نام: _____ تاریخ: _____ نمره: _____

کلاهبرداری‌های آنلاین و مهندسی اجتماعی راهنمای حفاظت

فیشینگ ایمیلی، دامنه‌های جعلی، فیشینگ صوتی، کلاهبرداری‌های پشتیبانی، تأیید خارج از باند، BEC

مرور آموزشی کلاهبرداری‌های آنلاین

ایمن‌شده
رمزگذاری داده
استاندارد AES 256 بیتی

منطبق
استانداردهای جهانی
چارچوب‌های GDPR و CCPA

اعتماد صفر
سیاست دسترسی
احراز هویت چندعاملی

خوش آمدید! این بستهٔ فعالیت شما را در دفاع در برابر کلاهبرداری آنلاین راهنمایی می‌کند. با وب‌سایت‌های جعلی فیشینگ، تاکتیک‌های مهندسی اجتماعی، کلاهبرداری‌های پشتیبانی، بردارهای کلاهبرداری حواله و روش‌های تأیید پرداخت 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**

باز کردن راهنمای امنیت سایبری VPN.com

URL: https://www.vpn.com/cybersecurity/online-scams/

نقشهٔ راه یادگیری محافظت در برابر کلاهبرداری آنلاین شما

- نشانگرهای رایج کلاهبرداری پشتیبانی و دامنه‌های typosquatting را شناسایی کنید.
- پروتکل‌های تأیید ایمیل (SPF، DKIM، DMARC) را در برابر جعل پیاده‌سازی کنید.
- تأیید تراکنش خارج از باند را برای جلوگیری از کلاهبرداری حواله تجاری برقرار کنید.

راهنمای دستورالعمل‌های کلاهبرداری‌های آنلاین

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 در برابر کلاهبرداری آنلاین به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

کلاهبرداری‌های آنلاین و حفاظت در برابر مهندسی اجتماعی (مقدمه)

کلاهبرداری‌های آنلاین با فیشینگ، پنجره‌های بازشوی پشتیبانی، تماس‌های صوتی فریبنده و کلاهبرداری انتقال بانکی از رفتار انسان سوءاستفاده می‌کنند. اجرای تأیید تراکنش از مسیر جداگانه و قوانین دامنهٔ SPF/DKIM/DMARC می‌تواند به مسدود کردن بردارهای مهندسی اجتماعی در دروازه کمک کند.

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

ایستگاه بررسی 1: چالش چندگزینه‌ای

1. نشانهٔ اصلی کلاهبرداری پشتیبانی جعلی چیست؟

- A. پنجرهٔ بازشویی که ادعا می‌کند سیستم شما آلوده است و از شما می‌خواهد به یک شمارهٔ تلفن زنگ بزنید
- B. به‌روزرسانی امنیتی خودکار که از یک رجیستری رسمی دانلود می‌شود
- C. مدیر گذرواژه‌ای که از پر کردن اعتبارنامه‌ها در یک دامنهٔ سازمانی خودداری می‌کند
- D. پشتیبان‌گیری پس‌زمینهٔ فایل که روی پیکربندی یک درایو خارجی اجرا می‌شود

2. کدام تکنیک از دامنه‌های فرستندهٔ جعلی برای سرقت جزئیات بانکی استفاده می‌کند؟

- A. فیشینگ ایمیلی
- B. اسکن پورت
- C. تزریق حافظه
- D. خرد کردن رمزنگاری

3. چه چیزی نمایندهٔ کلاهبرداری انتقال بانکی است؟

- A. فریب قربانیان با مهندسی اجتماعی برای ارسال پول به حساب‌های شرکتی جعلی
- B. رمزگذاری پایگاه‌های داده سیستم با بارهای مخرب باج‌افزار
- C. پرس‌وجو از پایگاه‌های داده با دستورهای تزریق SQL
- D. پشتیبان‌گیری از فایل‌های سیستم روی دیسک‌های ذخیره‌سازی آفلاین

4. چرا کلاهبرداران وب‌سایت‌های خرید جعلی می‌سازند؟

- A. برای سرقت جزئیات کارت اعتباری و اعتبارنامهٔ پرداخت خریداران
- B. میزبانی جدول‌های پایگاه دادهٔ تحلیل بدافزار در جعبهٔ شنی
- C. برای تسریع تحویل سفارش‌های آنلاین
- D. برای آزمایش رایگان طرح‌های جدید وب‌سایت

5. ویشینگ به چه معناست؟

- A. کلاهبرداری فیشینگ صوتی از طریق شبکه‌های تلفن برای سرقت اعتبارنامه
- B. اسکن شبکه‌های محلی برای یافتن دستگاه‌های ناامن سیستم
- C. بازیابی پایگاه‌های داده سیستم پس از نقض غیرمجاز
- D. اجرای کد نامطمئن درون کانتینرهای مجازی امن

ایستگاه بررسی 2: چالش درست یا نادرست

6 پرسش 6

6. کلاهبرداری‌های فیشینگ فقط کاربران نهایی را هدف می‌گیرند و هرگز اهداف نهنگ‌شکاری مدیران ارشد را.

○ درست ○ نادرست

7 پرسش 7

7. دامنه‌های جعلی اغلب از غلط‌های تایپی جزئی (مانند amaz0n.com) برای تقلید از برندهای معتبر استفاده می‌کنند.

○ درست ○ نادرست

8 پرسش 8

8. کلاهبرداری‌های پشتیبانی را می‌توان با دادن دسترسی راه‌دور به تماس‌گیرنده حل کرد.

○ درست ○ نادرست

9 پرسش 9

9. مهندسی اجتماعی از روان‌شناسی انسان مانند ترس و فوریت برای دور زدن قواعد امنیتی سوءاستفاده می‌کند.

○ درست ○ نادرست

10 پرسش 10

10. درخواست‌های انتقال بانکی باید همیشه از طریق کانال‌های ارتباطی خارج از باند راستی‌آزمایی شوند.

○ 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. ایمیل‌های فریبکارانه‌ای که کاربران را گول می‌زنند _____ نام دارند.
2. نشانی‌های وبی که برندهای معتبر را تقلید می‌کنند _____ هستند.
3. کلاهبرداری صوتی که اطلاعات بانکی را هدف می‌گیرد _____ نام دارد.
4. پنجره‌ای که برای پاک‌سازی ویروس پول می‌خواهد، یک _____ پشتیبانی فنی است.
5. اطمینان از درخواست پرداخت مستلزم _____ از مسیری مستقل است.
6. هدایت معاملات تجاری به حساب‌های سارقان، کلاهبرداری _____ نام دارد.

بانک واژگان

اسمیشینگ | تأیید | جعلی | حواله | فیشینگ | کلاهبرداری | نهنگ | ویشینگ

پاسخ‌های خود را اینجا بنویسید:

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

ایستگاه بررسی 4: تطبیق مفاهیم امنیت

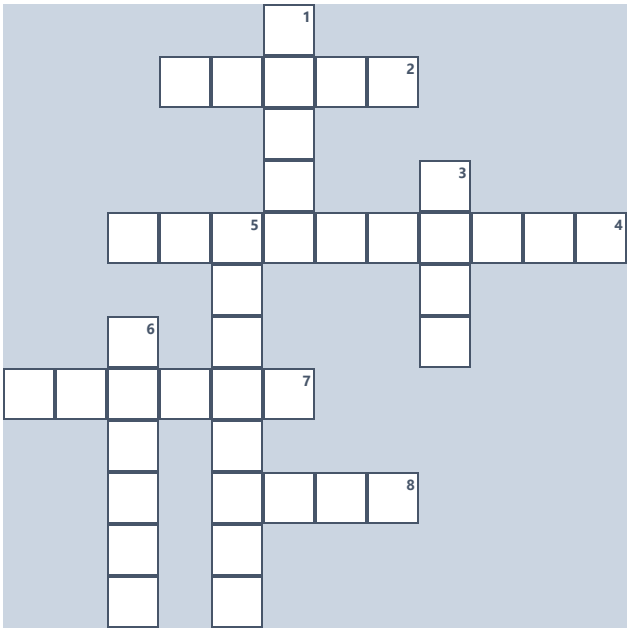
تطبیق تعاریف

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. فیشینگ	A	انحراف کلاهبردارانهٔ تراکنش‌های بانکی به حساب‌های مجرمانه.
2. جعلی	B	طرح کلاهبرداری که برای سرقت پول یا اطلاعات دسترسی از قربانیان طراحی شده است.
3. ویشینگ	C	ارسال پیامک‌های کلاهبرداری برای سرقت اطلاعات ورود حساب موبایل.
4. کلاهبرداری	D	تماس‌های صوتی جعلی که برای سرقت اطلاعات ورود و جزئیات حساب طراحی شده‌اند.
5. راستی‌آزمایی	E	حملات فیشینگ هدفمند با هدف سرقت اطلاعات ورود از مدیران ارشد.
6. سیم	F	نشانی فرستندهٔ ایمیل یا وب‌سایت جعلی که طوری طراحی شده که قانونی به نظر برسد.
7. نهنگ‌یابی	G	کارزارهای ایمیلی جعلی که برای سرقت اطلاعات ورود و گذرواژه‌ها طراحی شده‌اند.
8. اسمیشینگ	H	تأیید جزئیات پرداخت با روش تماس ثانویهٔ مورد اعتماد.

ایستگاه بررسی 5: جدول‌کلمات

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



افقی

2. هدایت متقلبانهٔ تراکنش‌های بانکی به حساب‌های مجرمان. (5)

4. طرح فریبکارانه برای سرقت پول یا دسترسی به اعتبارنامه‌های قربانیان. (10)

7. کمپین‌های ایمیلی فریبکارانه برای سرقت اطلاعات ورود و گذرواژه‌ها. (6)

8. نشانی فرستندهٔ ایمیل یا وب‌سایتی که طوری تقلید شده که معتبر به نظر برسد. (4)

عمودی

1. اطمینان از جزئیات پرداخت از طریق یک روش تماس ثانویهٔ مطمئن. (5)

3. حملات فیشینگ هدفمند برای سرقت اعتبارنامه از مدیران ارشد. (4)

5. ارسال پیامک‌های کلاهبردارانه برای سرقت اعتبارنامه‌های حساب موبایل. (8)

6. تماس‌های صوتی فریبکارانه برای سرقت اعتبارنامه‌ها و جزئیات حساب. (6)

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

2 افقی: هدایت متقلبانهٔ تراکنش‌های بانکی به حساب‌های مجرمان. (5 حرف):

4 افقی: طرح فریبکارانه برای سرقت پول یا دسترسی به اعتبارنامه‌های قربانیان. (10 حرف):

7 افقی: کمپین‌های ایمیلی فریبکارانه برای سرقت اطلاعات ورود و گذرواژه‌ها. (6 حرف):

8 افقی: نشانی فرستندهٔ ایمیل یا وب‌سایتی که طوری تقلید شده که معتبر به نظر برسد. (4 حرف):

عمودی

1 عمودی: اطمینان از جزئیات پرداخت از طریق یک روش تماس ثانویهٔ مطمئن. (5 حرف):

3 عمودی: حملات فیشینگ هدفمند برای سرقت اعتبارنامه از مدیران ارشد. (4 حرف):

5 عمودی: ارسال پیامک‌های کلاهبردارانه برای سرقت اعتبارنامه‌های حساب موبایل. (8 حرف):

6 عمودی: تماس‌های صوتی فریبکارانه برای سرقت اعتبارنامه‌ها و جزئیات حساب. (6 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.

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

فهرست واژگان

فیشینگ جعلی ویشینگ کلاهبرداری تأیید حواله نهنگ اسمیشینگ

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. فیشینگ	1. نشانی فرستندهٔ ایمیل یا وب‌سایتی که طوری تقلید شده که معتبر به نظر برسد.
B. جعلی	2. اطمینان از جزئیات پرداخت از طریق یک روش تماس ثانویهٔ مطمئن.
C. ویشینگ	3. هدایت متقلبانهٔ تراکنش‌های بانکی به حساب‌های مجرمان.
D. کلاهبرداری	4. ارسال پیامک‌های کلاهبردارانه برای سرقت اعتبارنامه‌های حساب موبایل.
E. تأیید	5. حملات فیشینگ هدفمند برای سرقت اعتبارنامه از مدیران ارشد.
F. حواله	6. تماس‌های صوتی فریبکارانه برای سرقت اعتبارنامه‌ها و جزئیات حساب.
G. نهنگ	7. کمپین‌های ایمیلی فریبکارانه برای سرقت اطلاعات ورود و گذرواژه‌ها.
H. اسمیشینگ	8. طرح فریبکارانه برای سرقت پول یا دسترسی به اعتبارنامه‌های قربانیان.

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. ش ف ی ن گ ی
2. گ و ش ن ی ی
3. ی ت د ی ا
4. گ ن ن ه
5. ی ج ل ع
6. ر ب ه د ا ک ل ر ی ا
7. ل ه ح ا و
8. ی س ش گ ا ن ی م

فعالیت تکمیلی: سریع فکر کن

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

1	دستگاه‌هایی که می‌توانند هک شوند		
2	عبارت‌هایی که کلاهبرداران اغلب به کار می‌برند		
3	روش‌های پرداختی که کلاهبرداران می‌خواهند		
4	انواع کلاهبرداری آنلاین		
5	پیشنهادهایی که بیش از حد خوب برای واقعی بودن‌اند		
6	جاهایی که می‌توان کلاهبرداری را گزارش کرد		
7	واژه‌های مرتبط با امنیت سایبری		
8	افرادی که می‌توانید دربارهٔ کلاهبرداری به آن‌ها هشدار دهید		
9	چیزهایی که پشتیبان می‌گیرید		
10	نشانه‌های هشدار در یک ایمیل		
11	نشانه‌های آلوده بودن رایانه		
12	روش‌های بررسی یک فروشگاه آنلاین		
13	روش‌های محافظت از حساب‌هایتان		
14	کارهایی که اگر کلاهبرداری شدید باید انجام داد		
15	کارهایی که پس از نشت داده باید انجام داد		

ایستگاه بررسی 8: مطالعات موردی امنیت سایبری

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

مطالعهٔ موردی 1: پیشگیری از کلاهبرداری انتقال سیمی شرکتی



سناریو: بخش مالی ایمیل فوری‌ای از یک نشانی فروشندهٔ جعلی دریافت می‌کند که می‌خواهد حواله‌های صورتحساب آینده به یک شمارهٔ مسیریابی جدید ارسال شود.

پرسش برای بحث: سیاست راستی‌آزمایی کلاهبرداری حواله را شرح دهید و بلوک‌های احراز هویت ایمیل را مشخص کنید.

مطالعهٔ موردی 2: رخداد فیشینگ نهنگ‌یابی علیه مدیران ارشد



سناریو: یک مدیر اجرایی روی پیوند فیشینگی کلیک کرد که ادعا می‌کرد سند جلسهٔ ایمن هیئت‌مدیره را در خود دارد و اعتبارنامه‌های اصلی شرکتی خود را روی یک پورتال جعلی وارد کرد.

پرسش برای بحث: مراحل واکنش به رخداد را شرح دهید و توضیح دهید چگونه ورودهای مدیر اجرایی را ممیزی کنیم.

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

1	2		26	29	32	16	32	23		32	32	1	15	1	29	16

24	32	24	10		10	32	32	1	4

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: کلاهبرداری آنلاین چیست؟

طرح کلاهبرداری که با استفاده از کانال‌های دیجیتال قربانیان را فریب می‌دهد تا پول بفرستند یا اعتبارنامهٔ شخصی خود را افشا کنند.

Q2: مهم‌ترین نشانهٔ فیشینگ ایمیلی چیست؟

پیامی که ادعای فوریت می‌کند (مانند تعلیق حساب) و شما را به پیوندی هدایت می‌کند که با دامنهٔ رسمی مطابقت ندارد.

Q3: typosquatting چیست؟

ثبت دامنه‌هایی با غلط‌های املایی رایج برندهای معروف (مانند amaz0n.com) برای میزبانی سایت‌های جعلی فیشینگ.

Q4: کلاه‌برداری پشتیبانی جعلی چیست؟

پنجرهٔ بازشو که ادعا می‌کند رایانه‌تان آلوده است و شما را هدایت می‌کند به شماره‌ای زنگ بزنید و بابت نرم‌افزار پاک‌سازی جعلی یا خدمات دسترسی از راه دور پول بپردازید. [1]

Q5: vishing چیست؟

حملات فیشینگ با تماس تلفنی صوتی برای فریب قربانیان تا اطلاعات حساب بانکی یا ورود را بدهند.

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

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

Q6: کلاه‌برداری بانکی از طریق انتقال وجه (wire fraud) به چه معناست؟

هدایت تراکنش‌های پرداخت به حساب‌های کلاهبرداری با جعل هویت فروشندگان یا مدیران.

Q7: whaling چیست؟

شکل بسیار هدفمند spear phishing که مستقیماً اهداف باارزش مانند مدیران ارشد شرکتی را نشانه می‌گیرد.

Q8: smishing چیست؟

پیامک‌های کلاهبرداری ارسال‌شده به دستگاه‌های همراه که حاوی پیوند به پورتال‌های جعلی یا به‌روزرسانی‌های ردیابی هستند.

Q9: چرا راستی‌آزمایی خارج از باند حیاتی است؟

جزئیات تراکنش را از طریق یک کانال ارتباطی جداگانه (مانند تماس تلفنی) تأیید می‌کند و از رشته‌های ایمیل در معرض خطر پرهیز می‌کند.

Q10: کلاهبرداری حساب امانی جعلی چگونه کار می‌کند؟

کلاهبرداران یک سایت امانی جعلی می‌سازند، ادعا می‌کنند وجه به‌طور امن نگه داشته می‌شود و سپس سپردهٔ حواله‌ای خریدار را می‌دزدند.

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

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

Q1: کلاهبرداران چگونه از BEC (نفوذ به ایمیل کسب‌وکار) برای اجرای کلاهبرداری انتقال بانکی استفاده می‌کنند؟

آن‌ها حساب ایمیل یک کارمند قانونی را تصاحب می‌کنند، رشته‌های صورت‌حساب را زیر نظر می‌گیرند و جزئیات پرداخت به‌روزشده با حساب‌های بانکی کلاهبرداری می‌فرستند.

Q2: خطر حملات هم‌شکل IDN در کلاهبرداری‌های آنلاین چیست؟

استفاده از نویسه‌های غیر-ASCII که شبیه حروف معمولی هستند (مثلاً 'а' سیریلیک) برای ثبت دامنه‌های جعلی که برندهای واقعی را تقلید می‌کنند.

Q3: چرا بررسی سرایند ایمیل در تشخیص کلاه‌برداری مهم است؟

IP واقعی سرور مبدأ و وضعیت اعتبارسنجی SPF/DKIM را آشکار می‌کند و نشان می‌دهد آیا دامنهٔ فرستنده جعلی است.

Q4: کلاه‌برداران پشتیبانی جعلی چگونه از نرم‌افزار دسکتاپ از راه دور سوءاستفاده می‌کنند؟

آن‌ها از ابزارهایی مانند AnyDesk یا TeamViewer برای اتصال به دستگاه قربانی، کاشتن بدافزار و سرقت گذرواژه‌های ذخیره‌شده استفاده می‌کنند.

Q5: هدف کلاه‌برداری‌های پیش‌پرداخت چیست؟

فریب دادن قربانیان برای پرداخت پیشاپیش هزینهٔ پردازش در ازای پاداش مالی بزرگی که وجود ندارد.

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

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

Q6: کلاه‌بردارها چگونه از پروفایل‌سازی شبکه‌های اجتماعی برای فیشینگ هدفمند استفاده می‌کنند؟

آن‌ها ساختارهای سازمانی شرکت‌ها و نام کارمندان را گردآوری می‌کنند تا ایمیل‌های فیشینگ هدفمند (spear-phishing) متقاعدکننده بنویسند.

Q7: چرا فروشگاه‌های وب جعلی تخفیف‌های شدید ارائه می‌دهند؟

برای وسوسه کردن خریداران به وارد کردن جزئیات کارت اعتباری و گرفتن اطلاعات ورود برای استفادهٔ مجدد یا فروش در انجمن‌های کارت‌دزدی.

Q8: رکوردهای DMARC چگونه کلاه‌برداری‌های فیشینگ را مسدود می‌کنند؟

DMARC به صاحبان دامنه اجازه می‌دهد از گیرنده‌ها بخواهند نامه‌هایی را که بررسی‌های هم‌راستای SPF و DKIM را رد نمی‌کنند، قرنطینه یا رد کنند و از جعل مستقیم جلوگیری شود. [5]

Q9: تهدید پورتال‌های برداشت اعتبارنامه چیست؟

صفحه‌های فرود جعلی که دقیقاً شبیه Microsoft 365 یا فضاهای کاری Google طراحی شده‌اند و اطلاعات ورود را همزمان با وارد شدن می‌دزدند.

Q10: تیم‌های امنیتی چگونه دامنه‌های کلاهبرداری را گزارش و غیرفعال می‌کنند؟

با ارسال شواهد کلاهبرداری به ایمیل سوءاستفادهٔ ثبت‌کننده، ارائه‌دهندهٔ میزبانی و رجیستری Google Safe Browsing.

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

فیشینگ و جعل هویت در سال 2025 با 191,561 شکایت، پرگزارش‌ترین نوع جرم نزد IC3 اف‌بی‌آی بودند. [2]

2. بینش امنیت

کلاهبرداری از طریق نفوذ به ایمیل کسب‌وکار (BEC) در سال 2025 باعث بیش از 3 میلیارد دلار زیان شد که به IC3 سازمان FBI گزارش شد. [2]

3. بینش امنیت

دامنه‌های دارای غلط تایپی عمدی یک یا دو نویسه با نام‌های واقعی برند تفاوت دارند، بنابراین نگاه سریع ممکن است آن‌ها را تشخیص ندهد.

4. بینش امنیت

کلاهبرداری‌های پشتیبانی فنی در سال 2025 بیش از 2.1 میلیارد دلار خسارت ایجاد کردند که به IC3 در FBI گزارش شد. [2]

5. بینش امنیت

حملات هم‌نگاشتی (homograph) در نوار آدرس مرورگر یکسان به نظر می‌رسند، مگر اینکه مرورگر پیکربندی‌های punycode را نمایش دهد.

6. بینش امنیت

کلاهبرداری‌های پیامکی (اسمیشینگ) از پیام‌های کوتاه و فوری حاوی پیوند استفاده می‌کنند و زمینهٔ اندکی برای تشخیص تقلب به قربانی می‌دهند.

7. بینش امنیت

حملات نهنگ‌یابی ایمیل مدیران ارشد را هدف می‌گیرند، زیرا آن‌ها دسترسی به انتقال‌های بانکی بزرگ را در اختیار دارند.

8. بینش امنیت

راستی‌آزمایی تغییر پرداخت با تماس با شمارهٔ تلفن شناخته‌شدهٔ ذخیره‌شده، دفاع کلیدی در برابر کلاهبرداری انتقال وجه BEC است.

9. بینش امنیت

وب‌سایت‌های حساب امانی جعلی کلاهبرداری رایج در بازارهای آنلاین هستند: شبیه یک سرویس پرداخت امن به نظر می‌رسند اما حوالهٔ خریدار را سرقت می‌کنند.

10. بینش امنیت

Google Safe Browsing پیش از باز کردن سایت‌هایی که برای فیشینگ یا بدافزار علامت‌گذاری کرده است به کاربران هشدار می‌دهد.

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.). 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

کلید پاسخ: ایستگاه بررسی 1 – چندگزینه‌ای

1 پرسش 1

پاسخ درست: A

نکتهٔ آموزشی

نشانهٔ اصلی کلاهبرداری پشتیبانی جعلی چیست؟ → پنجرهٔ بازشویی که ادعا می‌کند سیستم شما آلوده است و از شما می‌خواهد به یک شمارهٔ تلفن زنگ بزنید

2 پرسش 2

پاسخ درست: A

نکتهٔ آموزشی

کدام تکنیک از دامنه‌های فرستندهٔ جعلی برای سرقت جزئیات بانکی استفاده می‌کند؟ → فیشینگ ایمیلی

3 پرسش 3

پاسخ درست: A

نکتهٔ آموزشی

چه چیزی نمایندهٔ کلاهبرداری انتقال بانکی است؟ → فریب قربانیان با مهندسی اجتماعی برای ارسال پول به حساب‌های شرکتی جعلی

4 پرسش 4

پاسخ درست: A

نکتهٔ آموزشی

چرا کلاهبرداران وب‌سایت‌های خرید جعلی می‌سازند؟ → برای سرقت جزئیات کارت اعتباری و اعتبارنامهٔ پرداخت خریداران

5 پرسش 5

پاسخ درست: A

نکتهٔ آموزشی

ویشینگ به چه معناست؟ → کلاهبرداری فیشینگ صوتی از طریق شبکه‌های تلفن برای سرقت اعتبارنامه

کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

6 پرسش 6

پاسخ درست: نادرست

نکتهٔ آموزشی

نادرست: فیشینگ مدیران را هم هدف می‌گیرد؛ whaling فیشینگی است که رهبران ارشد را هدف قرار می‌دهد.

7 پرسش 7

پاسخ درست: درست

نکتهٔ آموزشی

دامنه‌های جعلی اغلب از غلط‌های تایپی جزئی (مانند amaz0n.com) برای تقلید از برندهای معتبر استفاده می‌کنند.

8 پرسش 8

پاسخ درست: نادرست

نکتهٔ آموزشی

نادرست: دادن دسترسی از راه دور به کلاهبردار پشتیبانی به او اجازه می‌دهد بدافزار بکارد و داده‌ها را بدزدد.

9 پرسش 9

پاسخ درست: درست

نکتهٔ آموزشی

مهندسی اجتماعی از روان‌شناسی انسان مانند ترس و فوریت برای دور زدن قواعد امنیتی سوءاستفاده می‌کند.

10 پرسش 10

پاسخ درست: درست

نکتهٔ آموزشی

درخواست‌های انتقال بانکی باید همیشه از طریق کانال‌های ارتباطی خارج از باند راستی‌آزمایی شوند.

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

G 1. فیشینگ	F 2. جعلی	D 3. ویشینگ	B 4. کلاهبرداری
H 5. راستی‌آزمایی	A 6. سیم	E 7. نهنگ‌یابی	C 8. اسمیشینگ

ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

1 فیشینگ	2 جعلی	3 ویشینگ	4 کلاهبرداری
5 تأیید	6 حواله		

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

1 B – جعلی	2 E – تأیید	3 F – حواله	4 H – اسمیشینگ
5 G – نهنگ	6 C – ویشینگ	7 A – فیشینگ	8 D – کلاهبرداری

یادداشت‌های بحث برای مدرسان

اصطلاحات کلیدی:
بررسی کنید که دانش‌آموزان بتوانند فیشینگ، جعلی و ویشینگ 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.

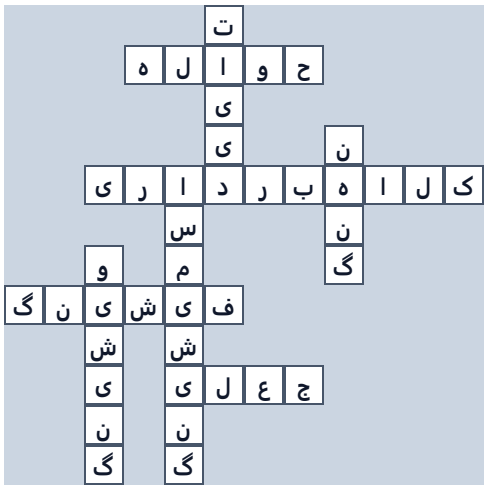
ارزیابی منابع:
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

کلیدهای معما و یادداشت‌های معلم

پاسخ جدول کلمات

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

پاسخ جدول‌کلمات



راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

افقی

2 افقی: حواله هدایت متقلبانهٔ تراکنش‌های بانکی به حساب‌های مجرمان. (5 حرف)

4 افقی: کلاهبرداری طرح فریبکارانه برای سرقت پول یا دسترسی به اعتبارنامه‌های قربانیان. (10 حرف)

7 افقی: فیشینگ کمپین‌های ایمیلی فریبکارانه برای سرقت اطلاعات ورود و گذرواژه‌ها. (6 حرف)

8 افقی: جعلی نشانی فرستندهٔ ایمیل یا وب‌سایتی که طوری تقلید شده که معتبر به نظر برسد. (4 حرف)

عمودی

1 عمودی: تأیید اطمینان از جزئیات پرداخت از طریق یک روش تماس ثانویهٔ مطمئن. (5 حرف)

3 عمودی: نهنگ حملات فیشینگ هدفمند برای سرقت اعتبارنامه از مدیران ارشد. (4 حرف)

5 عمودی: اسمیشینگ ارسال پیامک‌های کلاهبردارانه برای سرقت اعتبارنامه‌های حساب موبایل. (8 حرف)

6 عمودی: ویشینگ تماس‌های صوتی فریبکارانه برای سرقت اعتبارنامه‌ها و جزئیات حساب. (6 حرف)

کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

کلید مرتب‌سازی کلمات

1. شفینگی — فیشینگ
2. گوشنیی — ویشینگ
3. یتدیا — تأیید
4. گننه — نهنگ
5. یجلع — جعلی
6. ربهداکلریا — کلاهبرداری
7. لهحاو — حواله
8. یسشگانیم — اسمیشینگ

کلید چالش رمز مخفی

"شناسایی فیشینگ با تأیید دقیق"

کلید پاسخ مطالعات موردی

A مطالعهٔ موردی 1: پیشگیری از کلاهبرداری انتقال سیمی شرکتی

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: بخش مالی ایمیلی فوری از نشانی جعلی یک فروشنده دریافت می‌کند که می‌خواهد حواله‌های صورت‌حساب آینده به شمارهٔ مسیریابی جدیدی هدایت شود.
- راهبرد و راه‌حل پیشنهادی: سیاست تأیید دوگانه را برای همهٔ پرداخت‌ها اجرا کنید. تأیید خارج از باند را با شمارهٔ تلفن از پیش ذخیره‌شده پیاده کنید و ایمیل‌های دارای دامنهٔ جعلی را در دروازه مسدود کنید.

B مطالعهٔ موردی 2: رخداد فیشینگ نهنگ‌یابی علیه مدیران ارشد

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک مدیر اجرایی روی پیوند فیشینگی کلیک کرد که ادعا می‌کرد سندی امن برای جلسهٔ هیئت‌مدیره دارد و اطلاعات اصلی ورود سازمانی خود را در یک پورتال جعلی وارد کرد.
- راهبرد و راه‌حل پیشنهادی: دستگاه مدیر ارشد را ایزوله کنید. همهٔ توکن‌های نشست و اعتبارنامه‌های سازمانی را بازنشانی کنید. گزارش‌های دسترسی را از نظر خروج داده بررسی کنید و MFA سخت‌افزاری را روی همهٔ ورودها پیاده کنید.