姓名: _____ 日期: _____ 得分: _____

网络钓鱼攻击与社会工程

鱼叉式网络钓鱼、鲸钓诈骗、SPF/DKIM/DMARC 协议、发件人伪造和员工安全培训。

网络钓鱼攻击学习概览

受保护
数据加密
256 位 AES 标准

合规的
全球标准
GDPR 与 CCPA 框架

零信任
访问策略
多重身份验证

欢迎！ 本活动手册将带你了解网络钓鱼攻击和社会工程。你将探索鱼叉式网络钓鱼、鲸钓、域名欺骗、SPF/DKIM/DMARC 协议、链接安全和员工意识培训。

练习单检查点

- [ ] **第 1-4 部分: 掌握网络安全和威胁防范。**
- [ ] **第 5-7 部分: 解答填字游戏和单词搜索谜题。**
- [ ] **第 8-9 部分: 解答案例研究和密码挑战。**
- [ ] **第 10 部分: 查看基础和进阶 FAQ 页面。**
- [ ] **第 11 部分: 探索 10 个有趣的现实事实。**
- [ ] **附加: 快速思考挑战。**

打开 VPN.com 网络安全指南

URL: https://www.vpn.com/cybersecurity/phishing-attacks/

你的网络钓鱼防范学习路线图

- 识别常见的网络钓鱼、语音钓鱼和技术支持弹窗诈骗。
- 实施带外交易验证流程。
- 配置 SPF、DKIM 和 DMARC 规则以拦截伪造域名。

网络钓鱼攻击指南说明

回答单项选择题和判断题，使用词库完成填空句，配对定义，并解答填字游戏和找词游戏。将所学知识应用于电子邮件身份验证。 最后完成附加活动: 快速思考。

网络钓鱼攻击与社会工程（简介）

网络钓鱼攻击利用定向消息、鲸钓骗局和域名欺骗来窃取用户登录凭据。保护企业系统需要在网关处部署 SPF、DKIM 和 DMARC 规则，并配合带外审批步骤。

仔细阅读每个检查点，选择或写出正确的答案。

检查点 1: 单项选择挑战

1. 什么是鱼叉式网络钓鱼?
   - A. 针对特定个人或组织定制的定向网络钓鱼邮件
   - B. 发送给数百万个随机地址的大范围群发邮件
   - C. 向网络服务器发送海量流量的网络攻击
   - D. 一种针对用户记录的数据库提取技术

2. 哪种协议允许域名在 DNS 中列出其授权发送 IP 地址以对抗仿冒?
   - A. SPF
   - B. DKIM
   - C. DMARC
   - D. HTTPS

3. 什么是鲸钓攻击?
   - A. 专门针对知名企业高管的网络钓鱼活动
   - B. 针对数据库备份的 SQL 注入攻击
   - C. 对局域网路由器设备的实物盗窃
   - D. 自动化的凭据填充暴力破解扫描

4. 4. DKIM 有什么作用?
   - A. 为电子邮件添加加密签名以验证发件人真实性
   - B. 在防火墙处阻止传入的网络数据包流量
   - C. 对静态存储的数据库存储卷进行加密
   - D. 扫描电子邮件附件中基于特征码的恶意软件

5. 5. DMARC 的作用是什么?
   - A. 指示接收方邮件服务器如何处理未通过 SPF/DKIM 检查的邮件
   - B. 使用预先计算的彩虹表破解系统密码
   - C. 发送前压缩电子邮件附件
   - D. 配置网络路由访问权限

检查点 2: 判断正误挑战

6 问题 6

6. 鱼叉式网络钓鱼依赖于发送给数百万随机地址的通用批量邮件。

○ 正确 ○ 错误

7 问题 7

7. DMARC 策略可以指示邮件服务器拒收未经授权的伪造邮件。

○ 正确 ○ 错误

8 问题 8

8. SPF 验证通过校验电子邮件正文的加密签名来运作。

○ 正确 ○ 错误

9 问题 9

9. 鲸钓攻击以低级企业管理员为目标，以获取数据库文件。

○ 正确 ○ 错误

10 问题 10

10. 对付款请求进行带外验证有助于阻止电汇诈骗。

○ 正确 ○ 错误

检查点 3: 关键术语填空

阅读下面的每个句子，并从词库中选出正确的术语填空。

1. 利用个性化信息针对特定员工发起攻击称为 _____ 钓鱼。
2. 篡改邮件头使邮件看起来合法，称为发件人 _____ 。
3. 授权发件服务器 IP 的 DNS 记录列表是 _____ 。
4. 提供发件人验证的电子邮件签名标准是 _____ 。
5. 制定拒绝未通过 SPF/DKIM 检查邮件的策略，使用的是 _____ 。
6. 针对企业高管的钓鱼活动称为 _____ 。

词汇词库

钓鱼邮件　鲸钓攻击　伪造　鱼叉　语音钓鱼　DKIM　DMARC　SPF

在此写下你的答案:

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

检查点 4: 安全概念配对

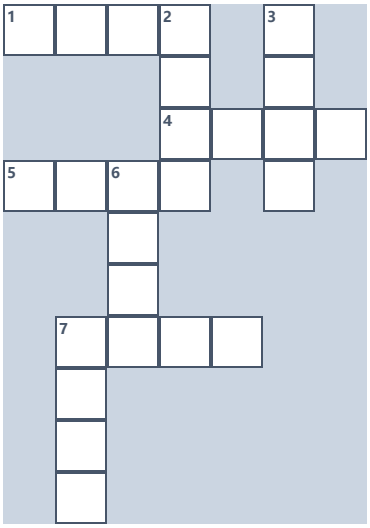
定义配对

将左侧的每个词汇与右侧正确的定义配对，在可填写的输入框中写出对应的字母（A-H）。

	1. 鱼叉式	**A**	基于语音的诈骗电话。
	2. 欺骗	**B**	针对 C 级高管。
	3. SPF	**C**	策略拒绝指令。
	4. DKIM	**D**	DNS 授权的发件人 IP。
	5. DMARC	**E**	社会工程学邮件。
	6. 鲸钓攻击	**F**	个性化定向电子邮件。
	7. 网络钓鱼	**G**	伪造发件人电子邮件地址。
	8. 语音钓鱼	**H**	电子邮件中的加密签名。

检查点 5: 填字游戏

在活动的白色方框中输入汉字，完成填字游戏。数字对应下面的提示。



横向

1. 社会工程类电子邮件 (4)

4. 利用伪装的消息或网站诱骗用户交出敏感信息的攻击 (4)

5. 基于语音的诈骗电话 (4)

7. 电子邮件中的加密签名 (4)

纵向

2. 个性化的定向电子邮件 (4)

3. 以企业高管为目标 (4)

6. 冒充可信机构、诱骗收件人交出信息的欺诈邮件 (4)

7. 伪造发件人邮箱地址 (4)

检查点 5 替代活动: 无障碍填字线索

使用屏幕阅读器和键盘的用户可以直接在下面的文本框中输入填字游戏的答案。

横向

1 横向: 社会工程类电子邮件 (4 字):

4 横向: 利用伪装的消息或网站诱骗用户交出敏感信息的攻击 (4 字):

5 横向: 基于语音的诈骗电话 (4 字):

7 横向: 电子邮件中的加密签名 (4 字):

纵向

2 纵向: 个性化的定向电子邮件 (4 字):

3 纵向: 以企业高管为目标 (4 字):

6 纵向: 冒充可信机构、诱骗收件人交出信息的欺诈邮件 (4 字):

7 纵向: 伪造发件人邮箱地址 (4 字):

检查点 6: 隐藏单词搜索

在下方网格中找出隐藏的 8 个关键词汇。单词可以是水平、垂直或对角线方向。

全 址 隧 安 息 邮 用 私 邮 共 鱼 输 务 墙 系
攻 协 护 软 火 全 人 服 网 安 理 协 击 私 鲸
务 鱼 器 安 份 私 访 公 身 络 信 风 户 软 域
务 钓 数 理 叉 络 护 址 道 问 钓 访 叉 险 传
录 叉 安 设 域 邮 器 名 伪 认 音 鱼 软 造 息
统 鱼 火 密 管 件 访 语 保 份 备 认 统 造 软
险 加 隧 传 公 签 用 防 音 址 数 网 数 加 击
钓 防 域 钓 议 名 造 人 协 钓 务 设 证 域 务
击 访 份 身 协 件 系 隐 证 证 鱼 件 管 传 人
攻 共 护 据 输 软 险 接 理 据 录 服 输 音 浏
鱼 邮 件 伪 造 加 叉 录 息 协 私 鲸 服 身 鲸
钓 务 设 伪 钓 系 加 道 数 网 鲸 风 服 钓 议
络 务 险 务 鱼 信 私 问 服 管 件 认 攻 用 访
理 叉 输 信 邮 设 览 户 络 络 设 击 击 身 统
人 造 件 域 件 管 人 理 码 身 语 数 息 理 伪

词汇列表

邮件签名 **邮件伪造** **钓鱼邮件** **语音钓鱼** **鱼叉钓鱼** **钓鱼攻击** **网络钓鱼** **鲸钓攻击**

检查点 6 替代活动: 无障碍词汇配对

将词语搜索中的 8 个词汇与其正确的定义配对，在空白处写出字母（A-H）。

词汇术语
A. 邮件签名
B. 邮件伪造
C. 钓鱼邮件
D. 语音钓鱼
E. 鱼叉钓鱼
F. 钓鱼攻击
G. 网络钓鱼
H. 鲸钓攻击

定义与配对字段
1. 伪造发件人邮箱地址。
2. 电子邮件中的加密签名。
3. 以企业高管为目标。
4. 冒充可信机构、诱骗收件人交出信息的欺诈邮件。
5. 社会工程类电子邮件。
6. 个性化的定向电子邮件。
7. 基于语音的诈骗电话。
8. 利用伪装的消息或网站诱骗用户交出敏感信息的攻击。

检查点 7: 乱序单词挑战

把下面的汉字重新排列，找出关键的网络安全概念和术语。把答案写在提供的输入框中。

1. 签 邮 名 件 _____

2. 钓 邮 件 鱼 _____

3. 鱼 鱼 钓 叉 _____

4. 鱼 钓 网 络 _____

5. 造 邮 伪 件 _____

6. 钓 鱼 语 音 _____

7. 攻 钓 击 鱼 _____

8. 鲸 击 攻 钓 _____

附加活动: 快速思考

每个类别写出 3 个答案。最先填完列表的人获胜。

1	可能被黑客入侵的设备			
2	网络钓鱼邮件的迹象			
3	电脑被感染的迹象			
4	制造虚假紧迫感的词语			
5	核实发件人的方法			
6	可以向其寻求 IT 帮助的人			
7	你要备份的内容			
8	你知道的鱼或海洋生物			
9	骗子假冒的公司			
10	你今天就可以开始的安全习惯			
11	点击虚假链接后要做的事			
12	数据泄露后要做的事			
13	发生网络钓鱼的渠道			
14	你绝不应通过电子邮件发送的内容			
15	保护账户的方法			

检查点 8: 网络安全案例研究

运用你所学的概念来解决下面的真实情景。

案例研究 1: 高管捕鲸攻击的补救



情景: 一位首席财务官收到一封高度个性化的邮件，声称来自 CEO，要求迅速电汇 50,000 美元以完成一笔保密的域名购买。

讨论问题: 分析品牌仿冒风险，并详细说明 SPF/DKIM/DMARC 和身份验证控制措施。

案例研究 2: 部署 SPF/DKIM/DMARC 网关策略



情景: 一家企业未能通过安全审计，原因是其外发的营销邮件经常被标记为垃圾邮件，并且黑客正在积极仿冒该公司的品牌域名。

讨论问题: 建立技术和管理控制措施来验证电子邮件的真实性。

检查点 9: 破解密码

网络安全专业人员保护网络资产免受网络威胁行为者的攻击。使用下面的汉字与数字对照表，在空白处写出对应的汉字，解密这条信息。

汉字转数字加密密钥

邮=1 网=2 件=3 现=4 社=5 叉=6 数=7 攻=8 鲸=9 造=10

发=11 络=12 音=13 鱼=14 交=15 钓=16 语=17 击=18 安=19 全=20

签=21 名=22 工=23 用=24 伪=25 据=26 计=27 关=28 审=29 程=30

24	1	3	2	28	29	27		11	4		5	15	23	30

解码后的信息:

提示: 每个数字对应下方密钥中的一个汉字。

检查点 10: 基础网络安全常见问题 (A 部分)

回顾有关缓解网络威胁的常见问题和解答。

Q1: 什么是网络钓鱼?

网络钓鱼是一种社会工程攻击，犯罪分子发送欺诈性消息，诱骗用户分享敏感数据。

Q2: 网络钓鱼与鱼叉式网络钓鱼有什么区别?

网络钓鱼以通用内容针对广泛人群，而鱼叉式网络钓鱼则利用定制的细节针对特定受害者。

Q3: 什么是鲸钓攻击 (whaling)?

鲸钓是一种高度定向的网络钓鱼攻击，针对拥有管理权限的高层管理人员。

Q4: 什么是电子邮件伪造?

电子邮件欺骗是指创建带有伪造发件人地址的邮件，诱骗收件人信任其来源。

Q5: SPF 如何防止伪造?

它在 DNS 中发布授权发送 IP 地址的列表，让接收服务器可以验证邮件来源。 [1]

检查点 10: 基础网络安全常见问题 (B 部分)

回顾有关缓解网络威胁的常见问题和解答。

Q6: DKIM 是什么?

DomainKeys Identified Mail 会为邮件头添加加密签名，证明某个域名承担了责任，且邮件未被篡改。

Q7: DMARC 代表什么?

基于域名的邮件认证、报告与一致性。 [2]

Q8: 什么是 DMARC 策略?

一项策略，告诉邮件服务器如何处理未通过 SPF/DKIM 的邮件（无操作、隔离或拒绝）。 [2]

Q9: 什么是语音钓鱼 (vishing)?

语音钓鱼，即攻击者通过欺诈电话套取管理或财务数据。

Q10: 链接扫描器有什么帮助?

它们会扫描并改写收到的电子邮件链接，在点击时验证目标网页的安全性。

检查点 10: 高级安全常见问题 (C 部分)

探索安全框架、恶意软件分析和数据合规的高级技术层面。

Q1: 同形异义字攻击是如何运作的?

攻击者使用外观相似的非 ASCII Unicode 字符注册域名，在视觉上模仿合法域名。

Q2: 什么是 Punycode 表示?

一种编码，将 Unicode 域名转换为以“xn--”开头的 ASCII 兼容字符串，以便 DNS 处理。

Q3: 为什么 'p=reject' 是最安全的 DMARC 状态?

它要求接收服务器在 SMTP 会话期间拒收未通过 DMARC（对齐的 SPF/DKIM）的邮件，从而阻止直接伪造。 [2]

Q4: 攻击者如何绕过 SPF 规则?

通过利用外观相似的域名（域名抢注）或使用合法第三方邮件服务上被攻陷的账户。

Q5: 什么是商业电子邮件诈骗 (BEC)?

一种企业诈骗，攻击者劫持或冒充企业电子邮件账户来授权欺诈性付款。

检查点 10: 高级安全常见问题 (D 部分)

探索安全框架、恶意软件分析和数据合规的高级技术层面。

Q6: 多因素身份验证如何阻止网络钓鱼?

它需要无法仅通过仿冒登录页面窃取的辅助令牌（如硬件密钥）。

Q7: 什么是凭据窃取落地页?

仿冒的登录门户，旨在实时捕获输入的用户名、密码和 MFA 令牌。

Q8: 什么是子域名劫持?

攻击者控制未使用的 DNS 子域名指针，在受信任的父域名下托管恶意网络钓鱼落地页。

Q9: DKIM 对齐检查如何工作?

它验证“From”标头中的域名是否与在 DKIM 标头中对邮件进行加密签名的域名一致。

Q10: 电子邮件网关的作用是什么?

过滤传入电子邮件、审计链接、对附件进行沙盒处理，并验证 SPF/DKIM/DMARC 合规性。

第 11 部分: 10 个现实中的网络安全事实与洞察

回顾有关安全漏洞、防御机制和合规标准的真实事实。

1. 安全洞察

2025 年，网络钓鱼和欺骗是向 FBI 的 IC3 举报最多的犯罪类型，共有 191,561 起投诉。 [4]

2. 安全洞察

2025 年，商业电子邮件诈骗（BEC）造成了向 FBI 的 IC3 报告的超过 $3 十亿的损失。 [4]

3. 安全洞察

同形异义攻击利用外观相似的西里尔字母，在浏览器中从视觉上复制精确匹配的品牌域名。

4. 安全洞察

使用“p=reject”时，域名会要求接收方在投递期间拒收未通过验证的邮件，而不是将其归入垃圾邮件。 [2]

5. 安全洞察

针对 CEO 的鲸钓攻击通常要求为机密并购或域名购买紧急付款。

6. 安全洞察

凭据收割门户会复制真实的登录页面，使受害者直接把密码输入到攻击者的表单中。

7. 安全洞察

CISA 的联合网络钓鱼指南建议在 DMARC、SPF、DKIM 和抗钓鱼 MFA 之外，同时开展用户培训。 [3]

8. 安全洞察

SPF 评估最多只限于 10 个需要 DNS 查询的项；超过限制会返回 'permerror' 结果。 [1]

9. 安全洞察

FIDO2 硬件安全密钥提供有加密技术支撑的保护，可抵御远程凭据窃取。

10. 安全洞察

网络钓鱼是攻击者最初入侵组织的最常见方式之一，因此定期开展安全意识培训是一种有效的防御措施。

技术参考资料与来源

本学习指南和互动谜题根据全球 NIST、OWASP 以及数据隐私合规标准编写。

学术与行业参考资料

[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

答案: 检查点 1 – 单项选择

1 问题 1 正确答案: A

教学提示

什么是鱼叉式网络钓鱼？ → 针对特定个人或组织定制的定向网络钓鱼邮件

2 问题 2 正确答案: A

教学提示

SPF 在 DNS 中发布域名的授权发送主机，以便接收方可以检查信封发件人。

3 问题 3 正确答案: A

教学提示

什么是鲸钓攻击？ → 专门针对知名企业高管的网络钓鱼活动

4 问题 4 正确答案: A

教学提示

DKIM 有什么作用？ → 为电子邮件添加加密签名以验证发件人真实性

5 问题 5 正确答案: A

教学提示

DMARC 的作用是什么？ → 指示接收方邮件服务器如何处理未通过 SPF/DKIM 检查的邮件

答案: 检查点 2 – 判断题（正确或错误）

6 **问题 6** **正确答案: 错误**

教学提示

错误: 鱼叉式网络钓鱼是针对特定人员量身定制的，不同于通用的批量网络钓鱼。

7 **问题 7** **正确答案: 正确**

教学提示

DMARC 策略可以指示邮件服务器拒收未经授权的伪造邮件。

8 **问题 8** **正确答案: 错误**

教学提示

错误: SPF 对照 DNS 检查发送 IP；验证加密签名的是 DKIM。

9 **问题 9** **正确答案: 错误**

教学提示

错误: 鲸钓针对的是高层管理人员，他们可以批准付款并访问敏感数据。

10 **问题 10** **正确答案: 正确**

教学提示

正确: 通过另一个已知的独立渠道确认付款请求，有助于阻止电汇诈骗。

词汇答案与评分标准

教师评分标准: 每个正确配对得 1 分（共 8 分），每个语境术语得 1 分（共 6 分）。

检查点 4: 答案 – 概念配对

F 1. 鱼叉式	G 2. 欺骗	D 3. SPF	H 4. DKIM
C 5. DMARC	B 6. 鲸钓攻击	E 7. 网络钓鱼	A 8. 语音钓鱼

检查点 3: 答案 – 关键术语

1 鱼叉	2 伪造	3 SPF	4 DKIM
5 DMARC	6 鲸钓攻击		

检查点 6 替代活动: 答案 – 词语配对

1 B – 邮件伪造	2 A – 邮件签名	3 H – 鲸钓攻击	4 C – 钓鱼邮件
5 G – 网络钓鱼	6 E – 鱼叉钓鱼	7 D – 语音钓鱼	8 F – 钓鱼攻击

教师讨论提示

关键术语:
检查学生能否用自己的话解释鱼叉式、欺骗和SPF，并为每个术语举例。

案例研究:
请学生用练习单中的事实而不是个人观点来支持自己的建议。

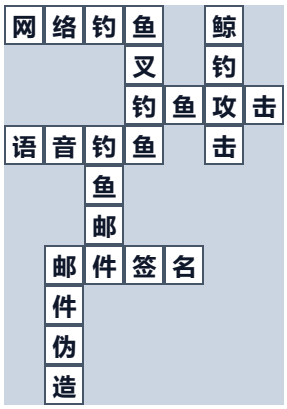
来源评估:
请学生根据练习单的参考资料至少核实一项说法，并讨论数字、价格和规则为什么可能随时间变化。

谜题答案与教师说明

找词答案

全	址	隧	安	息	邮	用	私	邮	共	鱼	输	务	墙	系
攻	协	护	软	火	全	人	服	网	安	理	协	击	私	鲸
务	鱼	器	安	份	私	访	公	身	络	信	风	户	软	域
务	钓	数	理	叉	络	护	址	道	问	钓	访	叉	险	传
录	叉	安	设	域	邮	器	名	伪	认	音	鱼	软	造	息
统	鱼	火	密	管	件	访	语	保	份	备	认	统	造	软
险	加	隧	传	公	签	用	防	音	址	数	网	数	加	击
钓	防	域	钓	议	名	造	人	协	钓	务	设	证	域	务
击	访	份	身	协	件	系	隐	证	证	鱼	件	管	传	人
攻	共	护	据	输	软	险	接	理	据	录	服	输	音	浏
鱼	邮	件	伪	造	加	叉	录	息	协	私	鲸	服	身	鲸
钓	务	设	伪	钓	系	加	道	数	网	鲸	风	服	钓	议
络	务	险	务	鱼	信	私	问	服	管	件	认	攻	用	访
理	叉	输	信	邮	设	览	户	络	络	设	击	击	身	统
人	造	件	域	件	管	人	理	码	身	语	数	息	理	伪

填字游戏答案



填字游戏答案教师指南

横向

1 横向: 网络钓鱼 社会工程类电子邮件 (4 字)

4 横向: 钓鱼攻击 利用伪装的消息或网站诱骗用户交出敏感信息的攻击 (4 字)

5 横向: 语音钓鱼 基于语音的诈骗电话 (4 字)

7 横向: 邮件签名 电子邮件中的加密签名 (4 字)

纵向

2 纵向: 鱼叉钓鱼 个性化的定向电子邮件 (4 字)

3 纵向: 鲸钓攻击 以企业高管为目标 (4 字)

6 纵向: 钓鱼邮件 冒充可信机构、诱骗收件人交出信息的欺诈邮件 (4 字)

7 纵向: 邮件伪造 伪造发件人邮箱地址 (4 字)

乱序单词与密码答案

词汇还原练习和秘密密码挑战的评分答案。

汉字重组答案

1. 签 邮 名 件 — **邮件签名**
2. 钓 邮 件 鱼 — **钓鱼邮件**
3. 鱼 鱼 钓 叉 — **鱼叉钓鱼**
4. 鱼 钓 网 络 — **网络钓鱼**
5. 造 邮 伪 件 — **邮件伪造**
6. 钓 鱼 语 音 — **语音钓鱼**
7. 攻 钓 击 鱼 — **钓鱼攻击**
8. 鲸 击 攻 钓 — **鲸钓攻击**

秘密密码挑战答案

“用邮件网关审计发现社交工程”

案例研究答案

A 案例研究 1: 高管捕鲸攻击的补救

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一位首席财务官收到一封高度个性化的电子邮件，声称来自首席执行官，要求紧急电汇 50,000 美元，以完成一笔保密的域名购买。
- 建议策略与方案: 配置 'p=reject' 策略的 DMARC 以拦截伪造的发件人域名。在网关添加外部发件人警告横幅，并要求所有财务交易都通过口头的带外方式确认。

B 案例研究 2: 部署 SPF/DKIM/DMARC 网关策略

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一家企业未能通过安全审计，因为其发出的营销邮件经常被标记为垃圾邮件，而且黑客正在积极伪造该公司的品牌域名。
- 推荐策略与解决方案: 发布包含授权发件 IP 的 SPF TXT 记录。在出站邮件服务器上配置 DKIM 签名密钥，并分析收到的 DMARC XML 反馈报告以识别滥用行为。