و |
| ژ | ر | ن | ک | ز | ا | ث | د | ع | ش | ر | ا | و | ث | ذ |
| ت | ت | س | ژ | ع | چ | ظ | خ | ی | ش | ش | ع | س | ب | غ |
| ش | ش | ف | ک | خ | ا | پ | ف | ظ | و | ض | د | ف | خ | پ |
| ا | ا | م | ث | ق | ه | گ | ف | ت | ی | م | ح | خ | ز | ی |
| د | د | ث | س | ث | ع | ز | ن | ظ | پ | گ | ب | ر | ا | ی | ض |
| ه | ه | ج | ن | د | ع | ا | م | ل | ی | ث | ژ | ا | ث | ض |
| ب | ب | ث | ج | خ | ذ | ر | ث | غ | ع | ش | چ | ف | ت | ی |
| ق | ق | ج | ع | ل | چ | ا | ا | ع | ط | س | ظ | ک | و | ع | ش |
| ز | ز | غ | ک | ف | ت | س | ه | پ | ح | ف | ن | م | ر | ا | غ |
| ی | ی | ه | ژ | ح | ذ | ش | غ | ز | س | س | ق | ط | خ | ظ |

## پاسخ جدول‌کلمات




## راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

### افقی

**3 افقی: باجافزار** بدافزاری که داده را رمزگذاری می‌کند و برای رمزگشایی پرداخت مالی می‌خواهد (8 حرف)

**4 افقی: طعمه** سیستم فریبی که برای جذب و تحلیل عوامل مخرب برپا می‌شود (4 حرف)

**7 افقی: دیواراتش** سد شبکه‌ای که ترافیک را بر اساس قواعد امنیتی پالایش می‌کند (8 حرف)

### عمودی

**1 عمودی: روزصفر** بهره‌برداری از آسیب‌پذیری پیش از انتشار وصلهٔ فروشنده (6 حرف)

**2 عمودی: چندعاملی** اعتبارسنجی امنیتی که دو یا چند عامل احراز هویت می‌خواهد (8 حرف)

**3 عمودی: بهداشت** بهترین روش‌ها برای مدیریت اعتبارنامه‌ها و کلیدهای احراز هویت (6 حرف)

**5 عمودی: چارچوب** رهنمودهای ساختاریافته مانند NIST برای مدیریت خطرهای سایبری (6 حرف)

**6 عمودی: پاسخ** طرح ساختاریافته برای مدیریت و کاهش اثر رخنه‌های امنیتی (4 حرف)

# کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

### کلید مرتب‌سازی کلمات

1. اافبزارج — باجافزار
2. ررزفصو — روزصفر
3. ایدراشتو — دیواراتش
4. تادشبه — بهداشت
5. امنیعچلد — چندعاملی
6. مهطع — طعمه
7. سپخا — پاسخ
8. ربچوچا — چارچوب

کلید چالش رمز مخفی

**"سیستم با ورود چندعاملی ایمن"**

# کلید پاسخ مطالعات موردی

## A مطالعهٔ موردی 1: راهبرد بازیابی از باج‌افزار

پاسخ معلم

### راهنمای نمره‌دهی

**پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:**

- تحلیل سناریو: شبکهٔ یک شرکت به باج‌افزار آلوده شده و پایگاه‌های داده حیاتی را قفل کرده است. مهاجمان پرداخت 100,000 دلار به رمزارز را می‌خواهند. شرکت پشتیبان‌های آفلاین مربوط به 24 ساعت پیش را دارد.
- راهبرد و راه‌حل پیشنهادی: خطرهای پرداخت: پرداخت رمزگشایی فایل‌ها را تضمین نمی‌کند، شرکت را هدفی پرداخت‌کننده معرفی می‌کند و فعالیت مجرمانه را تأمین مالی می‌کند. راهبرد بازیابی: تیم باید میزبان‌های آلوده را ایزوله کند، سرورهای نفوذشده را پاک‌سازی کند و داده‌ها را از پشتیبان‌های آفلاین بازیابی کند. آن‌ها باید بردار دسترسی اولیه (فیشینگ یا بهره‌برداری) را وصله کنند تا از آلودگی مجدد فوری جلوگیری شود.

## B مطالعهٔ موردی 2: دفاع در برابر پر کردن اعتبارنامه

پاسخ معلم

### راهنمای نمره‌دهی

**پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:**

- تحلیل سناریو: یک سرویس آنلاین با حملهٔ credential stuffing روبه‌رو است و هکرها میلیون‌ها جفت نام کاربری/گذرواژه را که از سایت‌های دیگر به سرقت رفته آزمایش می‌کنند.
- راهبرد و راه‌حل پیشنهادی: سازوکار: مهاجمان با استفاده از ربات‌های خودکار از استفادهٔ مجدد گذرواژه در سایت‌های مختلف بهره می‌برند تا وارد حساب‌های کاربران شوند. دفاع‌ها: 1. احراز هویت چندعاملی (MFA) حتی اگر گذرواژه درست باشد، تلاش‌های ورود را مسدود می‌کند. 2. پیاده‌سازی محدودسازی نرخ و CAPTCHA ترافیک ربات‌های خودکار را که نقاط ورود را پر می‌کنند مسدود می‌کند.