نام: _____ تاریخ: _____ نمره: _____

# پیشگیری از سرقت هویت و دارایی
# راهنمای امنیت

نشت اعتبارنامه، MFA، پایش وب تاریک، هشدارهای انجماد اعتبار، مهندسی اجتماعی

## نمای کلی یادگیری پیشگیری از سرقت هویت

**خوش آمدید!** این بستهٔ فعالیت شما را در پیشگیری از سرقت هویت و کاهش پیامدهای آن راهنمایی می‌کند. با نشت اعتبارنامه‌ها، احراز هویت چندعاملی، پایش وب تاریک، هشدارهای مسدودسازی اعتبار و دفاع در برابر مهندسی اجتماعی 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/identity-theft/

# نقشهٔ راه یادگیری حفاظت از هویت شما

- خطرهای افشای اطلاعات ورود در انجمن‌های وب تاریک را درک کنید.
- احراز هویت چندعاملی (MFA) و هشدارهای انجماد اعتبار را پیاده‌سازی کنید.
- دفاع‌های امنیتی سازمانی را در برابر کلاهبرداری‌های مهندسی اجتماعی هدفمند طراحی کنید.

### راهنمای سرقت هویت

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 حفاظت از هویت به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

### پیشگیری از سرقت هویت و امنیت دارایی (مقدمه)

سرقت هویت از اطلاعات ورود لو رفته و ورودهای ضعیف برای ربودن حساب‌های شخصی و سازمانی سوءاستفاده می‌کند. به‌کارگیری MFA، انجماد اعتبار، اسکنرهای دارک وب و چارچوب‌های SPF/DKIM/DMARC دفاعی حیاتی در برابر جعل هویت دیجیتال را شکل می‌دهد.

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

# ایستگاه بررسی 1: چالش چندگزینه‌ای

**1. روش اصلی سارقان هویت برای سرقت اعتبارنامه‌های ورود چیست؟**

A. ارسال هشدارهای جعلی ایمیلی که کاربران را فریب می‌دهد در درگاه‌های جعلی گذرواژه وارد کنند
B. گوش دادن به پخش رادیویی نزدیک دفتر سازمانی کاربر
C. یکپارچه‌سازی (defragment) درایو ذخیره‌سازی سرور محلی کاربر
D. قطع پیکربندی‌های پشتیبان‌گیری شبکهٔ خارجی

**2. کدام کنترل امنیتی قوی‌ترین دفاع را در برابر نشت اعتبارنامه فراهم می‌کند؟**

A. احراز هویت چندعاملی با کلیدهای سخت‌افزاری
B. ساخت گذرواژه‌های بلند با قالب‌های پیش‌فرض مرورگر
C. تغییر نام‌های کاربری ایمیل هر شش ماه
D. حذف تاریخچه‌های مرورگر مبتنی بر ردیابی کوکی‌های ذخیره‌شده

**3. چه چیزی نمایندهٔ انسداد اعتبار است؟**

A. قفل کردن گزارش‌های اعتباری برای جلوگیری از افتتاح وام‌های غیرمجاز توسط سارقان
B. حذف تاریخچهٔ تراکنش‌های حساب بانکی از پایگاه‌های داده
C. غیرفعال کردن کارت‌خوان‌های مغناطیسی کارت اعتباری روی اسکنرها
D. رمزگذاری درایوهای سخت پایگاه داده محلی در حالت سکون

**4. چرا پایش دارک‌وب مفید است؟**

A. اگر اعتبارنامهٔ نشت‌یافتهٔ کاربران در پایگاه‌های دادهٔ غیرقانونی ظاهر شود، به آن‌ها هشدار می‌دهد
B. از اجرای بدافزار فعال در جعبه‌های شنی مجازی جلوگیری می‌کند
C. سرعت مسیریابی مرورگر را در شبکه‌های مجازی افزایش می‌دهد
D. تلاش‌های دسترسی با تزریق SQL به پایگاه داده پشت‌صحنه را مسدود می‌کند

**5. مهندسی اجتماعی به چه معناست؟**

A. فریب افراد برای افشای داوطلبانهٔ اعتبارنامه‌های محرمانه
B. اسکن پورت‌های سرور سازمانی برای یافتن اکسپلویت‌های امنیتی فعال
C. پشتیبان‌گیری از فایل‌های پایگاه دادهٔ سیستم روی هارد دیسک‌های آفلاین
D. مسیریابی بسته‌های شبکه از طریق سه گرهٔ onion رمزگذاری‌شده

## ایستگاه بررسی 2: چالش درست یا نادرست

**6 پرسش 6**

6. سرقت هویت فقط حساب‌های دیجیتال آنلاین را تحت تأثیر قرار می‌دهد، نه نامه‌های پستی فیزیکی را.

○ درست ○ نادرست

**7 پرسش 7**

7. اعمال MFA روی همهٔ حساب‌های شخصی، بیشتر حملات ربات‌های پر کردن اعتبارنامه را مسدود می‌کند.

○ درست ○ نادرست

**8 پرسش 8**

8. فریز اعتباری بررسی‌های اعتباری را مسدود می‌کند، اما مانع دسترسی شما به حساب بانکی خودتان می‌شود.

○ درست ○ نادرست

**9 پرسش 9**

9. مدیران گذرواژه با خودداری از پر کردن خودکار گذرواژه‌ها در دامنه‌های جعلی، از کاربران در برابر فیشینگ محافظت می‌کنند.

○ درست ○ نادرست

**10 پرسش 10**

10. ایمیل‌های فیشینگ اغلب از زبان فوری استفاده می‌کنند تا واکنش‌های هیجانی و سریع را برانگیزند.

○ 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. سارقان هویت، رمزهای عبور شخصی و _____ کاربران را هدف می‌گیرند.
2. هشدار به کاربران دربارهٔ نقض پایگاه داده، _____ حساب‌های خصوصی را شناسایی می‌کند.
3. درخواست یک کد موقت برای ورود به حساب _____ نامیده می‌شود.
4. جست‌وجوی انجمن‌های هکرها برای یافتن داده‌های دزدیده‌شده، _____ وب تاریک نام دارد.
5. مسدود کردن بررسی‌های اعتباری غیرمجاز مستلزم یک _____ اعتبار است.
6. آموزش کارکنان در زمینهٔ آگاهی از فیشینگ، یک _____ امنیتی فعال می‌سازد.

**بانک واژگان**

احراز هویت چندعاملی | اعتبارنامه‌ها | انجماد | پایش | جعل | دفاع | فیشینگ | نشت‌ها

**پاسخ‌های خود را اینجا بنویسید:**

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

# ایستگاه بررسی 4: تطبیق مفاهیم امنیت

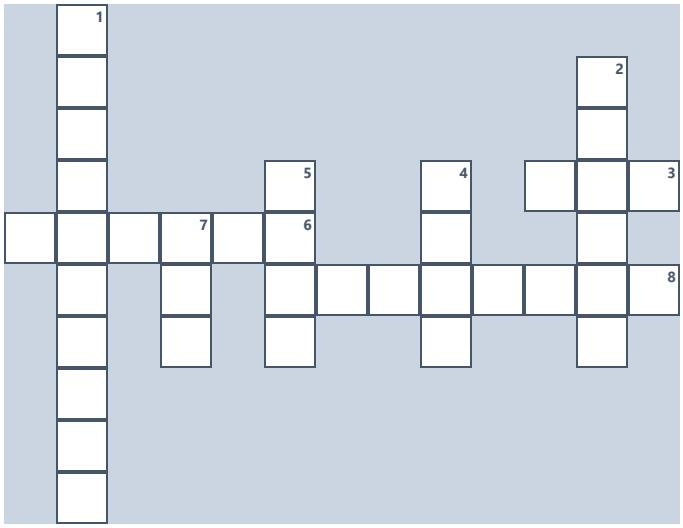
**تطبیق تعاریف**

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. اعتبارنامه‌ها | A | مرحلهٔ تأیید ثانویه (مانند کلیدهای سخت‌افزاری) که ورود به حساب را محافظت می‌کند. |
| 2. نشت‌ها | B | ساخت یک وب‌سایت یا ایمیل جعلی برای تقلید از یک سازمان قانونی. |
| 3. احراز هویت چندعاملی (MFA) | C | محدودکردن دسترسی به پرونده‌های اعتباری برای جلوگیری از درخواست‌های وام متقلبانه. |
| 4. پایش | D | افشای غیرمجاز پایگاه‌های داده خصوصی حاوی رکوردهای شخصی کاربران. |
| 5. انجماد | E | آموزش و کنترل‌های فنی برای محافظت در برابر سرقت هویت. |
| 6. دفاع | F | ارسال پیام‌های جعلی برای فریب کاربران و وادار کردن آن‌ها به افشای اطلاعات ورود. |
| 7. جعل | G | پویش انجمن‌های آنلاین و کانال‌های هکری برای یافتن داده‌های دزدیده‌شدهٔ سازمانی. |
| 8. فیشینگ | H | نام‌های کاربری، گذرواژه‌ها و توکن‌های خصوصی که برای احراز هویت‌های دیجیتال به کار می‌روند. |

# 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. افشای غیرمجاز پایگاه‌های داده حاوی سوابق شخصی کاربران. (3)**

**6. محدود کردن دسترسی به پرونده‌های اعتباری برای جلوگیری از درخواست‌های وام متقلبانه. (6)**

**8. گام تأیید ثانویه (مانند کلیدهای سخت‌افزاری) برای محافظت از ورود به حساب. (8)**

## عمودی

**1. نام کاربری، رمز عبور و توکن‌های خصوصی که برای احراز هویت دیجیتال به کار می‌روند. (10)**

**2. ارسال پیام‌های فریبکارانه برای وادار کردن کاربران به افشای اعتبارنامه‌هایشان. (6)**

**4. آموزش و کنترل‌های فنی برای محافظت در برابر سرقت هویت. (4)**

**5. جست‌وجو در انجمن‌ها و کانال‌های هکرها برای یافتن داده‌های سازمانی دزدیده‌شده. (4)**

**7. ساختن وب‌سایت یا ایمیل ساختگی برای تقلید از یک سازمان معتبر. (3)**

# 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: افشای غیرمجاز پایگاه‌های داده حاوی سوابق شخصی کاربران. (3 حرف):**

**6 افقی: محدود کردن دسترسی به پرونده‌های اعتباری برای جلوگیری از درخواست‌های وام متقلبانه. (6 حرف):**

**8 افقی: گام تأیید ثانویه (مانند کلیدهای سخت‌افزاری) برای محافظت از ورود به حساب. (8 حرف):**

## عمودی

**1 عمودی: نام کاربری، رمز عبور و توکن‌های خصوصی که برای احراز هویت دیجیتال به کار می‌روند. (10 حرف):**

**2 عمودی: ارسال پیام‌های فریبکارانه برای وادار کردن کاربران به افشای اعتبارنامه‌هایشان. (6 حرف):**

**4 عمودی: آموزش و کنترل‌های فنی برای محافظت در برابر سرقت هویت. (4 حرف):**

**5 عمودی: جست‌وجو در انجمن‌ها و کانال‌های هکرها برای یافتن داده‌های سازمانی دزدیده‌شده. (4 حرف):**

**7 عمودی: ساختن وب‌سایت یا ایمیل ساختگی برای تقلید از یک سازمان معتبر. (3 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.

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

### فهرست واژگان

اعتبارنامه
نشت
چندعاملی
پایش
انجماد
دفاع
جعل
فیشینگ

# 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 | تعاریف و فیلدهای تطبیق |
|---|---|
| **A. اعتبارنامه** | 1. ارسال پیام‌های فریبکارانه برای وادار کردن کاربران به افشای اعتبارنامه‌هایشان. |
| **B. نشت** | 2. نام کاربری، رمز عبور و توکن‌های خصوصی که برای احراز هویت دیجیتال به کار می‌روند. |
| **C. چندعاملی** | 3. ساختن وب‌سایت یا ایمیل ساختگی برای تقلید از یک سازمان معتبر. |
| **D. پایش** | 4. آموزش و کنترل‌های فنی برای محافظت در برابر سرقت هویت. |
| **E. انجماد** | 5. جست‌وجو در انجمن‌ها و کانال‌های هکرها برای یافتن داده‌های سازمانی دزدیده‌شده. |
| **F. دفاع** | 6. محدود کردن دسترسی به پرونده‌های اعتباری برای جلوگیری از درخواست‌های وام متقلبانه. |
| **G. جعل** | 7. افشای غیرمجاز پایگاه‌های داده حاوی سوابق شخصی کاربران. |
| **H. فیشینگ** | 8. گام تأیید ثانویه (مانند کلیدهای سخت‌افزاری) برای محافظت از ورود به حساب. |

## 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. م ن ر ا ع ا ا ه ب ت _____
2. ع چ ی ن ل م ا د _____
3. ا ج م د ا ن _____
4. ع ل ج _____
5. ت ش ن _____
6. ی ش پ ا _____
7. ا د ع ف _____
8. ش گ ف ن ی ی _____

# فعالیت تکمیلی: سریع فکر کن

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

| | | | | |
|---|---|---|---|---|
| 1 | کارهایی که اگر هویت شما دزدیده شد باید انجام داد | | | |
| 2 | چیزهایی که نباید در شبکه‌های اجتماعی به اشتراک گذاشت | | | |
| 3 | چیزهایی که پشتیبان می‌گیرید | | | |
| 4 | کارت‌ها یا مدارک شناسایی در کیف پول شما | | | |
| 5 | مدارکی که باید محافظت کنید | | | |
| 6 | کارهایی که پس از نشت داده باید انجام داد | | | |
| 7 | دلایل به‌روزرسانی نرم‌افزار | | | |
| 8 | اطلاعاتی که یک سارق هویت می‌خواهد | | | |
| 9 | دستگاه‌هایی که می‌توانند هک شوند | | | |
| 10 | جاهایی که داده‌های شما می‌توانند از آن‌ها نشت کنند | | | |
| 11 | عادت‌های ایمن که می‌توانید از امروز شروع کنید | | | |
| 12 | نشانه‌های آلوده بودن رایانه | | | |
| 13 | روش‌های اثبات هویت | | | |
| 14 | نشانه‌های سرقت هویت | | | |
| 15 | نشانه‌های هشدار در یک ایمیل | | | |

# ایستگاه بررسی 8: مطالعات موردی امنیت سایبری

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

### مطالعهٔ موردی 1: حفاظت در برابر جعل هویت مدیران ارشد



**سناریو:** یک مدیر ارشد سرشناس (C-suite) هدف نام‌های دامنهٔ typo-squatted قرار گرفته که ایمیل شخصی او را برای کلاهبرداری از مشتریان تقلید می‌کنند. یک برنامهٔ محافظت از برند طراحی کنید.

**پرسش برای بحث:** ریسک‌های جعل برند را تحلیل کنید و کنترل‌های SPF/DKIM/DMARC و احراز هویت را شرح دهید.

### مطالعهٔ موردی 2: افشای اعتبارنامه‌های شرکتی در وب تاریک



**سناریو:** یک dump از پایگاه داده در وب تاریک شامل صدها اعتبارنامهٔ شرکتی متعلق به مدیران سیستم یک سازمان است. یک راهبرد کاهش خطر طراحی کنید.

**پرسش برای بحث:** فرایند پاک‌سازی اعتبارنامه‌ها را شرح دهید و استقرار مدیر گذرواژه را برنامه‌ریزی 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

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 27 | 1 | 4 | 32 | 6 | 32 | 10 | | 4 | 32 | 30 | 31 | | 4 | 20 | 23 | 1 | 8 | 28 |
| | | | | | | | | | | | | | | | | | | |
| 32 | 27 | 28 | 1 | 21 | 10 | 29 | 7 | | 13 | 1 | 12 | 8 | 1 | | 1 | 2 | | |
| | | | | | | | | | | | | | | | | | | |

**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: سرقت هویت چیست؟

جرمی که در آن مهاجم سوابق شخصی (مانند گذرواژه‌ها یا SSN) را می‌دزدد تا برای سود مالی خود را جای دیگری جا بزند.

### Q2: رایج‌ترین علت سرقت هویت چیست؟

فیشینگ یکی از راه‌های اصلی سرقت گذرواژه توسط سارقان است که کاربران را به وب‌سایت‌های جعلی می‌کشاند.

### Q3: احراز هویت چندعاملی (MFA) چگونه از هویت‌ها محافظت می‌کند؟

MFA برای ورود به یک اثبات ثانویه (مانند کلید سخت‌افزاری) نیاز دارد و حتی اگر گذرواژهٔ شما را بدزدند، مهاجمان را مسدود می‌کند.

### Q4: انجماد اعتبار چیست؟

سرویس رایگانی که مانع می‌شود دفاتر اعتباری پروندهٔ اعتباری شما را به اشتراک بگذارند و جلوی افتتاح وام‌های جدید به نام شما را توسط سارقان می‌گیرد. [2]

### Q5: پایش دارک‌وب چیست؟

نرم‌افزاری که انجمن‌های هکرها را برای ایمیل‌ها، گذرواژه‌ها و سوابق شخصی افشاشده بررسی می‌کند و در صورت افشای داده‌های شما به شما هشدار می‌دهد.

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

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

### Q6: credential stuffing به چه معناست؟

بات‌های خودکاری که فهرست‌های گذرواژهٔ لورفته را در صدها وب‌سایت آزمایش می‌کنند تا حساب‌های فعال را تصاحب کنند.

### Q7: چرا جعل ایمیل خطرناک است؟

به مهاجمان اجازه می‌دهد نام فرستنده را در ایمیل‌ها جعل کنند و پیام‌های فیشینگ را طوری نشان دهند که گویی از همکاران مورد اعتماد آمده‌اند.

### Q8: مدیران گذرواژه چگونه جلوی سرقت هویت را می‌گیرند؟

آن‌ها گذرواژه‌های پیچیده و یکتا برای هر حساب ذخیره می‌کنند و از پرکردن خودکار اطلاعات ورود در دامنه‌های فیشینگ جعلی خودداری می‌کنند.

### Q9: فیشینگ هدفمند (spear phishing) چیست؟

حملهٔ فیشینگ بسیار هدفمند که با نام و جزئیات قربانی سفارشی‌سازی می‌شود تا احتمال فریب را افزایش دهد.

### Q10: هشدار اعتباری چه تفاوتی با انسداد اعتباری دارد؟

هشدار به وام‌دهندگان می‌گوید پیش از افتتاح حساب هویت شما را تأیید کنند، در حالی که فریز اعتباری دسترسی به پروندهٔ اعتباری شما را به‌طور کامل مسدود می‌کند. [2]

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

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

### Q1: تعویض سیم‌کارت (SIM swapping) چگونه به سرقت هویت منجر می‌شود؟

مهاجمان کارکنان اپراتور را متقاعد می‌کنند شمارهٔ تلفن قربانی را به سیم‌کارت جدیدی منتقل کنند و کدهای 2FA پیامکی را می‌ربایند.

### Q2: نقش DMARC در جلوگیری از سرقت هویت چیست؟

DMARC به صاحبان دامنه اجازه می‌دهد از رسیدن ایمیل‌های جعلی به صندوق ورودی جلوگیری کنند و مانع از تقلید دامنه‌های شرکتی توسط ایمیل‌های جعلی شوند.

### Q3: چرا تشخیص سرقت هویت ساختگی دشوار است؟

سارقان شماره‌های واقعی SSN را با نام‌ها و تاریخ تولدهای جعلی ترکیب می‌کنند تا نمایه‌های اعتباری کاملاً جدید بسازند و هشدارهای پایهٔ کلاهبرداری را دور بزنند.

### Q4: دلالان داده چگونه از هویت‌های شخصی سوءاستفاده می‌کنند؟

کارگزاران داده سوابق عمومی، رفتار وب و تاریخچهٔ خرید را جمع‌آوری می‌کنند تا پرونده‌های نمایه بسازند که ممکن است نشت یا فروخته شوند.

### Q5: چرا MFA مبتنی بر پیامک آسیب‌پذیر تلقی می‌شود؟

ترافیک SMS در برابر رهگیری، فیشینگ و سوءاستفاده‌های تعویض سیم‌کارت در سطح اپراتور آسیب‌پذیر است.

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

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

### Q6: قفل پروندهٔ اعتباری چیست؟

سرویس تجاری مشابه فریز که به کاربران اجازه می‌دهد پروندهٔ اعتباری خود را از طریق برنامهٔ موبایل فوراً باز یا قفل کنند.

### Q7: نقض داده‌های شرکتی چگونه به سرقت هویت دامن می‌زند؟

پایگاه‌های دادهٔ لو رفته میلیون‌ها اعتبارنامهٔ متنِ ساده را افشا می‌کنند و داده‌های خام لازم برای کلاهبرداری هدفمند هویتی را در اختیار سارقان می‌گذارند.

### Q8: خطر اشتراک‌گذاری بیش‌ازحد در شبکه‌های اجتماعی چیست؟

اشتراک‌گذاری عمومی نام حیوان خانگی، محل تولد و نام خانوادگی دوران دختری مادر، پاسخ پرسش‌های رایج بازیابی حساب را به سارقان می‌دهد.

### Q9: ورود زیست‌سنجی چگونه از نمایه‌های هویتی محافظت می‌کند؟

زیست‌سنجی ورود را به ویژگی‌هایی مانند اثر انگشت یا چهره پیوند می‌دهد؛ اگر روی دستگاه نگه داشته شود سرقتش دشوار است، اما داده‌های زیست‌سنجی ذخیره‌شده می‌توانند نشت کنند.

### Q10: قانون Red Flags Rule چگونه با سرقت هویت مقابله می‌کند؟

مقرره‌ای فدرال که مؤسسات مالی را ملزم می‌کند برنامه‌های مکتوب برای شناسایی و پاسخ به نشانه‌های هشداردهندهٔ سرقت هویت تدوین کنند.

## 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**

IdentityTheft.gov، که توسط FTC اداره می‌شود، به قربانیان آمریکایی اجازه می‌دهد سرقت هویت را گزارش کنند و یک برنامهٔ بازیابی شخصی دریافت کنند. [1]

**2. بینش امنیت**

کلیدهای امنیتی سخت‌افزاری MFA مقاوم در برابر فیشینگ هستند، قوی‌ترین نوع MFA که CISA به آن توصیه می‌کند. [4]

**3. بینش امنیت**

گذرواژه‌های لو رفته نقطهٔ ورود رایج در نقض داده‌ها هستند و کلاهبرداری هویتی بعدی را دامن می‌زنند.

**4. بینش امنیت**

طبق قانون فدرال، فریز اعتباری رایگان است و تا زمان باز شدن، مانع بررسی پرونده‌های اعتباری توسط وام‌دهندگان می‌شود. [2]

**5. بینش امنیت**

DMARC به صاحبان دامنه اجازه می‌دهد به سرورهای ایمیل بگویند ایمیل جعلی را که بررسی‌ها را رد نمی‌کند، رد یا قرنطینه کنند. [7]

**6. بینش امنیت**

تعویض سیم‌کارت به هکرها اجازه می‌دهد احراز هویت دومرحله‌ای مبتنی بر SMS را در پورتال‌های بانکی دور بزنند.

**7. بینش امنیت**

کلاهبرداری هویت ساختگی جزئیات واقعی و جعلی را ترکیب می‌کند و تشخیص آن را برای وام‌دهندگان دشوار می‌کند.

**8. بینش امنیت**

بسیاری از افراد یک گذرواژه را در حساب‌های آنلاین مختلف دوباره به کار می‌برند، بنابراین یک نشت می‌تواند چند حساب را افشا کند.

**9. بینش امنیت**

دلالان داده پرونده‌های دقیقی از شمار زیادی از مصرف‌کنندگان گردآوری می‌کنند و خطر متمرکز حریم خصوصی ایجاد می‌کنند.

**10. بینش امنیت**

بازیابی پس از سرقت هویت می‌تواند ماه‌ها کار ببرد، مانند اعتراض به هزینه‌ها و اصلاح گزارش‌های اعتباری.

# 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] Federal Trade Commission. (n.d.). IdentityTheft.gov: Report identity theft and get a recovery plan.
https://www.identitytheft.gov/

[2] Federal Trade Commission. (2025). Credit Freezes and Fraud Alerts.
https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts

[3] Federal Trade Commission. (n.d.). What To Know About Identity Theft.
https://consumer.ftc.gov/articles/what-know-about-identity-theft

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

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

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

[7] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).
https://www.rfc-editor.org/rfc/rfc7489.html

## کلید پاسخ: ایستگاه بررسی 1 – چندگزینه‌ای

**1 پرسش 1**

پاسخ درست: A

### نکتهٔ آموزشی

روش اصلی سارقان هویت برای سرقت اعتبارنامه‌های ورود چیست؟ → ارسال هشدارهای جعلی ایمیلی که کاربران را فریب می‌دهد در درگاه‌های جعلی گذرواژه وارد کنند

**2 پرسش 2**

پاسخ درست: A

### نکتهٔ آموزشی

کدام کنترل امنیتی قوی‌ترین دفاع را در برابر نشت اعتبارنامه فراهم می‌کند؟ → احراز هویت چندعاملی با کلیدهای سخت‌افزاری

**3 پرسش 3**

پاسخ درست: A

### نکتهٔ آموزشی

چه چیزی نمایندهٔ انسداد اعتبار است؟ → قفل کردن گزارش‌های اعتباری برای جلوگیری از افتتاح وام‌های غیرمجاز توسط سارقان

**4 پرسش 4**

پاسخ درست: A

### نکتهٔ آموزشی

چرا پایش دارک‌وب مفید است؟ → اگر اعتبارنامهٔ نشت‌یافتهٔ کاربران در پایگاه‌های دادهٔ غیرقانونی ظاهر شود، به آن‌ها هشدار می‌دهد

**5 پرسش 5**

پاسخ درست: A

### نکتهٔ آموزشی

مهندسی اجتماعی به چه معناست؟ → فریب افراد برای افشای داوطلبانهٔ اعتبارنامه‌های محرمانه

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

**6** پرسش 6

پاسخ درست: نادرست

### نکتهٔ آموزشی

سرقت هویت می‌تواند به‌صورت آفلاین هم شروع شود، مانند نامه یا مدارک دزدیده‌شده.

**7** پرسش 7

پاسخ درست: درست

### نکتهٔ آموزشی

اعمال MFA روی همهٔ حساب‌های شخصی، بیشتر حملات ربات‌های پر کردن اعتبارنامه را مسدود می‌کند.

**8** پرسش 8

پاسخ درست: نادرست

### نکتهٔ آموزشی

فریز اعتبار بررسی‌های اعتباری جدید را متوقف می‌کند اما بر حساب‌های موجود شما اثری ندارد.

**9** پرسش 9

پاسخ درست: درست

### نکتهٔ آموزشی

مدیران گذرواژه با خودداری از پر کردن خودکار گذرواژه‌ها در دامنه‌های جعلی، از کاربران در برابر فیشینگ محافظت می‌کنند.

**10** پرسش 10

پاسخ درست: درست

### نکتهٔ آموزشی

ایمیل‌های فیشینگ اغلب از زبان فوری استفاده می‌کنند تا واکنش‌های هیجانی و سریع را برانگیزند.

# 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

| | | | |
|---|---|---|---|
| H 1. اعتبارنامه‌ها | D 2. نشت‌ها | A 3. احراز هویت چندعاملی (MFA) | G 4. پایش |
| C 5. انجماد | E 6. دفاع | B 7. جعل | F 8. فیشینگ |

## ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

| | | | |
|---|---|---|---|
| 1 اعتبارنامه‌ها | 2 نشت‌ها | 3 احراز هویت چندعاملی | 4 پایش |
| 5 انجماد | 6 دفاع | | |

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

| | | | |
|---|---|---|---|
| 1 H – فیشینگ | 2 A – اعتبارنامه | 3 G – جعل | 4 F – دفاع |
| 5 D – پایش | 6 E – انجماد | 7 B – نشت | 8 C – چندعاملی |

### یادداشت‌های بحث برای مدرسان

**اصطلاحات کلیدی:**
بررسی کنید که دانش‌آموزان بتوانند اعتبارنامه‌ها، نشت‌ها و احراز هویت چندعاملی (MFA) 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.

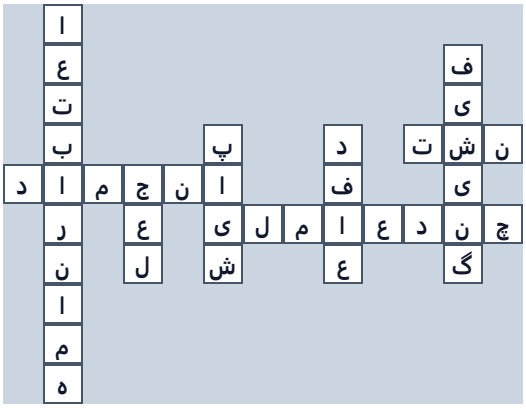
**ارزیابی منابع:**
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

# کلیدهای معما و یادداشت‌های معلم

## پاسخ جدول کلمات

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

## پاسخ جدول‌کلمات




## راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

### افقی

**3 افقی: نشت** افشای غیرمجاز پایگاه‌های داده حاوی سوابق شخصی کاربران. (3 حرف)

**6 افقی: انجماد** محدود کردن دسترسی به پرونده‌های اعتباری برای جلوگیری از درخواست‌های وام متقلبانه. (6 حرف)

**8 افقی: چندعاملی** گام تأیید ثانویه (مانند کلیدهای سخت‌افزاری) برای محافظت از ورود به حساب. (8 حرف)

### عمودی

**1 عمودی: اعتبارنامه** نام کاربری، رمز عبور و توکن‌های خصوصی که برای احراز هویت دیجیتال به کار می‌روند. (10 حرف)

**2 عمودی: فیشینگ** ارسال پیام‌های فریبکارانه برای وادار کردن کاربران به افشای اعتبارنامه‌هایشان. (6 حرف)

**4 عمودی: دفاع** آموزش و کنترل‌های فنی برای محافظت در برابر سرقت هویت. (4 حرف)

**5 عمودی: پایش** جست‌وجو در انجمن‌ها و کانال‌های هکرها برای یافتن داده‌های سازمانی دزدیده‌شده. (4 حرف)

**7 عمودی: جعل** ساختن وب‌سایت یا ایمیل ساختگی برای تقلید از یک سازمان معتبر. (3 حرف)

# کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

### کلید مرتب‌سازی کلمات

1. منراعااهبت — اعتبارنامه
2. عچینلماد — چندعاملی
3. اجمدان — انجماد
4. علج — جعل
5. تشن — نشت
6. یشپا — پایش
7. ادعف — دفاع
8. شگفنیی — فیشینگ

### کلید چالش رمز مخفی

**"محافظت هویت دیجیتال با احراز چندعاملی"**

# کلید پاسخ مطالعات موردی

## A مطالعهٔ موردی 1: حفاظت در برابر جعل هویت مدیران ارشد

پاسخ معلم

### راهنمای نمره‌دهی

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

- تحلیل سناریو: یک مدیر ارشد سرشناس هدف دامنه‌های typo-squatted شده است که ایمیل شخصی او را تقلید می‌کنند تا مشتریان را فریب دهند. یک برنامهٔ حفاظت از برند طراحی کنید.
- راهبرد و راه‌حل پیشنهادی: همهٔ املاهای رایج نام مدیر ارشد را ثبت کنید. پروتکل‌های احراز هویت ایمیل (DMARC، DKIM، SPF) را برای جلوگیری از جعل دامنه مستقر کنید. MFA سخت‌افزاری را روی همهٔ ورودهای سازمانی مدیران رده‌بالا اعمال کنید.

## B مطالعهٔ موردی 2: افشای اعتبارنامه‌های شرکتی در وب تاریک

پاسخ معلم

### راهنمای نمره‌دهی

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

- تحلیل سناریو: یک نشت پایگاه داده در وب تاریک شامل چند صد اعتبارنامهٔ سازمانی متعلق به مدیران سیستم یک شرکت است. راهبرد کاهش خطر طراحی کنید.
- راهبرد و راه‌حل توصیه‌شده: بازنشانی گذرواژهٔ سراسری شرکت را انجام دهید. استفاده از مدیر گذرواژهٔ سازمانی را الزامی کنید. MFA را در همهٔ پورتال‌های سیستم اعمال کنید و هشدارهای پایش خودکار و مداوم دارک‌وب را راه‌اندازی کنید.