姓名: _____ 日期: _____ 得分: _____

网络诈骗与社会工程防护指南

电子邮件网络钓鱼、域名欺骗、语音钓鱼、客服诈骗、带外验证、BEC

网络诈骗学习概览

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诈骗防御。你将探索虚假钓鱼网站、社会工程策略、技术支持诈骗、电汇欺诈途径和付款验证方法。

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/online-scams/

你的网络诈骗防护学习路线图

- 识别技术支持诈骗和仿冒域名（typosquatting）的常见迹象。
- 实施电子邮件验证协议（SPF、DKIM、DMARC）以防范伪造。
- 建立带外交易验证，以防止商业电汇诈骗。

网络诈骗指南说明

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。将所学知识应用于在线诈骗防护。最后完成附加活动: 快速思考。

网络诈骗与社会工程防护（简介）

网络诈骗利用网络钓鱼、技术支持弹窗、语音钓鱼和电汇欺诈等手段利用人的行为。强制执行带外交易验证以及 SPF/DKIM/DMARC 域名规则，有助于在网关处阻止社会工程攻击途径。

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. 技术支持诈骗的主要迹象是什么?
   - A. 声称你的系统已被感染并要求你拨打电话号码的弹出窗口
   - B. 从官方注册中心下载的自动安全更新
   - C. 密码管理器拒绝在企业域名上填充凭据
   - D. 在外部驱动器配置上运行的后台文件备份

2. 哪种手法利用伪造的发件人域名窃取银行信息?
   - A. 电子邮件网络钓鱼
   - B. 端口扫描
   - C. 内存注入
   - D. 加密销毁

3. 什么代表电汇诈骗?
   - A. 利用社会工程诱骗受害者向虚假公司账户汇款
   - B. 使用勒索软件载荷加密系统数据库
   - C. 通过 SQL 注入命令查询数据库
   - D. 将系统文件备份到离线存储磁盘

4. 诈骗者为什么创建虚假购物网站?
   - A. 窃取买方的信用卡信息和支付凭据
   - B. 托管沙盒恶意软件分析数据库表
   - C. 加快网购订单的送达速度
   - D. 免费测试新的网站设计

5. 语音钓鱼是什么意思?
   - A. 通过电话网络窃取凭据的语音网络钓鱼诈骗
   - B. 扫描本地网络中不安全的系统设备
   - C. 未经授权的入侵后恢复系统数据库
   - D. 在安全的虚拟容器内运行不受信任的代码

检查点 2: 判断正误挑战

6 问题 6

6. 网络钓鱼骗局只针对终端用户，从不针对高管鲸钓目标。

○ 正确 ○ 错误

7 问题 7

7. 伪造的域名常常使用细微的拼写错误（如 amaz0n.com）来模仿可信品牌。

○ 正确 ○ 错误

8 问题 8

8. 通过向来电者授予远程访问权限可以解决技术支持诈骗。

○ 正确 ○ 错误

9 问题 9

9. 社会工程学利用恐惧和紧迫感等人类心理来绕过安全规则。

○ 正确 ○ 错误

10 问题 10

10. 电汇请求应始终通过带外通信渠道进行核实。

○ 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. 欺骗用户的诈骗电子邮件称为 _____ 。
2. 模仿可信品牌的网址属于 _____ 。
3. 通过电话套取银行信息的骗局称为 _____ 。
4. 要求付费清除病毒的弹窗属于技术支持 _____ 。
5. 确认付款请求需要带外 _____ 。
6. 把企业交易转到窃贼账户的行为是 _____ 。

词汇词库

电汇诈骗　仿冒网址　鲸钓攻击　勒索软件　身份验证　网络钓鱼　语音诈骗　诈骗

在此写下你的答案:

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

检查点 4: 安全概念配对

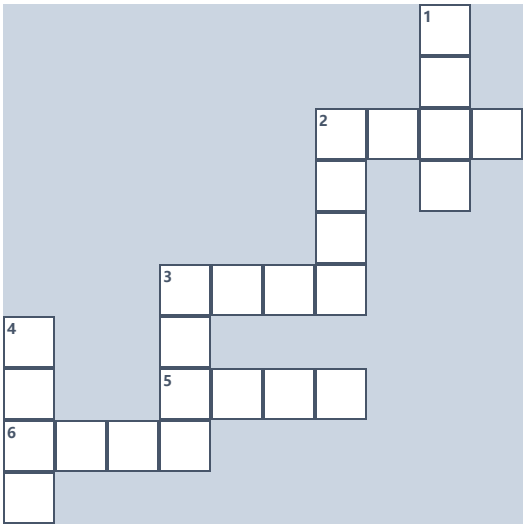
定义配对

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. 网络钓鱼	**A**	将银行交易欺诈性地转移到犯罪分子账户。
	2. 伪造的	**B**	旨在从受害者处骗取钱财或访问凭据的欺诈手段。
	3. 语音钓鱼	**C**	发送诈骗短信，窃取移动账户凭据。
	4. 诈骗	**D**	旨在窃取凭据和账户信息的欺诈性语音电话。
	5. 验证	**E**	旨在窃取 C 级高管凭据的定向网络钓鱼攻击。
	6. 电汇诈骗	**F**	伪造的、看起来合法的电子邮件发件人或网站地址。（B）
	7. 鲸钓攻击	**G**	旨在窃取登录凭据和密码的欺诈性电子邮件活动。
	8. 短信钓鱼	**H**	通过可信的第二联系方式确认付款详情。

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. 将银行交易欺诈性地转向犯罪分子账户 (4)

3. 发送诈骗短信以窃取移动账户凭证 (4)

5. 冒充可信机构、诱骗收件人交出信息的欺诈邮件 (4)

6. 旨在窃取登录凭证和密码的欺诈性电子邮件活动 (4)

纵向

1. 旨在窃取凭证和账户信息的欺诈性语音电话 (4)

2. 骗子通过打电话骗取钱财或账户信息 (4)

3. 通过诈骗短信诱导用户点击链接或泄露信息 (4)

4. 模仿发件人邮箱或网站地址，使其看起来合法 (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: 将银行交易欺诈性地转向犯罪分子账户 (4 字):

3 横向: 发送诈骗短信以窃取移动账户凭证 (4 字):

5 横向: 冒充可信机构、诱骗收件人交出信息的欺诈邮件 (4 字):

6 横向: 旨在窃取登录凭证和密码的欺诈性电子邮件活动 (4 字):

纵向

1 纵向: 旨在窃取凭证和账户信息的欺诈性语音电话 (4 字):

2 纵向: 骗子通过打电话骗取钱财或账户信息 (4 字):

3 纵向: 通过诈骗短信诱导用户点击链接或泄露信息 (4 字):

4 纵向: 模仿发件人邮箱或网站地址，使其看起来合法 (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 域 浏 安 息 骗 用 连 钓 隧 汇 共 器 认 软
系 防 隐 设 认 全 道 务 语 安 输 议 统 连 冒
务 鱼 用 安 风 连 问 人 风 音 信 攻 信 设 协
务 钓 数 输 仿 络 隐 域 记 地 诈 问 仿 击 公
诈 络 安 管 名 短 器 协 邮 身 音 骗 件 电 保
件 网 认 密 传 信 问 电 护 险 理 证 件 邮 设
击 密 浏 共 人 诈 户 火 话 域 据 网 数 加 统
话 火 协 话 防 骗 电 道 议 诈 务 管 身 名 务
骗 问 风 份 防 备 软 私 份 份 骗 备 传 公 浏
诈 隧 隐 加 共 设 击 访 输 据 诈 务 人 音 记
汇 短 信 钓 鱼 加 仿 诈 保 议 连 冒 服 份 仿
电 器 管 邮 钓 软 加 览 数 网 冒 攻 务 冒 防
络 器 击 器 鱼 信 私 地 服 传 备 身 网 用 问
输 仿 共 息 邮 管 短 信 络 络 管 址 统 风 软
道 电 备 协 件 传 浏 公 码 风 语 数 保 输 邮

词汇列表

短信诈骗 **短信钓鱼** **钓鱼邮件** **电话诈骗** **网络钓鱼** **电汇诈骗** **语音诈骗** **仿冒网址**

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. 短信诈骗
B. 短信钓鱼
C. 钓鱼邮件
D. 电话诈骗
E. 网络钓鱼
F. 电汇诈骗
G. 语音诈骗
H. 仿冒网址

定义与配对字段
1. 通过诈骗短信诱导用户点击链接或泄露信息。
2. 旨在窃取登录凭证和密码的欺诈性电子邮件活动。
3. 将银行交易欺诈性地转向犯罪分子账户。
4. 模仿发件人邮箱或网站地址，使其看起来合法。
5. 旨在窃取凭证和账户信息的欺诈性语音电话。
6. 冒充可信机构、诱骗收件人交出信息的欺诈邮件。
7. 发送诈骗短信以窃取移动账户凭证。
8. 骗子通过打电话骗取钱财或账户信息。

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. 诈 短 骗 信
2. 钓 邮 件 鱼
3. 鱼 网 钓 络
4. 骗 诈 语 音
5. 鱼 短 钓 信
6. 诈 骗 电 话
7. 诈 电 骗 汇
8. 仿 址 网 冒

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	骗子常用的话术			
3	骗子要求的付款方式			
4	网络诈骗的类型			
5	好得令人难以置信的优惠			
6	举报诈骗的地方			
7	与网络安全相关的词语			
8	可以提醒其注意诈骗的人			
9	你要备份的内容			
10	电子邮件中的警示信号			
11	电脑被感染的迹象			
12	核实网店的方法			
13	保护账户的方法			
14	遭遇诈骗后要做的事			
15	数据泄露后要做的事			

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: 预防企业电汇诈骗



情景: 财务部门收到一封来自伪造供应商地址的紧急邮件，要求将未来的发票电汇款项汇到新的银行路由号码。

讨论问题: 概述电汇欺诈核实政策，并指明电子邮件身份验证的拦截措施。

案例研究 2: 高管捕鲸式网络钓鱼事件



情景: 一名高管点击了一个声称含有安全董事会会议文件的钓鱼链接，并在伪造的门户上输入了主要的公司凭据。

讨论问题: 详细说明事件响应步骤，并解释如何审计高管的登录记录。

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

扫=1 诈=2 信=3 全=4 钓=5 安=6 冒=7 外=8 骗=9 络=10

电=11 鱼=12 验=13 描=14 证=15 语=16 邮=17 汇=18 联=19 音=20

件=21 址=22 网=23 用=24 短=25 话=26 现=27 数=28 发=29 仿=30

24	1	14	13	15		29	27		5	12	8	19

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: 什么是网络诈骗?

一种利用数字渠道诱骗受害者汇款或交出个人凭据的欺诈手段。

Q2: 电子邮件网络钓鱼的主要迹象是什么?

声称情况紧急（如账户被停用）并引导你点击与官方域名不符的链接的消息。

Q3: 什么是域名拼写劫持 (typosquatting)?

注册带有知名品牌常见拼写错误的域名（如 amaz0n.com），用于托管虚假钓鱼网站。

Q4: 什么是技术支持诈骗?

弹出窗口声称你的电脑已被感染，引导你拨打电话并为虚假的清理软件或远程访问服务付费。 [1]

Q5: 什么是语音钓鱼 (vishing)?

通过语音电话诱骗受害者提供银行账户或登录信息的网络钓鱼攻击。

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: 电信欺诈是什么意思?

通过冒充供应商或高管，将付款交易重定向到诈骗账户。

Q7: 什么是鲸钓攻击 (whaling)?

一种高度定向的鱼叉式网络钓鱼，直接针对公司高管等高价值目标。

Q8: 什么是短信钓鱼 (smishing)?

发送到移动设备的诈骗短信，包含指向虚假门户或物流更新的链接提示。

Q9: 带外验证为什么至关重要?

它通过单独的通信渠道（如电话）确认交易详情，避免使用已被入侵的电子邮件线程。

Q10: 虚假第三方托管账户骗局是如何运作的?

骗子创建一个仿冒的第三方托管网站，声称资金被安全持有，然后窃取买方汇入的款项。

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: 骗子如何利用 BEC（商业电子邮件入侵）实施电汇欺诈?

他们劫持合法员工的电子邮箱账户，监视发票往来邮件，并发送带有诈骗银行账户的更新后账单信息。

Q2: 在网络诈骗中，IDN 同形异义字攻击有什么风险?

使用外观与普通字母相同的非 ASCII 字符（例如西里尔字母 'a'）来注册模仿真实品牌的伪造域名。

Q3: 邮件头检查在诈骗识别中为什么重要?

它会显示实际的源服务器 IP 以及 SPF/DKIM 验证状态，从而表明发件人域名是否被伪造。

Q4: 技术支持诈骗者如何利用远程桌面软件?

他们使用 AnyDesk 或 TeamViewer 等工具连接到受害者的设备，植入恶意软件，并窃取已保存的密码。

Q5: 预付费用诈骗的目的是什么?

骗受害者预先支付手续费，以换取根本不存在的巨额财务回报。

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: 诈骗者如何利用社交媒体画像进行定向网络钓鱼?

他们收集企业组织架构和员工姓名，起草令人信服的鱼叉式网络钓鱼邮件。

Q7: 虚假网店为什么提供大幅折扣?

诱骗买家输入信用卡信息，窃取凭据以便重复使用，或在盗卡论坛上转售。

Q8: DMARC 记录如何拦截网络钓鱼诈骗?

DMARC 允许域名所有者要求接收方隔离或拒收未通过对齐的 SPF 和 DKIM 检查的邮件，从而阻止直接伪造。 [5]

Q9: 凭据窃取门户有什么威胁?

伪造的登录页面被设计得与 Microsoft 365 或 Google 工作区一模一样，会在输入时窃取登录凭据。

Q10: 安全团队如何举报并停用诈骗域名?

通过向注册商的滥用举报邮箱、托管服务商和 Google Safe Browsing 注册库提交欺诈证据。

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。 [2]

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。 [2]

3. 安全洞察

域名抢注（typosquatting）域名与真实品牌名称只差一两个字符，所以匆匆一瞥很容易漏看。

4. 安全洞察

2025 年，向 FBI 的 IC3 报告的技术支持诈骗损失超过 $2.1 billion。 [2]

5. 安全洞察

除非浏览器显示 punycode 形式，否则同形异义攻击在浏览器地址栏中看起来与正常域名完全一样。

6. 安全洞察

短信诈骗（smishing）使用带链接的简短紧急信息，让受害者几乎没有上下文来识别欺诈。

7. 安全洞察

鲸钓攻击以高管邮箱为目标，因为他们掌控大额电汇付款的权限。

8. 安全洞察

通过拨打已知的、已保存的电话号码来核实付款变更，是防范 BEC 电汇欺诈的关键手段。

9. 安全洞察

虚假的第三方托管网站是在线交易平台上常见的骗局: 它们看起来像安全的支付服务，实则窃取买家的电汇款项。

10. 安全洞察

在用户打开被 Google Safe Browsing 标记为网络钓鱼或恶意软件的网站之前，它会向用户发出警告。

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.). 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

答案: 检查点 1 – 单项选择

1 问题 1 正确答案: A

教学提示

技术支持诈骗的主要迹象是什么？ → 声称你的系统已被感染并要求你拨打电话号码的弹出窗口

2 问题 2 正确答案: A

教学提示

哪种手法利用伪造的发件人域名窃取银行信息？ → 电子邮件网络钓鱼

3 问题 3 正确答案: A

教学提示

什么代表电汇诈骗？ → 利用社会工程诱骗受害者向虚假公司账户汇款

4 问题 4 正确答案: A

教学提示

诈骗者为什么创建虚假购物网站？ → 窃取买方的信用卡信息和支付凭据

5 问题 5 正确答案: A

教学提示

语音钓鱼是什么意思？ → 通过电话网络窃取凭据的语音网络钓鱼诈骗

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: 网络钓鱼也针对高管；鲸钓是针对高层领导的网络钓鱼。

7 问题 7

正确答案: 正确

教学提示

伪造的域名常常使用细微的拼写错误（如 amaz0n.com）来模仿可信品牌。

8 问题 8

正确答案: 错误

教学提示

错误: 向技术支持骗子提供远程访问权限，会让他们植入恶意软件并窃取数据。

9 问题 9

正确答案: 正确

教学提示

社会工程学利用恐惧和紧迫感等人类心理来绕过安全规则。

10 问题 10

正确答案: 正确

教学提示

电汇请求应始终通过带外通信渠道进行核实。

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

G 1. 网络钓鱼	F 2. 伪造的	D 3. 语音钓鱼	B 4. 诈骗
H 5. 验证	A 6. 电汇诈骗	E 7. 鲸钓攻击	C 8. 短信钓鱼

检查点 3: 答案 – 关键术语

1 网络钓鱼	2 仿冒网址	3 语音诈骗	4 诈骗
5 身份验证	6 电汇诈骗		

检查点 6 替代活动: 答案 – 词语配对

1 B – 短信钓鱼	2 E – 网络钓鱼	3 F – 电汇诈骗	4 H – 仿冒网址
5 G – 语音诈骗	6 C – 钓鱼邮件	7 A – 短信诈骗	8 D – 电话诈骗

教师讨论提示

关键术语:
检查学生能否用自己的话解释网络钓鱼、伪造的和语音钓鱼，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。

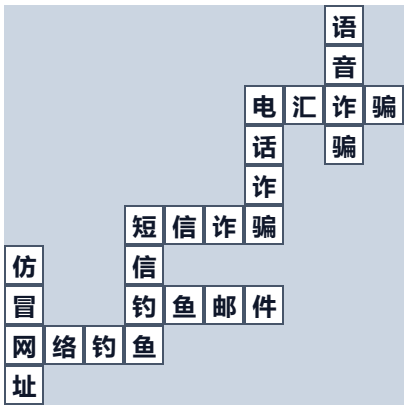
来源评估:
请学生根据练习单的参考资料至少核实一项说法，并讨论数字、价格和规则为什么可能随时间变化。

谜题答案与教师说明

找词答案

全	域	浏	安	息	骗	用	连	钓	隧	汇	共	器	认	软
系	防	隐	设	认	全	道	务	语	安	输	议	统	连	冒
务	鱼	用	安	风	连	问	人	风	音	信	攻	信	设	协
务	钓	数	输	仿	络	隐	域	记	地	诈	问	仿	击	公
诈	络	安	管	名	短	器	协	邮	身	音	骗	件	电	保
件	网	认	密	传	信	问	电	护	险	理	证	件	邮	设
击	密	浏	共	人	诈	户	火	话	域	据	网	数	加	统
话	火	协	话	防	骗	电	道	议	诈	务	管	身	名	务
骗	问	风	份	防	备	软	私	份	份	骗	备	传	公	浏
诈	隧	隐	加	共	设	击	访	输	据	诈	务	人	音	记
汇	短	信	钓	鱼	加	仿	诈	保	议	连	冒	服	份	仿
电	器	管	邮	钓	软	加	览	数	网	冒	攻	务	冒	防
络	器	击	器	鱼	信	私	地	服	传	备	身	网	用	问
输	仿	共	息	邮	管	短	信	络	络	管	址	统	风	软
道	电	备	协	件	传	浏	公	码	风	语	数	保	输	邮

填字游戏答案



填字游戏答案教师指南

横向

2 横向: 电汇诈骗 将银行交易欺诈性地转向犯罪分子账户 (4 字)

3 横向: 短信诈骗 发送诈骗短信以窃取移动账户凭证 (4 字)

5 横向: 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)

6 横向: 网络钓鱼 旨在窃取登录凭证和密码的欺诈性电子邮件活动 (4 字)

纵向

1 纵向: 语音诈骗 旨在窃取凭证和账户信息的欺诈性语音电话 (4 字)

2 纵向: 电话诈骗 骗子通过打电话骗取钱财或账户信息 (4 字)

3 纵向: 短信钓鱼 通过诈骗短信诱导用户点击链接或泄露信息 (4 字)

4 纵向: 仿冒网址 模仿发件人邮箱或网站地址，使其看起来合法 (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. 诈短骗信 — **短信诈骗**
2. 钓邮件鱼 — **钓鱼邮件**
3. 鱼网钓络 — **网络钓鱼**
4. 骗诈语音 — **语音诈骗**
5. 鱼短钓信 — **短信钓鱼**
6. 诈骗电话 — **电话诈骗**
7. 诈电骗汇 — **电汇诈骗**
8. 仿址网冒 — **仿冒网址**

秘密密码挑战答案

“用扫描验证发现钓鱼外联”

案例研究答案

A 案例研究 1: 预防企业电汇诈骗

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 财务部门收到一封来自仿冒供应商地址的紧急电子邮件，要求将今后的发票汇款发送到一个新的路由号码。
- 推荐策略与解决方案: 对所有付款实行双重授权政策。使用预先保存的电话号码进行带外验证，并在网关处拦截仿冒域名的电子邮件。

B 案例研究 2: 高管捕鲸式网络钓鱼事件

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一名高管点击了声称含有安全董事会会议文件的网络钓鱼链接，并在伪造的门户上输入了自己的主要企业凭据。
- 推荐策略与解决方案: 隔离该高管的设备。重置所有企业会话令牌和凭据。检查访问日志中的数据外泄情况，并在所有登录上实施硬件 MFA。