姓名: _____ 日期: _____ 得分: _____

公共 Wi-Fi 安全与加密

中间人攻击、恶意接入点、数据包嗅探、VPN 隧道和 HTTPS 加密。

公共 Wi-Fi 安全学习概览

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公共 Wi-Fi 安全。你将探索未加密网络、中间人（MitM）攻击、恶意接入点、数据包嗅探、VPN 隧道和 HTTPS 传输安全。

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/public-wifi-security/

你的公共 Wi-Fi 安全学习路线图

- 识别常见的公共 Wi-Fi 风险，包括数据包嗅探和恶意接入点。
- 部署 VPN 加密隧道以保护传输中的数据。
- 为远程办公人员强制使用 HTTPS 和安全的网络浏览器设置。

公共 Wi-Fi 安全指南说明

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。将所学知识应用于远程访问安全。最后完成附加活动: 快速思考。

公共 Wi-Fi 安全与传输保护（简介）

未加密的公共 Wi-Fi 热点会使网络流量暴露于数据包嗅探和恶意双子星（Evil Twin）欺骗之下。强制流量通过安全的 VPN 加密隧道，并执行仅限 HTTPS 的 HSTS 规则，可以保护会话免遭本地网络拦截。

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. 什么是中间人（MitM）攻击?
   - A. 拦截并篡改共享网络上两方之间的通信
   - B. 针对用户记录的数据库提取技术
   - C. 用大量网络流量请求压垮网络服务器
   - D. 擦除本地硬盘存储卷

2. 什么是流氓接入点（邪恶双胞胎）?
   - A. 与合法网络使用相同 SSID 的恶意 Wi-Fi 热点
   - B. 用于监控数据库备份的管理工具
   - C. 安全的 VPN 网关配置
   - D. 映射授权邮件服务器的 DNS 记录

3. VPN 如何保护公共 Wi-Fi 流量?
   - A. 它将所有网络数据包封装在加密隧道中，使嗅探器无法读取
   - B. 它会自动阻止所有传入的连接请求
   - C. 它更改物理网卡的 MAC 地址
   - D. 它删除网络浏览器中缓存的 Cookie

4. 什么是数据包嗅探?
   - A. 使用硬件或软件工具捕获并记录网络数据包
   - B. 扫描本地目录中的重复文件
   - C. 根据用户角色限制数据库读取权限
   - D. 使用 AES-256 密钥加密存储驱动器

5. HTTPS 的作用是什么?
   - A. 加密浏览器与网站服务器之间的会话流量
   - B. 在网关处过滤传入的电子邮件
   - C. 压缩图片以加快页面加载
   - D. 管理网络附加存储中的文件结构

检查点 2: 判断正误挑战

6 问题 6

6. 已连接的用户可以轻易在开放的公共 Wi-Fi 网络上捕获明文数据。

○ 正确 ○ 错误

7 问题 7

7. 流氓接入点（Evil Twin，邪恶双胞胎）始终由网络管理员授权。

○ 正确 ○ 错误

8 问题 8

8. VPN 无法有效保护公共网络上的流量免受数据包嗅探。

○ 正确 ○ 错误

9 问题 9

9. HTTPS 仅加密 URL 路径，数据包有效载荷仍为明文。

○ 正确 ○ 错误

10 问题 10

10. 使用 WPA3 安全的 Wi-Fi 热点比开放的、无密码的网络提供更强的保护。

○ 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. 在公共无线网络上窃取私人密码属于通信 _____ 。
2. 在本地网络上分析原始数据包使用的是数据包 _____ 。
3. 模仿酒店无线网络的恶意热点是一种 _____ 。
4. 保护网页流量传输需要使用 _____ 加密。
5. 加密所有网络输出需要使用客户端 _____ 。
6. 穿过公共网络的加密通信路径是一条 _____ 。

词汇词库

加密隧道 | 流量拦截 | 数据传输 | 邪恶双子 | 嗅探 | 虚拟专网 | HTTPS | WPA3

在此写下你的答案:

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

检查点 4: 安全概念配对

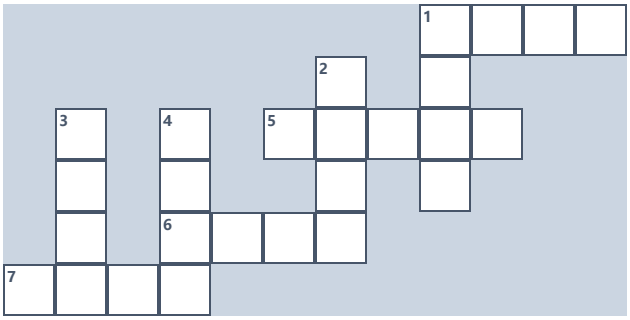
定义配对

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. 拦截	**A**	现代 Wi-Fi 安全标准。（G）
	2. 嗅探	**B**	传输过程中的安全数据通道。
	3. 恶意双子热点	**C**	过滤传入流量。
	4. HTTPS	**D**	模仿 Wi-Fi 的流氓热点。
	5. VPN	**E**	读取传输中的流量。
	6. 隧道	**F**	捕获网络数据包。
	7. WPA3	**G**	加密的虚拟专用网络。
	8. 防火墙	**H**	安全的网页传输。

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. 在传输途中截获他人的数据 (4)

5. 捕获并分析网络上传输的数据包 (5)

6. 对传输中的数据加密，防止被窃听 (4)

7. 对穿过隧道的数据进行加密保护 (4)

纵向

1. 捕获网络数据包 (4)

2. 数据从一台设备经网络发送到另一台设备的过程 (4)

3. 传输中的安全数据通路 (4)

4. 对无线网络中传输的数据进行加密保护 (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: 在传输途中截获他人的数据 (4 字):

5 横向: 捕获并分析网络上传输的数据包 (5 字):

6 横向: 对传输中的数据加密，防止被窃听 (4 字):

7 横向: 对穿过隧道的数据进行加密保护 (4 字):

纵向

1 纵向: 捕获网络数据包 (4 字):

2 纵向: 数据从一台设备经网络发送到另一台设备的过程 (4 字):

3 纵向: 传输中的安全数据通路 (4 字):

4 纵向: 对无线网络中传输的数据进行加密保护 (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 地 公 安 信 览 器 隐 记 输 包 理 务 防 攻
险 名 护 系 防 全 输 服 数 安 备 域 攻 隐 截
服 密 器 安 证 隐 接 传 证 据 户 份 户 系 址
服 加 数 备 拦 络 护 地 人 访 拦 接 拦 份 管
浏 线 安 软 址 数 务 址 嗅 墙 线 截 系 探 息
击 无 防 密 设 据 访 加 息 身 件 墙 击 嗅 统
风 加 公 管 传 包 器 议 密 地 数 网 数 加 险
探 协 址 包 协 嗅 嗅 公 域 传 务 软 墙 址 服
密 接 证 认 名 探 统 击 护 认 输 认 统 设 管
加 公 输 保 据 理 系 风 连 备 数 浏 服 理 线
道 数 据 嗅 探 隧 加 拦 浏 息 名 隐 截 服 加
隧 认 务 软 数 录 击 据 共 全 网 截 身 密 服
名 络 务 风 据 务 户 隐 访 码 设 统 隧 墙 器
接 备 拦 理 传 户 软 道 用 络 络 道 软 险 证
击 公 探 统 输 址 设 公 备 码 证 无 数 息 备

词汇列表

数据嗅探 **数据传输** **数据包嗅探** **加密传输** **无线加密** **隧道加密** **数据拦截** **加密隧道**

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. 数据嗅探
B. 数据传输
C. 数据包嗅探
D. 加密传输
E. 无线加密
F. 隧道加密
G. 数据拦截
H. 加密隧道

定义与配对字段
1. 在传输途中截获他人的数据。
2. 捕获并分析网络上传输的数据包。
3. 数据从一台设备经网络发送到另一台设备的过程。
4. 对穿过隧道的数据进行加密保护。
5. 传输中的安全数据通路。
6. 捕获网络数据包。
7. 对无线网络中传输的数据进行加密保护。
8. 对传输中的数据加密，防止被窃听。

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. 嗅 数 探 据 _____
2. 数 探 嗅 包 据 _____
3. 密 无 加 线 _____
4. 截 拦 数 据 _____
5. 输 数 传 据 _____
6. 传 输 加 密 _____
7. 加 隧 密 道 _____
8. 加 道 隧 密 _____

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	更新软件的原因			
2	会自动连接 Wi-Fi 的设备			
3	你绝不应分享的信息			
4	你今天就可以开始的安全习惯			
5	在咖啡馆保持安全的方法			
6	可能被黑客入侵的设备			
7	黑客在开放 Wi-Fi 上能看到的内容			
8	虚假 Wi-Fi 网络的迹象			
9	公共 Wi-Fi 的替代方案			
10	电子邮件中的警示信号			
11	在公共 Wi-Fi 上不要做的事			
12	提供免费 Wi-Fi 的地方			
13	保护账户的方法			
14	电脑被感染的迹象			
15	看起来可疑的 Wi-Fi 名称			

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: 遏制公共 Wi-Fi 数据包嗅探



情景: 一名远程销售主管连接到机场公共 Wi-Fi 网络后，发现几封以明文发送的敏感商务邮件在发出后不久就被泄露。

讨论问题: 分析公共网络的风险，并概述一种流量加密解决方案。

案例研究 2: 防御恶意双胞胎流氓热点



情景: 攻击者部署了一个名为“CoffeeShop_Guest”的恶意无线接入点，模仿合法的咖啡店热点，捕获毫无防备的客人的网络流量。

讨论问题: 详细说明检测和阻止恶意接入点的验证步骤。

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

服=1 专=2 嗅=3 输=4 密=5 拟=6 码=7 探=8 截=9 络=10

户=11 据=12 公=13 隧=14 加=15 用=16 器=17 安=18 道=19 拦=20

虚=21 网=22 包=23 传=24 无=25 线=26 共=27 全=28 务=29 数=30

16	21	6	2	22		15	5		13	27	25	26	22	10

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: 公共 Wi-Fi 为什么不安全?

开放的公共 Wi-Fi 不会对空中传输的流量加密，因此附近的其他人可以截获任何未受保护的数据。 [2]

Q2: 什么是数据包嗅探?

数据包嗅探器会捕获流经网络接口的原始数据，暴露明文密码和流量详情。

Q3: 什么是 Evil Twin（邪恶双胞胎）?

黑客设置的恶意接入点，模仿可信本地 Wi-Fi 热点的名称和设置。

Q4: VPN 如何保护我?

它将你的流量通过加密隧道路由，向本地网络嗅探器隐藏你的浏览活动。

Q5: HTTPS 能在公共 Wi-Fi 上保护我吗?

是的，它会加密浏览器与网站之间交换的数据，而 VPN 增加了另一层保护。

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: WPA3 是什么?

现代 Wi-Fi 保护访问标准，提供更强的加密，并能防范离线字典攻击。 [1]

Q7: 公共 Wi-Fi 会传播恶意软件吗?

是的，攻击者可以拦截流量，并向你的浏览器会话注入恶意下载提示（路过式下载）。

Q8: 文件共享有什么风险?

如果启用了文件共享，公共网络上的其他用户可能读取或修改你的本地文件夹目录。

Q9: 什么是强制门户?

酒店或咖啡馆网络用来授予上网权限的登录页面，有时可能被攻击者伪造。

Q10: 不使用 Wi-Fi 时我应该关闭它吗?

是的，关闭 Wi-Fi 可防止你的设备自动连接到不受信任的网络。

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: 中间人攻击如何利用 DNS?

通过在恶意路由器上使用 DNS 欺骗，将目标浏览器引导到外观相似的网络钓鱼登录页面，而不是目标域名。

Q2: 什么是会话劫持?

攻击者在公共 Wi-Fi 上嗅探未加密的会话 Cookie，并导入它以绕过凭据登录。

Q3: 什么是 SSL 剥离?

一种中间人攻击，攻击者将用户的安全 HTTPS 请求降级为未加密的 HTTP，从而以明文捕获登录信息。

Q4: HSTS 如何防御 SSL 剥离?

HTTP Strict Transport Security 会强制浏览器仅通过 HTTPS 连接，并拒绝回退到未加密的 HTTP。 [3]

Q5: 什么是分应用隧道 VPN?

一种仅将公司流量路由经过 VPN、而将公共互联网数据直接发送的配置，可能带来泄漏路径暴露的风险。

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: WPA2 为什么容易受到 KRACK 攻击?

密钥重装攻击利用 WPA2 四次握手，在不知道 Wi-Fi 密码的情况下解密数据包。

Q7: 什么是客户端隔离?

一项路由器安全设置，阻止已连接的 Wi-Fi 设备彼此直接通信，从而阻止本地嗅探。

Q8: 攻击者如何使用虚假的 DNS 服务器?

他们配置恶意路由器，向客户端分配虚假 DNS 服务器，从而拦截并改写所有网页查询。

Q9: VPN 能隐藏我的本地 MAC 地址吗?

不会。MAC 地址是本地的第二层标识符；请改用设备内置的 MAC 随机化（私有地址）设置。

Q10: 什么是强制门户欺骗攻击?

攻击者在恶意热点上托管虚假身份验证门户，以免费 Wi-Fi 接入为幌子窃取凭据。

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

远程工作者经常在咖啡馆、酒店和机场使用 Wi-Fi，而在这些地方他们无法控制网络的安全性。

2. 安全洞察

Evil Twin 恶意热点可以复制可信网络的确切名称和 MAC 地址，使设备产生混淆。

3. 安全洞察

Wireshark 等数据包嗅探软件是免费的，可以以明文形式显示未加密的 HTTP 密码。

4. 安全洞察

WPA3 安全使用对等同时验证（SAE）来防范本地暴力破解攻击。

5. 安全洞察

SSL 剥离攻击通过在网关处拦截最初的 HTTP 重定向，绕过基本的 HTTPS 保护。

6. 安全洞察

HTTP Strict Transport Security (HSTS) 响应头可阻止浏览器回退到未加密的 HTTP 连接。 [3]

7. 安全洞察

关闭“自动连接”可防止智能手机在公共场所连接到外观相似的恶意网络。

8. 安全洞察

企业“始终开启”的 VPN 配置会强制所有远程办公人员的网络流量通过企业防火墙。

9. 安全洞察

流氓接入点可以发出伪造的 DNS 应答，将目标域名重定向到钓鱼服务器。

10. 安全洞察

没有 VPN 时，开放热点上的其他用户可以看到你的设备访问了哪些网站和服务器。

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] Wi-Fi Alliance. (n.d.). Security.
https://www.wi-fi.org/discover-wi-fi/security

[2] Federal Trade Commission. (2023). Are Public Wi-Fi Networks Safe? What You Need To Know.
https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[3] MDN Web Docs. (n.d.). Strict-Transport-Security header.
https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Strict-Transport-Security

[4] 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

[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

什么是中间人（MitM）攻击？ → 拦截并篡改共享网络上两方之间的通信

2 问题 2 正确答案: A

教学提示

什么是流氓接入点（邪恶双胞胎）？ → 与合法网络使用相同 SSID 的恶意 Wi-Fi 热点

3 问题 3 正确答案: A

教学提示

VPN 如何保护公共 Wi-Fi 流量？ → 它将所有网络数据包封装在加密隧道中，使嗅探器无法读取

4 问题 4 正确答案: A

教学提示

什么是数据包嗅探？ → 使用硬件或软件工具捕获并记录网络数据包

5 问题 5 正确答案: A

教学提示

HTTPS 的作用是什么？ → 加密浏览器与网站服务器之间的会话流量

答案: 检查点 2 – 判断题（正确或错误）

6 问题 6 正确答案: 正确

教学提示

已连接的用户可以轻易在开放的公共 Wi-Fi 网络上捕获明文数据。

7 问题 7 正确答案: 错误

教学提示

错误: 邪恶双胞胎是攻击者设置的未经授权的热点，用来模仿真实热点。

8 问题 8 正确答案: 错误

教学提示

错误: VPN 在隧道中加密流量，因此本地嗅探器无法读取。

9 问题 9 正确答案: 错误

教学提示

错误: HTTPS 会加密整个 HTTP 交换，包括 URL 路径和页面内容。

10 问题 10 正确答案: 正确

教学提示

使用 WPA3 安全的 Wi-Fi 热点比开放的、无密码的网络提供更强的保护。

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

E 1. 拦截	F 2. 嗅探	D 3. 恶意双子热点	H 4. HTTPS
G 5. VPN	B 6. 隧道	A 7. WPA3	C 8. 防火墙

检查点 3: 答案 – 关键术语

1 流量拦截	2 嗅探	3 邪恶双子	4 HTTPS
5 虚拟专网	6 加密隧道		

检查点 6 替代活动: 答案 – 词语配对

1 G – 数据拦截	2 C – 数据包嗅探	3 B – 数据传输	4 F – 隧道加密
5 H – 加密隧道	6 A – 数据嗅探	7 E – 无线加密	8 D – 加密传输

教师讨论提示

关键术语:
检查学生能否用自己的话解释拦截、嗅探和恶意双子热点，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。

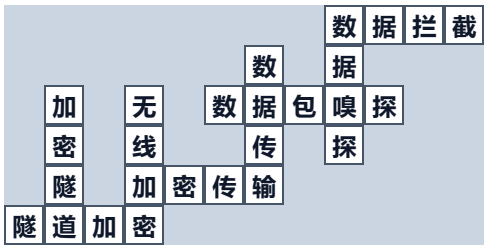
来源评估:
请学生根据练习单的参考资料至少核实一项说法，并讨论数字、价格和规则为什么可能随时间变化。

谜题答案与教师说明

找词答案

全	地	公	安	信	览	器	隐	记	输	包	理	务	防	攻
险	名	护	系	防	全	输	服	数	安	备	域	攻	隐	截
服	密	器	安	证	隐	接	传	证	据	户	份	户	系	址
服	加	数	备	拦	络	护	地	人	访	拦	接	拦	份	管
浏	线	安	软	址	数	务	址	嗅	墙	线	截	系	探	息
击	无	防	密	设	据	访	加	息	身	件	墙	击	嗅	统
风	加	公	管	传	包	器	议	密	地	数	网	数	加	险
探	协	址	包	协	嗅	嗅	公	域	传	务	软	墙	址	服
密	接	证	认	名	探	统	击	护	认	输	认	统	设	管
加	公	输	保	据	理	系	风	连	备	数	浏	服	理	线
道	数	据	嗅	探	隧	加	拦	浏	息	名	隐	截	服	加
隧	认	务	软	数	录	击	据	共	全	网	截	身	密	服
名	络	务	风	据	务	户	隐	访	码	设	统	隧	墙	器
接	备	拦	理	传	户	软	道	用	络	络	道	软	险	证
击	公	探	统	输	址	设	公	备	码	证	无	数	息	备

填字游戏答案



填字游戏答案教师指南

横向

1 横向: 数据拦截 在传输途中截获他人的数据 (4 字)

5 横向: 数据包嗅探 捕获并分析网络上传输的数据包 (5 字)

6 横向: 加密传输 对传输中的数据加密，防止被窃听 (4 字)

7 横向: 隧道加密 对穿过隧道的数据进行加密保护 (4 字)

纵向

1 纵向: 数据嗅探 捕获网络数据包 (4 字)

2 纵向: 数据传输 数据从一台设备经网络发送到另一台设备的过程 (4 字)

3 纵向: 加密隧道 传输中的安全数据通路 (4 字)

4 纵向: 无线加密 对无线网络中传输的数据进行加密保护 (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. 嗅数探据 — **数据嗅探**
2. 数探嗅包据 — **数据包嗅探**
3. 密无加线 — **无线加密**
4. 截拦数据 — **数据拦截**
5. 输数传据 — **数据传输**
6. 传输加密 — **加密传输**
7. 加隧密道 — **隧道加密**
8. 加道隧密 — **加密隧道**

秘密密码挑战答案

“用虚拟专网加密公共无线网络”

案例研究答案

A 案例研究 1: 遏制公共 Wi-Fi 数据包嗅探

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一位连接到机场公共 Wi-Fi 网络的远程销售主管注意到，几封敏感的商务邮件在以明文发送后不久就被泄露了。
- 推荐策略与解决方案: 要求所有远程工作站使用企业 VPN 客户端。强制使用仅限 HTTPS 的浏览器扩展，并在客户端防火墙处阻止未加密的协议（如 HTTP 和 FTP）。

B 案例研究 2: 防御恶意双胞胎流氓热点

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 攻击者部署了一个名为“CoffeeShop_Guest”的恶意无线接入点，冒充合法的咖啡馆热点，截获毫无戒备的客人的网络流量。
- 建议策略与方案: 审核接入点的 BSSID MAC 地址以验证网络真实性。强制执行客户端合规验证以阻止连接开放网络，并要求敏感工作使用手机热点。