姓名: _____ 日期: _____ 得分: _____

身份盗用预防与资产安全指南

凭据泄露、MFA、暗网监控、信用冻结提醒、社会工程

身份盗用预防学习概览

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身份盗用的预防与缓解。你将探索凭据泄露、多因素身份验证、暗网监控、信用冻结提醒和社会工程防御。

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/identity-theft/

你的身份保护学习路线图

- 了解暗网论坛上的凭据暴露风险。
- 实施多因素身份验证（MFA）和信用冻结提醒。
- 设计企业安全防御措施，抵御有针对性的社会工程诈骗。

身份盗用指南说明

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。将所学知识应用于身份保护。 最后完成附加活动: 快速思考。

身份盗用预防与资产安全（简介）

身份盗用利用泄露的凭据和薄弱的登录方式来劫持个人和企业账户。部署 MFA、信用冻结、暗网扫描器以及 SPF/DKIM/DMARC 框架，是抵御数字冒充的关键防线。

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. 身份窃贼窃取登录凭据的主要手段是什么?

- A. 发送虚假邮件警报，诱骗用户在仿冒门户上输入密码
- B. 收听用户公司办公室附近的无线电广播
- C. 对用户的本地服务器存储盘进行碎片整理
- D. 断开外部网络备份配置

2. 哪项安全控制对凭据泄露提供最强的防御?

- A. 使用硬件密钥的多重身份验证
- B. 使用默认的浏览器格式创建长密码
- C. 每六个月更改一次电子邮件用户名
- D. 删除已存储的 Cookie 跟踪浏览器历史记录

3. 什么代表信用冻结?

- A. 锁定信用报告以防止窃贼办理未经授权的贷款
- B. 从数据库中删除银行账户交易记录
- C. 禁用扫描仪上的信用卡磁条读卡器
- D. 对本地数据库硬盘进行静态加密

4. 暗网监控为什么有用?

- A. 如果泄露的凭据出现在非法数据库中，它会提醒用户
- B. 它会阻止活动的恶意软件在虚拟沙盒中运行
- C. 它加快虚拟网络上的浏览器路由速度
- D. 它阻止后端数据库 SQL 注入访问尝试

5. 社会工程是什么意思?

- A. 操纵他人主动透露机密凭据
- B. 扫描企业服务器端口以查找可被利用的安全漏洞
- C. 将系统数据库文件备份到离线硬盘
- D. 通过三个加密的洋葱节点路由网络数据包

检查点 2: 判断正误挑战

6 问题 6

6. 身份盗用只影响线上数字账户，不影响实体邮寄信件。

○ 正确 ○ 错误

7 问题 7

7. 对所有个人账户强制启用 MFA 可阻止大多数撞库机器人攻击。

○ 正确 ○ 错误

8 问题 8

8. 信用冻结会阻止信用查询，但也会阻止你访问自己的银行账户。

○ 正确 ○ 错误

9 问题 9

9. 密码管理器会拒绝在仿冒域名上自动填写密码，从而保护用户免受网络钓鱼。

○ 正确 ○ 错误

10 问题 10

10. 网络钓鱼电子邮件常使用紧迫的措辞来引发情绪化的快速反应。

○ 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. 身份窃贼的目标是个人密码和用户 _____ 。
2. 向用户通报数据库泄露事件，能发现私人账户的 _____ 。
3. 要求输入临时验证码才能登录的做法称为 _____ 。
4. 扫描黑客论坛中被盗数据的做法属于暗网 _____ 。
5. 阻止未经授权查询信用记录需要进行信用 _____ 。
6. 培训员工提高网络钓鱼防范意识，可建立主动的安全 _____ 。

词汇词库

登录凭证　冻结　多因素验证　防御　监控　数据备份　数据泄漏　网络钓鱼

在此写下你的答案:

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

检查点 4: 安全概念配对

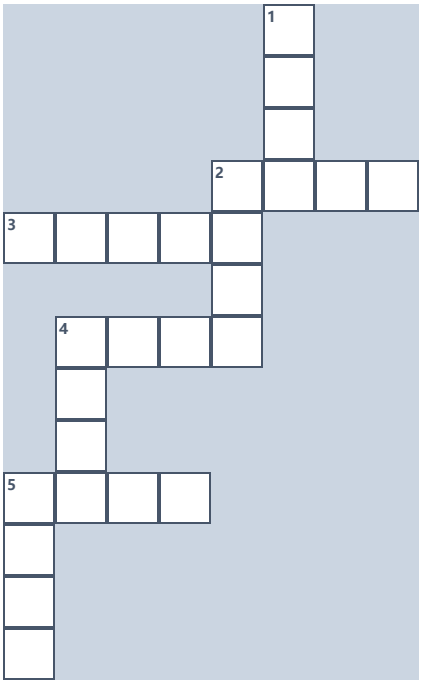
定义配对

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. 凭据	**A**	保护账户登录的辅助验证步骤（如硬件密钥）。
	2. 泄漏	**B**	创建虚假网站或电子邮件来冒充合法组织。
	3. MFA	**C**	限制对信用档案的访问，以防止欺诈性贷款申请。
	4. 监控	**D**	包含用户个人记录的私有数据库遭到未经授权的暴露。
	5. 冻结	**E**	用于防范身份盗用的培训和技术控制措施。
	6. 防御	**F**	发送欺诈性消息，诱骗用户交出凭据。
	7. 欺骗	**G**	扫描在线论坛和黑客频道，查找被盗的企业数据。
	8. 网络钓鱼	**H**	用于验证数字身份的用户名、密码和私有令牌。

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

2. 通过欺骗或入侵手段获取他人的登录信息 (4)

3. 保护账户登录的辅助验证步骤（例如硬件密钥）(5)

4. 包含个人用户记录的私有数据库遭到未经授权的暴露 (4)

5. 用于防范身份盗窃的培训和技术控制措施 (4)

纵向

1. 用于验证数字身份的用户名、密码和私有令牌 (4)

2. 用户名、密码等登录凭证被意外暴露 (4)

4. 为防止丢失而另外保存的一份数据副本 (4)

5. 确认用户确实是其所声称的那个人 (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

2 横向: 通过欺骗或入侵手段获取他人的登录信息 (4 字):

3 横向: 保护账户登录的辅助验证步骤（例如硬件密钥） (5 字):

4 横向: 包含个人用户记录的私有数据库遭到未经授权的暴露 (4 字):

5 横向: 用于防范身份盗窃的培训和技术控制措施 (4 字):

纵向

1 纵向: 用于验证数字身份的用户名、密码和私有令牌 (4 字):

2 纵向: 用户名、密码等登录凭证被意外暴露 (4 字):

4 纵向: 为防止丢失而另外保存的一份数据副本 (4 字):

5 纵向: 确认用户确实是其所声称的那个人 (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 道 安 息 泄 用 连 泄 人 因 公 务 墙 统
击 议 隐 软 墙 全 人 服 凭 安 传 协 系 私 登
务 御 器 安 份 私 问 公 份 证 信 险 户 软 名
务 防 数 传 取 络 隐 域 浏 地 窃 访 取 攻 传
录 份 安 设 名 多 器 名 御 证 窃 取 软 验 保
软 身 墙 密 理 因 问 数 保 风 管 认 软 验 件
攻 加 道 输 共 素 用 防 据 址 数 网 数 加 系
多 防 名 多 议 验 验 隧 协 备 务 备 证 域 务
证 问 份 身 议 证 件 统 隐 身 份 身 设 管 输
验 隧 人 护 加 输 件 攻 接 传 据 凭 服 公 窃
份 凭 证 泄 漏 览 加 取 凭 保 协 私 登 服 登
身 身 务 备 数 御 统 加 道 数 网 登 风 录 服
议 络 务 攻 据 务 信 私 问 服 管 设 凭 证 用
问 传 取 公 泄 信 备 记 户 络 络 证 备 击 份
统 隧 验 件 漏 名 理 隧 传 码 份 素 数 保 传

词汇列表

凭证泄漏 **数据泄漏** **数据备份** **身份防御** **身份验证** **多因素验证** **凭证窃取** **登录凭证**

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. 凭证泄漏
B. 数据泄漏
C. 数据备份
D. 身份防御
E. 身份验证
F. 多因素验证
G. 凭证窃取
H. 登录凭证

定义与配对字段
1. 用于验证数字身份的用户名、密码和私有令牌。
2. 用户名、密码等登录凭证被意外暴露。
3. 通过欺骗或入侵手段获取他人的登录信息。
4. 保护账户登录的辅助验证步骤（例如硬件密钥）。
5. 用于防范身份盗窃的培训和技术控制措施。
6. 确认用户确实是其所声称的那个人。
7. 包含个人用户记录的私有数据库遭到未经授权的暴露。
8. 为防止丢失而另外保存的一份数据副本。

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. 泄凭漏证 _____

2. 数备份据 _____

3. 证身验份 _____

4. 取窃凭证 _____

5. 漏数泄据 _____

6. 防御身份 _____

7. 验证多素因 _____

8. 登证凭录 _____

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	身份被盗后要做的事			
2	不应在社交媒体上分享的内容			
3	你要备份的内容			
4	钱包里的卡片或证件			
5	你应该保护的文件			
6	数据泄露后要做的事			
7	更新软件的原因			
8	身份窃贼想要的信息			
9	可能被黑客入侵的设备			
10	你的数据可能泄露的来源			
11	你今天就可以开始的安全习惯			
12	电脑被感染的迹象			
13	证明身份的方法			
14	身份被盗的迹象			
15	电子邮件中的警示信号			

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: 防范冒充高管身份



情景: 一位高调的高管遭到抢注拼写错误域名的攻击，这些域名模仿其个人邮箱来欺骗客户。请设计一个品牌保护方案。

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: 企业凭据在暗网中的暴露



情景: 一份暗网数据库泄露文件中包含属于某企业系统管理员的数百条公司凭据。请设计一个缓解策略。

讨论问题: 概述凭据清理流程，并规划密码管理器的推广。

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

安=1 泄=2 素=3 护=4 份=5 漏=6 保=7 据=8 因=9 验=10

登=11 防=12 证=13 窃=14 备=15 网=16 身=17 全=18 密=19 录=20

多=21 御=22 凭=23 加=24 码=25 取=26 数=27 络=28 字=29 用=30

30	21	9	3	10	13	7	4	27	29	17	5

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: 什么是身份盗窃?

一种犯罪行为，攻击者窃取个人记录（如密码或社会保障号）来冒充他人以牟取经济利益。

Q2: 身份盗窃最常见的原因是什么?

网络钓鱼是窃贼获取密码的主要方式之一，会引诱用户访问虚假的仿冒网站。

Q3: 多因素身份验证 (MFA) 如何保护身份?

MFA 要求在登录时提供第二重验证（如硬件密钥），即使攻击者窃取了你的密码也无法登录。

Q4: 什么是信用冻结?

一项免费服务，阻止信用机构共享你的信用档案，防止窃贼以你的名义申请新贷款。 [2]

Q5: 什么是暗网监控?

检查黑客论坛中泄露的邮箱、密码和个人记录，并在你的数据暴露时发出警报的软件。

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: 撞库攻击是什么意思?

自动化机器人在数百个网站上测试泄露的密码列表，以接管活跃账户。

Q7: 电子邮件伪造为什么危险?

它允许攻击者伪造电子邮件中的发件人姓名，使网络钓鱼邮件看起来像是来自可信的同事。

Q8: 密码管理器如何防止身份盗窃?

它们为每个账户存储复杂且唯一的密码，并拒绝在虚假的网络钓鱼域名上自动填充凭据。

Q9: 什么是鱼叉式网络钓鱼?

一种高度定向的网络钓鱼攻击，根据受害者的姓名和详细信息定制，以增加得逞的几率。

Q10: 信用提醒与冻结有何不同?

提醒会告诉贷款机构在开立账户前核实你的身份，而冻结则会完全阻止访问你的信用档案。 [2]

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: SIM 卡交换如何导致身份盗窃?

攻击者说服运营商员工将受害者的电话号码转移到新的 SIM 卡上，从而劫持基于短信的双重身份验证（2FA）验证码。

Q2: DMARC 在防止身份盗窃中起什么作用?

DMARC 允许域名所有者阻止伪造邮件到达收件箱，防止虚假邮件冒充企业域名。

Q3: 为什么合成身份盗窃难以发现?

窃贼将真实的 SSN 与虚假姓名和出生日期组合，构建全新的信用档案，从而绕过基本的欺诈警报。

Q4: 数据经纪商如何利用个人身份信息?

数据经纪商收集公开记录、网络行为和购买历史来编制个人档案，这些档案可能被泄露或出售。

Q5: 基于短信的 MFA 为什么被认为存在漏洞?

短信流量容易遭到拦截、网络钓鱼以及运营商层面的 SIM 卡交换攻击。

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: 什么是信用档案锁定?

一种类似冻结的商业服务，允许用户通过手机应用即时解锁或锁定其信用档案。

Q7: 企业数据泄露如何助长身份盗窃?

泄露的数据库会暴露数百万条明文凭据，给窃贼提供了实施有针对性身份欺诈所需的原始数据。

Q8: 在社交媒体上过度分享有什么风险?

公开分享宠物名字、出生地和母亲的婚前姓氏，会让窃贼得到常见账户恢复问题的答案。

Q9: 生物识别登录如何保护身份档案?

生物识别将登录与指纹或面部等特征绑定；如果保存在设备本地则很难被窃取，但存储的生物识别数据可能会泄露。

Q10: 《危险信号规则》如何打击身份盗窃?

一项联邦法规，要求金融机构制定书面计划，以发现并应对身份盗用的预警信号。

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

由 FTC 运营的 IdentityTheft.gov 让美国受害者可以举报身份盗用并获得个人恢复计划。 [1]

2. 安全洞察

硬件安全密钥属于抗网络钓鱼的 MFA，是 CISA 所倡导的最强类型的 MFA。 [4]

3. 安全洞察

被泄露的密码是数据泄露事件中常见的入口，会助长后续的身份欺诈。

4. 安全洞察

根据联邦法律，信用冻结是免费的，在解冻之前可阻止贷款机构查看信用档案。 [2]

5. 安全洞察

DMARC 让域名所有者可以告知邮件服务器，拒绝或隔离未通过检查的伪造邮件。 [7]

6. 安全洞察

SIM 卡交换（SIM swapping）使黑客能够绕过银行门户上基于短信的双因素身份验证。

7. 安全洞察

合成身份欺诈混合了真实和虚假的信息，使贷款机构难以察觉。

8. 安全洞察

许多人在多个在线账户中重复使用同一个密码，因此一次泄露就可能暴露其中的多个账户。

9. 安全洞察

数据经纪商会汇编大量消费者的详细档案，造成集中的隐私风险。

10. 安全洞察

从身份盗用中恢复可能需要数月的工作，例如争议扣款和修正信用报告。

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] 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

答案: 检查点 1 – 单项选择

1 问题 1

正确答案: A

教学提示

身份窃贼窃取登录凭据的主要手段是什么？ → 发送虚假邮件警报，诱骗用户在仿冒门户上输入密码

2 问题 2

正确答案: A

教学提示

哪项安全控制对凭据泄露提供最强的防御？ → 使用硬件密钥的多重身份验证

3 问题 3

正确答案: A

教学提示

什么代表信用冻结？ → 锁定信用报告以防止窃贼办理未经授权的贷款

4 问题 4

正确答案: A

教学提示

暗网监控为什么有用？ → 如果泄露的凭据出现在非法数据库中，它会提醒用户

5 问题 5

正确答案: A

教学提示

社会工程是什么意思？ → 操纵他人主动透露机密凭据

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

身份盗窃也可能从线下开始，例如被盗的邮件或文件。

7 **问题 7** 正确答案: 正确

教学提示

对所有个人账户强制启用 MFA 可阻止大多数撞库机器人攻击。

8 **问题 8** 正确答案: 错误

教学提示

信用冻结会阻止新的信用查询，但不影响你现有的账户。

9 **问题 9** 正确答案: 正确

教学提示

密码管理器会拒绝在仿冒域名上自动填写密码，从而保护用户免受网络钓鱼。

10 **问题 10** 正确答案: 正确

教学提示

网络钓鱼电子邮件常使用紧迫的措辞来引发情绪化的快速反应。

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

H 1. 凭据	D 2. 泄漏	A 3. MFA	G 4. 监控
C 5. 冻结	E 6. 防御	B 7. 欺骗	F 8. 网络钓鱼

检查点 3: 答案 – 关键术语

1 登录凭证	2 数据泄漏	3 多因素验证	4 监控
5 冻结	6 防御		

检查点 6 替代活动: 答案 – 词语配对

1 H – 登录凭证	2 A – 凭证泄漏	3 G – 凭证窃取	4 F – 多因素验证
5 D – 身份防御	6 E – 身份验证	7 B – 数据泄漏	8 C – 数据备份

教师讨论提示

关键术语:
检查学生能否用自己的话解释凭据、泄漏和MFA，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。

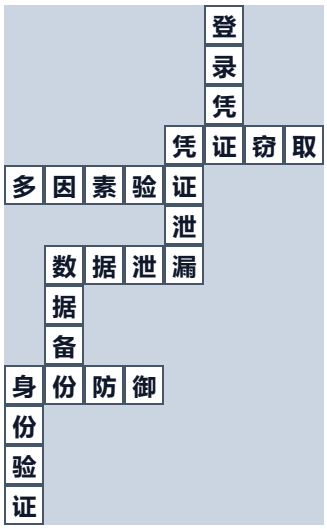
来源评估:
请学生根据练习单的参考资料至少核实一项说法，并讨论数字、价格和规则为什么可能随时间变化。

谜题答案与教师说明

找词答案

全	址	道	安	息	泄	用	连	泄	人	因	公	务	墙	统
击	议	隐	软	墙	全	人	服	凭	安	传	协	系	私	登
务	御	器	安	份	私	问	公	份	证	信	险	户	软	名
务	防	数	传	取	络	隐	域	浏	地	窃	访	取	攻	传
录	份	安	设	名	多	器	名	御	证	窃	取	软	验	保
软	身	墙	密	理	因	问	数	保	风	管	认	软	验	件
攻	加	道	输	共	素	用	防	据	址	数	网	数	加	系
多	防	名	多	议	验	验	隧	协	备	务	备	证	域	务
证	问	份	身	议	证	件	统	隐	身	份	身	设	管	输
验	隧	人	护	加	输	件	攻	接	传	据	凭	服	公	窃
份	凭	证	泄	漏	览	加	取	凭	保	协	私	登	服	登
身	身	务	备	数	御	统	加	道	数	网	登	风	录	服
议	络	务	攻	据	务	信	私	问	服	管	设	凭	证	用
问	传	取	公	泄	信	备	记	户	络	络	证	备	击	份
统	隧	验	件	漏	名	理	隧	传	码	份	素	数	保	传

填字游戏答案



填字游戏答案教师指南

横向

2 横向: 凭证窃取 通过欺骗或入侵手段获取他人的登录信息 (4 字)

3 横向: 多因素验证 保护账户登录的辅助验证步骤（例如硬件密钥） (5 字)

4 横向: 数据泄漏 包含个人用户记录的私有数据库遭到未经授权的暴露 (4 字)

5 横向: 身份防御 用于防范身份盗窃的培训和技术控制措施 (4 字)

纵向

1 纵向: 登录凭证 用于验证数字身份的用户名、密码和私有令牌 (4 字)

2 纵向: 凭证泄漏 用户名、密码等登录凭证被意外暴露 (4 字)

4 纵向: 数据备份 为防止丢失而另外保存的一份数据副本 (4 字)

5 纵向: 身份验证 确认用户确实是其所声称的那个人 (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. 泄凭漏证 → **凭证泄漏**
2. 数备份据 → **数据备份**
3. 证身验份 → **身份验证**
4. 取窃凭证 → **凭证窃取**
5. 漏数泄据 → **数据泄漏**
6. 防御身份 → **身份防御**
7. 验证多素因 → **多因素验证**
8. 登证凭录 → **登录凭证**

秘密密码挑战答案

“用多因素验证保护数字身份”

案例研究答案

A 案例研究 1: 防范冒充高管身份

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一位高知名度的高层管理人员成为模仿其个人邮箱的拼写抢注域名的目标，这些域名被用来欺骗客户。请设计品牌保护计划。
- 推荐策略与解决方案: 注册该高管姓名的所有常见拼写变体。部署电子邮件身份验证协议（DMARC、DKIM、SPF）以防止域名欺骗。对所有高层管理人员的企业登录实施硬件 MFA。

B 案例研究 2: 企业凭据在暗网中的暴露

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一份暗网数据库转储中包含某企业系统管理员的数百条企业凭据。请设计缓解策略。
- 建议策略与方案: 进行全公司范围的密码重置。强制使用企业密码管理器。在所有系统门户上强制启用 MFA，并设置持续的自动化暗网监控警报。