نام: _____ تاریخ: _____ نمره: _____

حملات فیشینگ و مهندسی اجتماعی

فیشینگ هدفمند، کلاهبرداری‌های نهنگ‌شکاری (whaling)، پروتکل‌های SPF/DKIM/DMARC، جعل فرستنده و آموزش امنیتی کارکنان.

مرور آموزشی حملات فیشینگ

خوش آمدید! این بستهٔ فعالیت شما را در بررسی حملات فیشینگ و مهندسی اجتماعی راهنمایی می‌کند. با اسپیر فیشینگ، ویل‌ینگ، جعل دامنه، پروتکل‌های SPF/DKIM/DMARC، ایمنی پیوندها و آموزش آگاهی کارکنان 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/phishing-attacks/

نقشهٔ راه یادگیری کاهش خطر فیشینگ شما

- کلاهبرداری‌های رایج فیشینگ، ویشینگ و پنجره‌های بازشوی پشتیبانی را شناسایی کنید.
- رویه‌های تأیید تراکنش خارج از باند را پیاده‌سازی کنید.
- قوانین SPF، DKIM و DMARC را برای مسدود کردن دامنه‌های جعلی پیکربندی کنید.

راهنمای دستورالعمل‌های حملات فیشینگ

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

حملات فیشینگ و مهندسی اجتماعی (مقدمه)

حملات فیشینگ از پیام‌های هدفمند، کلاهبرداری نهنگ‌شکاری و جعل دامنه برای جمع‌آوری اعتبارنامه‌های ورود کاربران استفاده می‌کنند. ایمن‌سازی سامانه‌های شرکتی مستلزم استقرار قوانین SPF، DKIM و DMARC در دروازه در کنار مراحل تأیید از مسیر جداگانه است.

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

ایستگاه بررسی 1: چالش چندگزینه‌ای

1 **1. فیشینگ هدفمند (spear phishing) چیست؟**

- A. ایمیل فیشینگ هدفمند که برای یک فرد یا سازمان خاص سفارشی شده است
- B. ایمیل انبوه گسترده که برای میلیون‌ها نشانی تصادفی فرستاده می‌شود
- C. حملهٔ شبکه‌ای که سرورهای وب را با ترافیک اشباع می‌کند
- D. یک روش استخراج پایگاه داده که رکوردهای کاربران را هدف می‌گیرد

2 **2. کدام پروتکل به یک دامنه اجازه می‌دهد نشانی‌های IP مجاز ارسال خود را برای مبارزه با جعل در DNS فهرست کند؟**

- A. SPF
- B. DKIM
- C. DMARC
- D. HTTPS

3 **3. حملهٔ نهنگ‌یابی چیست؟**

- A. کارزار فیشینگی که به‌طور ویژه مدیران ارشد شرکتی سرشناس را هدف می‌گیرد
- B. حملهٔ تزریق SQL که پشتیبان‌های پایگاه داده را هدف می‌گیرد
- C. سرقت فیزیکی تجهیزات مسیریاب شبکهٔ محلی
- D. یک اسکن خودکار حدس‌زنی بی‌رحمانه با پر کردن اعتبارنامه

4 **4. DKIM چه کاری انجام می‌دهد؟**

- A. امضای رمزنگاری به ایمیل‌ها می‌افزاید تا اصالت فرستنده تأیید شود
- B. ترافیک بسته‌های شبکهٔ ورودی را در دیوار آتش مسدود می‌کند
- C. رمزگذاری حجم‌های ذخیره‌سازی پایگاه داده در حالت سکون
- D. پیوست‌های ایمیل را برای یافتن بدافزار مبتنی بر امضا اسکن می‌کند

5 **5. نقش DMARC چیست؟**

- A. تعیین نحوهٔ برخورد سرورهای ایمیل گیرنده با بررسی‌های ناموفق SPF/DKIM
- B. رمزگشایی گذرواژه‌های سیستم با استفاده از جدول‌های رنگین‌کمان از پیش محاسبه‌شده
- C. فشرده‌سازی پیوست‌های ایمیل پیش از ارسال
- D. پیکربندی امتیازهای دسترسی مسیریابی شبکه

ایستگاه بررسی 2: چالش درست یا نادرست

6 پرسش 6

6. فیشینگ هدفمند (spear phishing) به ایمیل‌های انبوه عمومی ارسال‌شده به میلیون‌ها نشانی تصادفی متکی است.

○ درست ○ نادرست

7 پرسش 7

7. سیاست‌های DMARC می‌توانند به سرورهای ایمیل دستور دهند پیام‌های جعلی غیرمجاز را رد کنند.

○ درست ○ نادرست

8 پرسش 8

8. راستی‌آزمایی SPF با اعتبارسنجی امضای رمزنگاری بدنهٔ ایمیل انجام می‌شود.

○ درست ○ نادرست

9 پرسش 9

9. حملات نهنگ‌یابی مدیران سطح پایین شرکت را برای دسترسی به فایل‌های پایگاه داده هدف می‌گیرند.

○ درست ○ نادرست

10 پرسش 10

10. تأیید خارج از باند (out-of-band) درخواست‌های پرداخت به توقف کلاهبرداری‌های حواله مالی کمک می‌کند.

○ 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. هدف‌گیری یک کارمند خاص با اطلاعات شخصی‌شده، فیشینگ _____ است.
2. ساختگی کردن سرایند ایمیل برای معتبر جلوه دادن پیام‌ها، جعل _____ فرستنده نام دارد.
3. فهرست رکوردهای DNS از IPهای مجاز سرور ایمیل، _____ است.
4. استاندارد امضای ایمیل که تأیید فرستنده را فراهم می‌کند، _____ است.
5. تعیین سیاست‌هایی برای رد بررسی‌های ناموفق SPF/DKIM از _____ استفاده می‌کند.
6. کمپین فیشینگی که مدیران ارشد را هدف می‌گیرد، «شکار _____ » نام دارد.

بانک واژگان

جعل | نشانی | نهنگ | ویشینگ | هدفمند | DKIM | DMARC | SPF

پاسخ‌های خود را اینجا بنویسید:

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

ایستگاه بررسی 4: تطبیق مفاهیم امنیت

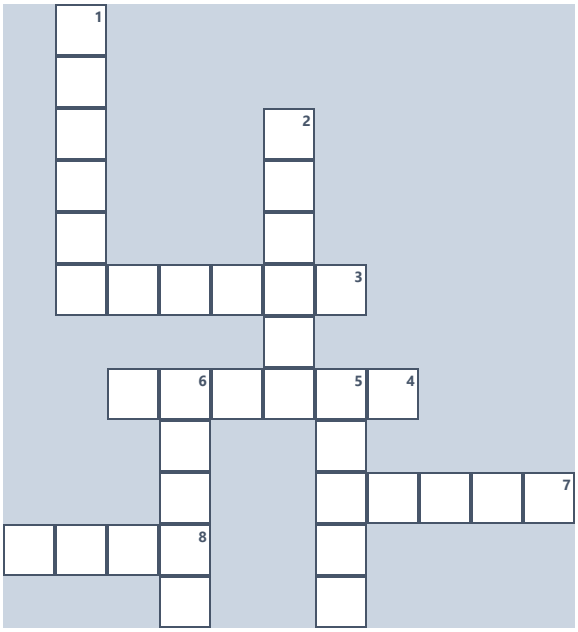
تطبیق تعاریف

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 نیزه‌ای	A	تماس‌های کلاهبرداری صوتی.
2. جعل	B	هدف قرار دادن مدیران ارشد.
3. SPF	C	دستورهای رد سیاست.
4. DKIM	D	IPهای مجاز فرستنده در DNS.
5. DMARC	E	ایمیل مهندسی اجتماعی.
6. نهنگ‌یابی	F	ایمیل هدفمند شخصی‌سازی‌شده.
7. فیشینگ	G	جعل آدرس ایمیل فرستنده.
8. ویشینگ	H	امضای رمزنگاری در ایمیل.

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. ایمیل مهندسی اجتماعی. (6)

4. ایمیل شخصی‌سازی‌شده و هدف‌گیری‌شده. (6)

7. دستورالعمل سیاست رد پیام. (5)

8. هدف قرار دادن مدیران ارشد. (4)

عمودی

1. تماس‌های کلاهبردارانهٔ صوتی. (6)

2. فهرست IPهای مجاز فرستنده در DNS. (6)

5. امضای رمزنگاری در ایمیل. (5)

6. تغییر دروغین آدرس ایمیل فرستنده. (5)

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: ایمیل مهندسی اجتماعی. (6 حرف):

4 افقی: ایمیل شخصی‌سازی‌شده و هدف‌گیری‌شده. (6 حرف):

7 افقی: دستورالعمل سیاست رد پیام. (5 حرف):

8 افقی: هدف قرار دادن مدیران ارشد. (4 حرف):

عمودی

1 عمودی: تماس‌های کلاهبردارانهٔ صوتی. (6 حرف):

2 عمودی: فهرست IPهای مجاز فرستنده در DNS. (6 حرف):

5 عمودی: امضای رمزنگاری در ایمیل. (5 حرف):

6 عمودی: تغییر دروغین آدرس ایمیل فرستنده. (5 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.

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

فهرست واژگان

هدفمند　نشانی　اسپیاف　دیکیم　دمارک　نهنگ　فیشینگ　ویشینگ

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. هدفمند	1. تغییر دروغین آدرس ایمیل فرستنده.
B. نشانی	2. ایمیل شخصی‌سازی‌شده و هدف‌گیری‌شده.
C. اسپیاف	3. تماس‌های کلاهبردارانهٔ صوتی.
D. دیکیم	4. فهرست IPهای مجاز فرستنده در DNS.
E. دمارک	5. ایمیل مهندسی اجتماعی.
F. نهنگ	6. دستورالعمل سیاست رد پیام.
G. فیشینگ	7. امضای رمزنگاری در ایمیل.
H. ویشینگ	8. هدف قرار دادن مدیران ارشد.

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. ف ه م ن د د
2. ف ا پ ا ی س
3. ا د ک ر م
4. گ ی ش ن ف ی
5. ا ی ن ن ش
6. ی د ک م ی
7. ن ن گ ه
8. ش گ و ن ی ی

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	نشانه‌های ایمیل فیشینگ		
3	نشانه‌های آلوده بودن رایانه		
4	واژه‌هایی که فوریت جعلی ایجاد می‌کنند		
5	روش‌های بررسی فرستنده		
6	افرادی که می‌توانید برای کمک فناوری اطلاعات از آن‌ها بپرسید		
7	چیزهایی که پشتیبان می‌گیرید		
8	ماهی‌ها یا موجودات دریایی که می‌شناسید		
9	شرکت‌هایی که کلاهبرداران خود را جای آن‌ها جا می‌زنند		
10	عادت‌های ایمن که می‌توانید از امروز شروع کنید		
11	کارهایی که پس از کلیک بر پیوند جعلی باید انجام داد		
12	کارهایی که پس از نشت داده باید انجام داد		
13	کانال‌هایی که فیشینگ در آن‌ها رخ می‌دهد		
14	چیزهایی که هرگز با ایمیل نمی‌فرستید		
15	روش‌های محافظت از حساب‌هایتان		

ایستگاه بررسی 8: مطالعات موردی امنیت سایبری

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

مطالعهٔ موردی 1: رفع حملهٔ نهنگ‌یابی علیه مدیران ارشد



سناریو: یک مدیر ارشد مالی (CFO) ایمیلی بسیار شخصی‌سازی‌شده دریافت می‌کند که ادعا می‌کند از طرف مدیرعامل است و برای نهایی کردن یک خرید محرمانهٔ دامنه، حوالهٔ سریع $50,000 می‌خواهد.

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

مطالعهٔ موردی 2: استقرار سیاست‌های دروازهٔ SPF/DKIM/DMARC



سناریو: یک سازمان در ممیزی‌های امنیتی مردود می‌شود، چون ایمیل‌های بازاریابی خروجی مکرراً هرزنامه علامت‌گذاری می‌شوند و هکرها فعالانه دامنهٔ برند شرکت را جعل می‌کنند.

پرسش برای بحث: کنترل‌های فنی و مدیریتی برای راستی‌آزمایی اصالت ایمیل برقرار 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

32	15	10	29	31	28		32	32	1	15	1	29	16

31	13	1	30	12	10		1	2		32	21	1	28	4	6	1

27	32	28	32	1

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: فیشینگ چیست؟

فیشینگ یک حملهٔ مهندسی اجتماعی است که در آن مجرمان پیام‌های جعلی می‌فرستند تا کاربران را به اشتراک‌گذاری داده‌های حساس فریب دهند.

Q2: تفاوت فیشینگ و فیشینگ هدفمند چیست؟

فیشینگ گروه‌های گسترده را با محتوای عمومی هدف می‌گیرد، در حالی که فیشینگ هدفمند قربانیان مشخص را با جزئیات سفارشی هدف قرار می‌دهد.

Q3: whaling چیست؟

نهنگ‌یابی یک حملهٔ فیشینگ بسیار هدفمند است که مدیران ارشد صاحب‌نام دارای قدرت اجرایی را نشانه می‌گیرد.

Q4: جعل ایمیل چیست؟

جعل ایمیل یعنی ساخت پیام‌های ایمیل با نشانی فرستندهٔ جعلی برای فریب گیرنده تا به منبع اعتماد کند.

Q5: SPF چگونه از جعل جلوگیری می‌کند؟

فهرستی از آدرس‌های IP مجاز ارسال را در DNS منتشر می‌کند و به سرورهای دریافت‌کننده اجازه می‌دهد منبع نامه را راستی‌آزمایی کنند. [1]

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

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

Q6: DKIM چیست؟

DomainKeys Identified Mail یک امضای رمزنگاری به سرآیندهای ایمیل اضافه می‌کند و ثابت می‌کند یک دامنه مسئولیت را پذیرفته و پیام تغییر نکرده است.

Q7: DMARC مخفف چیست؟

احراز هویت، گزارش‌دهی و انطباق پیام مبتنی بر دامنه. [2]

Q8: سیاست DMARC چیست؟

سیاستی که به سرورهای ایمیل می‌گوید با پیام‌هایی که SPF/DKIM را رد می‌کنند چگونه رفتار کنند (هیچ، قرنطینه یا رد). [2]

Q9: vishing چیست؟

فیشینگ صوتی، که در آن مهاجمان با تماس‌های تلفنی جعلی تلاش می‌کنند اطلاعات مدیریتی یا مالی را استخراج کنند.

Q10: اسکنرهای پیوند چگونه کمک می‌کنند؟

آن‌ها پیوندهای ایمیل ورودی را اسکن و بازنویسی می‌کنند تا ایمنی صفحات وب مقصد را در لحظهٔ کلیک بررسی 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 هم‌شکل (homograph) چگونه کار می‌کند؟

مهاجمان نام‌های دامنه را با نویسه‌های یونیکد غیر ASCII شبیه به دامنهٔ معتبر ثبت می‌کنند تا از نظر ظاهری آن را تقلید کنند.

Q2: نمایش punycode چیست؟

کدگذاری‌ای که نام‌های دامنهٔ Unicode را به رشته‌های سازگار با ASCII با پیشوند 'xn--' تبدیل می‌کند تا DNS بتواند آن‌ها را مدیریت کند.

Q3: چرا 'p=reject' امن‌ترین حالت DMARC است؟

از سرورهای دریافت‌کننده می‌خواهد نامه‌هایی را که در نشست SMTP در DMARC (SPF/DKIM همسو) ناموفق‌اند رد کنند و جعل مستقیم را مسدود می‌کند. [2]

Q4: مهاجمان چگونه قوانین SPF را دور می‌زنند؟

با سوءاستفاده از دامنه‌های شبیه‌ساز (typosquatting) یا استفاده از حساب‌های به‌خطرافتاده در سرویس‌های ایمیل شخص ثالث معتبر.

Q5: نفوذ به ایمیل کسب‌وکار (BEC) چیست؟

کلاهبرداری شرکتی که در آن مهاجمان حساب‌های ایمیل کسب‌وکار را ربوده یا جعل می‌کنند تا پرداخت‌های جعلی را تأیید کنند.

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

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

Q6: احراز هویت چندعاملی چگونه جلوی فیشینگ را می‌گیرد؟

توکن‌های ثانویه (مانند کلیدهای سخت‌افزاری) را الزامی می‌کند که فقط از طریق صفحات فرود شبیه‌سازی‌شده قابل سرقت نیستند.

Q7: صفحهٔ فرود برداشت اعتبارنامه چیست؟

درگاه ورود شبیه اصلی که برای ضبط لحظه‌ای نام‌های کاربری، گذرواژه‌ها و توکن‌های MFA واردشده طراحی شده است.

Q8: ربایش زیردامنه چیست؟

مهاجمی که کنترل یک اشاره‌گر زیردامنهٔ DNS استفاده‌نشده را به دست می‌گیرد تا صفحات فرود فیشینگ مخرب را زیر یک دامنهٔ والد مورد اعتماد میزبانی کند.

Q9: بررسی هم‌ترازی DKIM چگونه کار می‌کند؟

راستی‌آزمایی می‌کند که دامنهٔ سرایند 'From' با دامنه‌ای که پیام را در سرایند DKIM با رمزنگاری امضا کرده مطابقت دارد.

Q10: نقش دروازهٔ ایمیل چیست؟

پالایش ایمیل ورودی، حسابرسی پیوندها، جعبه‌شنی‌سازی پیوست‌ها و اعتبارسنجی انطباق SPF/DKIM/DMARC.

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. [4]

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. [4]

3. بینش امنیت

حملات هم‌نگاشتی از حروف شبیه سیریلیک استفاده می‌کنند تا دامنه‌های برند با تطابق دقیق را در مرورگرها به‌صورت بصری تکرار کنند.

4. بینش امنیت

با 'p=reject'، دامنه از دریافت‌کنندگان می‌خواهد ایمیل‌های ناموفق را هنگام تحویل رد کنند، نه اینکه آن را به‌عنوان هرزنامه بایگانی کنند. [2]

5. بینش امنیت

حملات نهنگ‌یابی که مدیرعامل‌ها را هدف می‌گیرند، معمولاً پرداخت‌های فوری برای ادغام‌های محرمانه یا خرید دامنه را درخواست می‌کنند.

6. بینش امنیت

درگاه‌های برداشت اعتبارنامه صفحه‌های ورود واقعی را کپی می‌کنند تا قربانیان گذرواژه‌ها را مستقیماً در فرم مهاجم تایپ کنند.

7. بینش امنیت

راهنمای مشترک فیشینگ CISA، آموزش کاربران را در کنار DMARC، SPF، DKIM و MFA مقاوم در برابر فیشینگ توصیه می‌کند. [3]

8. بینش امنیت

ارزیابی SPF به 10 عبارت پرس‌وجوکنندهٔ DNS محدود است؛ فراتر رفتن از این حد نتیجهٔ 'permerror' برمی‌گرداند. [1]

9. بینش امنیت

کلیدهای امنیتی سخت‌افزاری FIDO2 حفاظتی با پشتوانهٔ رمزنگاری در برابر برداشت اعتبارنامه از راه دور فراهم می‌کنند.

10. بینش امنیت

فیشینگ یکی از رایج‌ترین راه‌هایی است که مهاجمان نخست وارد یک سازمان می‌شوند، به همین دلیل آموزش منظم آگاهی‌رسانی یک دفاع مؤثر است.

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] IETF. (2014). RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1.

https://www.rfc-editor.org/rfc/rfc7208.html

[2] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).

https://www.rfc-editor.org/rfc/rfc7489.html

[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] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

کلید پاسخ: ایستگاه بررسی 1 – چندگزینه‌ای

1 پرسش 1 — پاسخ درست: **A**

نکتهٔ آموزشی

فیشینگ هدفمند (spear phishing) چیست؟ → ایمیل فیشینگ هدفمند که برای یک فرد یا سازمان خاص سفارشی شده است

2 پرسش 2 — پاسخ درست: **A**

نکتهٔ آموزشی

SPF میزبان‌های مجاز ارسال یک دامنه را در DNS منتشر می‌کند تا گیرندگان بتوانند فرستندهٔ envelope را بررسی کنند.

3 پرسش 3 — پاسخ درست: **A**

نکتهٔ آموزشی

حملهٔ نهنگ‌یابی چیست؟ → کارزار فیشینگی که به‌طور ویژه مدیران ارشد شرکتی سرشناس را هدف می‌گیرد

4 پرسش 4 — پاسخ درست: **A**

نکتهٔ آموزشی

DKIM چه کاری انجام می‌دهد؟ → امضای رمزنگاری به ایمیل‌ها می‌افزاید تا اصالت فرستنده تأیید شود

5 پرسش 5 — پاسخ درست: **A**

نکتهٔ آموزشی

نقش DMARC چیست؟ → تعیین نحوهٔ برخورد سرورهای ایمیل گیرنده با بررسی‌های ناموفق SPF/DKIM

کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

6 پرسش 6

پاسخ درست: نادرست

نکتهٔ آموزشی

نادرست: spear phishing برای افراد مشخص سفارشی‌سازی می‌شود، برخلاف فیشینگ انبوه عمومی.

7 پرسش 7

پاسخ درست: درست

نکتهٔ آموزشی

سیاست‌های DMARC می‌توانند به سرورهای ایمیل دستور دهند پیام‌های جعلی غیرمجاز را رد کنند.

8 پرسش 8

پاسخ درست: نادرست

نکتهٔ آموزشی

نادرست: SPF نشانی IP فرستنده را با DNS بررسی می‌کند؛ این DKIM است که یک امضای رمزنگاری را تأیید می‌کند.

9 پرسش 9

پاسخ درست: نادرست

نکتهٔ آموزشی

نادرست: whaling مدیران ارشد را هدف می‌گیرد، چون می‌توانند پرداخت‌ها را تأیید کنند و به داده‌های حساس دسترسی دارند.

10 پرسش 10

پاسخ درست: درست

نکتهٔ آموزشی

درست: تأیید درخواست‌های پرداخت از طریق یک کانال جداگانهٔ شناخته‌شده به توقف کلاهبرداری حواله کمک می‌کند.

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

F 1. فیشینگ نیزه‌ای	G 2. جعل	D 3. SPF	H 4. DKIM
C 5. DMARC	B 6. نهنگ‌یابی	E 7. فیشینگ	A 8. ویشینگ

ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

1 هدفمند	2 نشانی	3 SPF	4 DKIM
5 DMARC	6 نهنگ		

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

1 B – نشانی	2 A – هدفمند	3 H – ویشینگ	4 C – اسپیاف
5 G – فیشینگ	6 E – دمارک	7 D – دیکیم	8 F – نهنگ

یادداشت‌های بحث برای مدرسان

اصطلاحات کلیدی:
بررسی کنید که دانش‌آموزان بتوانند فیشینگ نیزه‌ای، جعل و SPF 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.

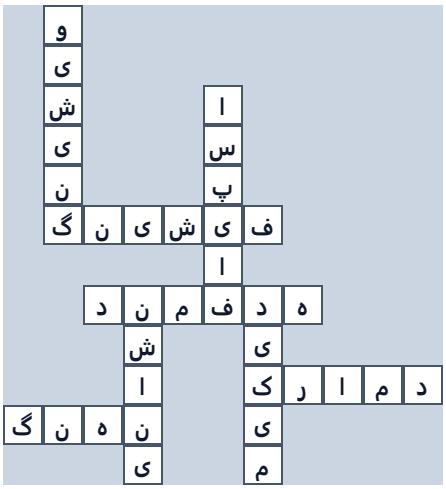
ارزیابی منابع:
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

کلیدهای معما و یادداشت‌های معلم

پاسخ جدول کلمات

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

پاسخ جدول‌کلمات



راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

افقی

3 افقی: فیشینگ ایمیل مهندسی اجتماعی. (6 حرف)

4 افقی: هدفمند ایمیل شخصی‌سازی‌شده و هدف‌گیری‌شده. (6 حرف)

7 افقی: دمارک دستورالعمل سیاست رد پیام. (5 حرف)

8 افقی: نهنگ هدف قرار دادن مدیران ارشد. (4 حرف)

عمودی

1 عمودی: ویشینگ تماس‌های کلاهبردارانهٔ صوتی. (6 حرف)

2 عمودی: اسپیاف فهرست IPهای مجاز فرستنده در DNS. (6 حرف)

5 عمودی: دیکیم امضای رمزنگاری در ایمیل. (5 حرف)

6 عمودی: نشانی تغییر دروغین آدرس ایمیل فرستنده. (5 حرف)

کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

کلید مرتب‌سازی کلمات

1. فهمندد → هدفمند
2. فاپایس → اسپیاف
3. ادکرم → دمارک
4. گیشنفی → فیشینگ
5. اینئش → نشانی
6. یدکمی → دیکیم
7. ننگه → نهنگ
8. شگونیی → ویشینگ

کلید چالش رمز مخفی

"شناسایی مهندسی اجتماعی با دروازه ایمیل"

کلید پاسخ مطالعات موردی

A مطالعهٔ موردی 1: رفع حملهٔ نهنگ‌یابی علیه مدیران ارشد

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک مدیر ارشد مالی ایمیلی بسیار شخصی‌سازی‌شده دریافت می‌کند که ادعا می‌کند از طرف مدیرعامل است و حواله‌ای فوری به مبلغ 50,000 دلار برای نهایی‌کردن خرید محرمانهٔ یک دامنه می‌خواهد.
- راهبرد و راه‌حل توصیه‌شده: DMARC را با سیاست 'p=reject' پیکربندی کنید تا دامنه‌های فرستندهٔ جعلی مسدود شوند. بنرهای هشدار فرستندهٔ خارجی را در دروازه اضافه کنید و برای همهٔ تراکنش‌های مالی تأیید شفاهی خارج از باند را الزامی کنید.

B مطالعهٔ موردی 2: استقرار سیاست‌های دروازهٔ SPF/DKIM/DMARC

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک سازمان در ممیزی‌های امنیتی رد می‌شود، زیرا ایمیل‌های بازاریابی خروجی آن مرتب به‌عنوان هرزنامه علامت‌گذاری می‌شوند و هکرها فعالانه دامنهٔ برند شرکت را جعل می‌کنند.
- راهبرد و راه‌حل پیشنهادی: یک رکورد TXT برای SPF منتشر کنید که IPهای فرستندهٔ مجاز را مشخص کند. کلیدهای امضای DKIM را روی سرورهای ایمیل خروجی پیکربندی کنید و گزارش‌های بازخورد XML مربوط به DMARC را برای شناسایی سوءاستفاده تحلیل کنید.