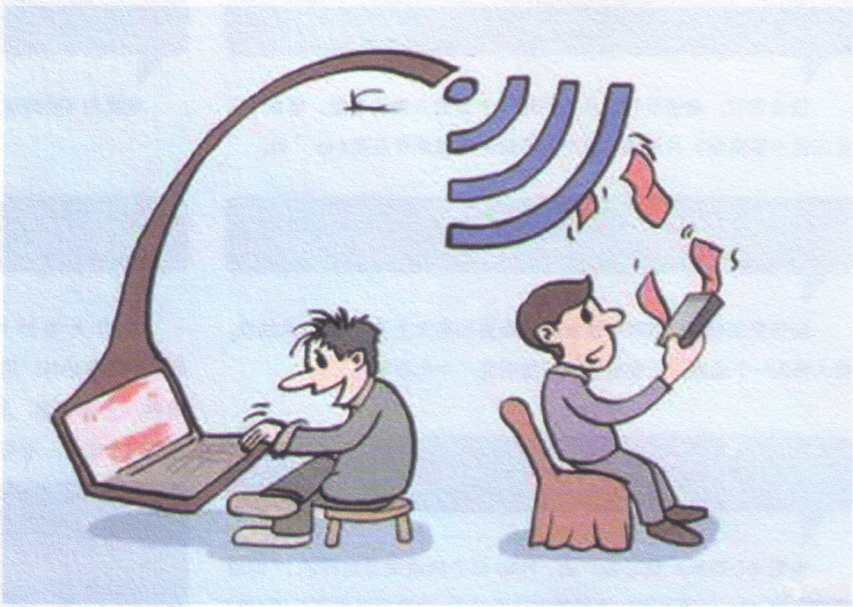
网络安全之WIFI安全

方便的WIFI，还方便了什么？

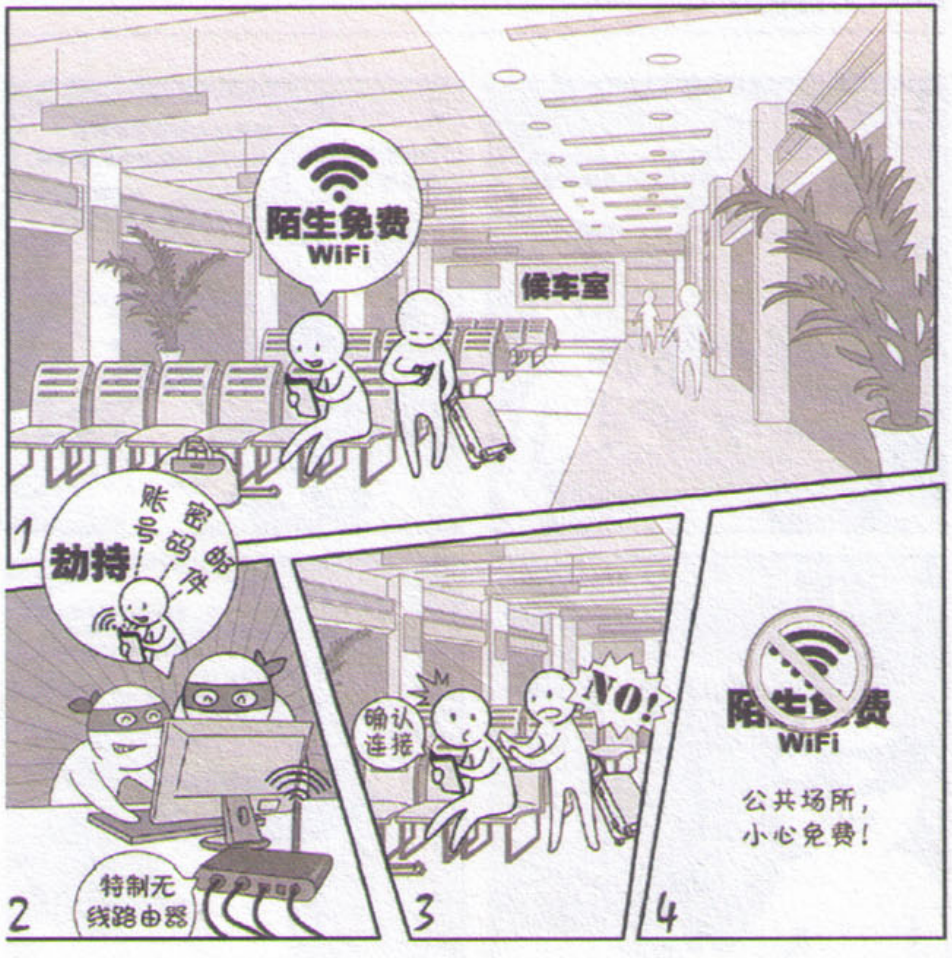


随着移动终端的兴起和互联网技术的不断进步，古老的盗窃、诈骗、骚扰手段也是旧貌换了新颜。我们身边有多少人知道 WIFI 并不安全？

亲没看错，就是这个问题。使用 WIFI 上网时我们的个人信息安全时刻存在着巨大的风险和隐患。

黑客自己搭建一个“山寨 WIFI”，起一个与附近 WIFI 相似的名字，不设登录密码诱使人连接。用户使用时，传输的数据就会被黑客监控，个人隐私、账号名和密码等相关信息也可以轻易被盗取。不少人喜欢随时开着手机的无线网自动连接功能，这样存在很大风险。

免费 WIFI 接入

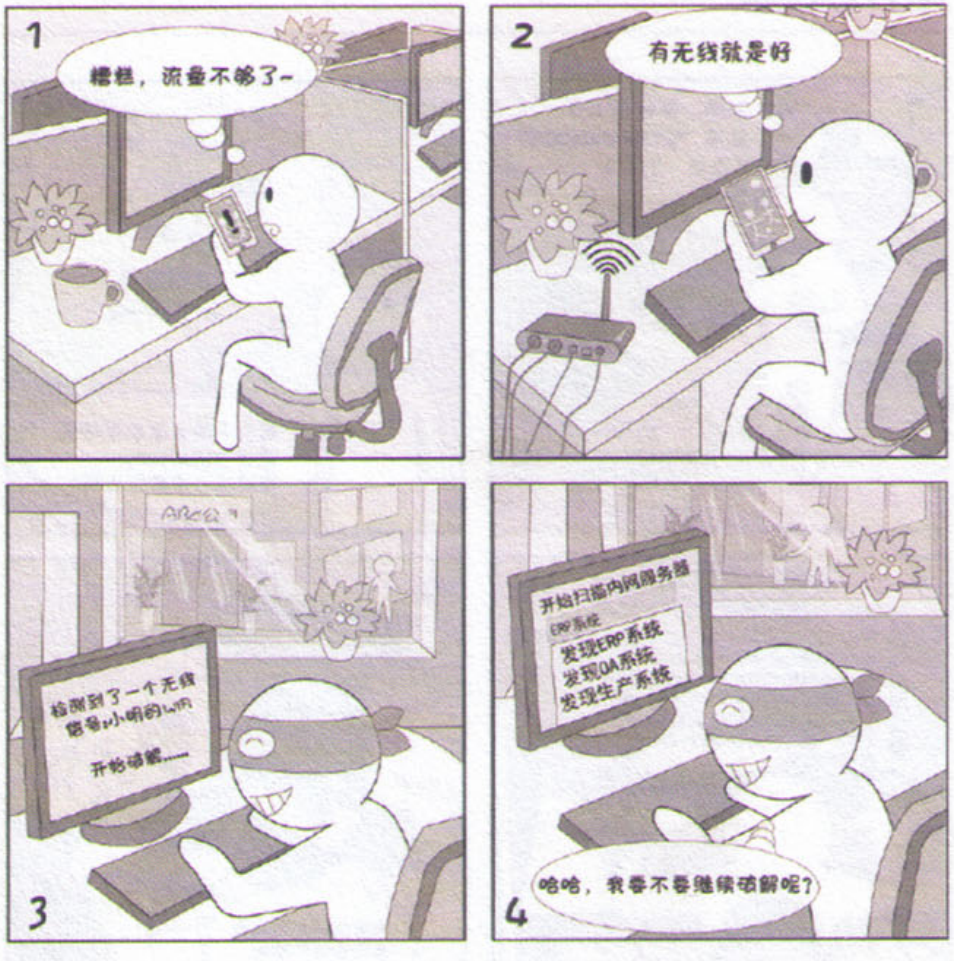


不法分子通常会搭建与常用 WIFI 相同或相近的 WIFI，设置空密码或者相同密码吸引公众连接，然后在 WIFI 路由器上劫持 DNS，将用户引入到钓鱼网站获取账号密码，或者在路由器上监听手机流量，获取明文密码。

小编温馨提示：

- 在公共场合链接 WIFI 时请同商家仔细确认 WIFI 名称；
- 没有密码的公共 WIFI 请慎用；
- 在使用支付 APP 时请使用运营商的 4G 网络，不要使用公共 WIFI 哦。

私搭 WIFI 热点

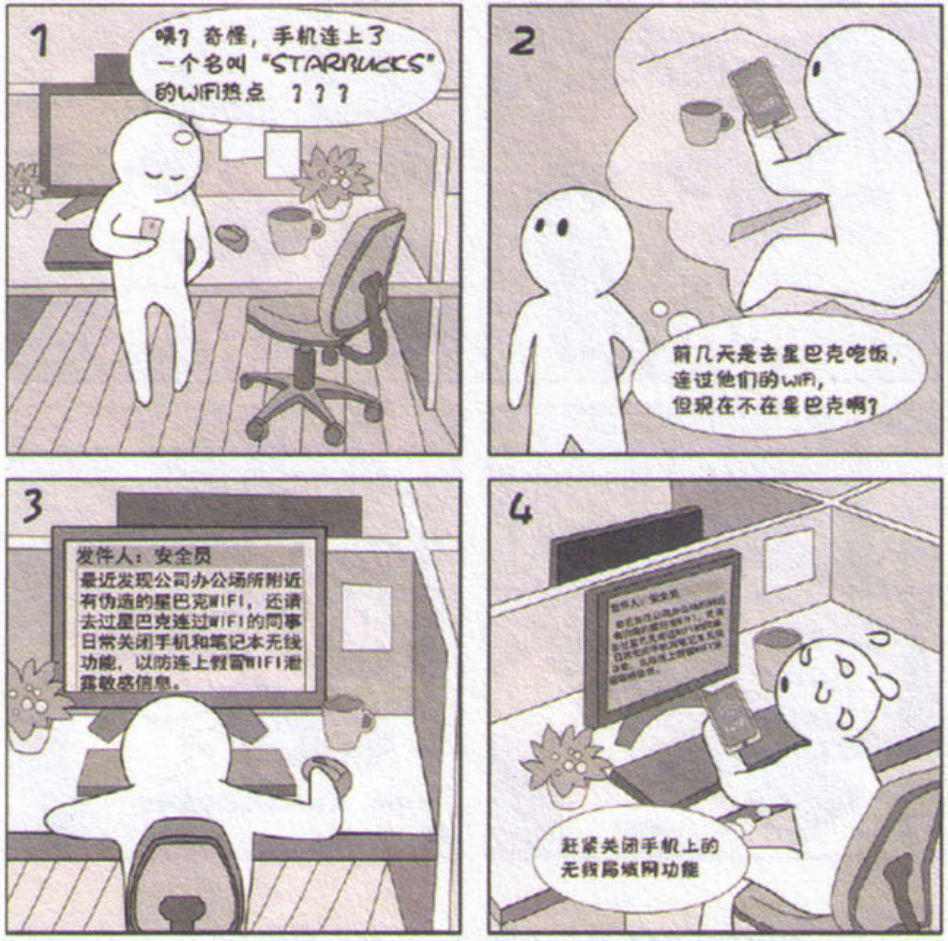


无线路由器有较多的安全隐患，比如之前的 WEP 认证能很轻易破解。个人架设无线路由器，如果配备不当，家用最多导致蹭网或个人资料泄漏，但在公司使用可能会导致内网被入侵，公司机密、客户资料泄密，后果不堪设想。

小编温馨提示：

- 在办公网络架设无线路由器必须经过公司批准并进行安全检查
- 认证方式使用安全的 WPA2 算法
- 建议隐藏 SSID，绑定接入设备的 MAC 地址
- WIFI 密码必须八位以上，包含大小写、数字和标点符号，定期改密码

WIFI 自动连接

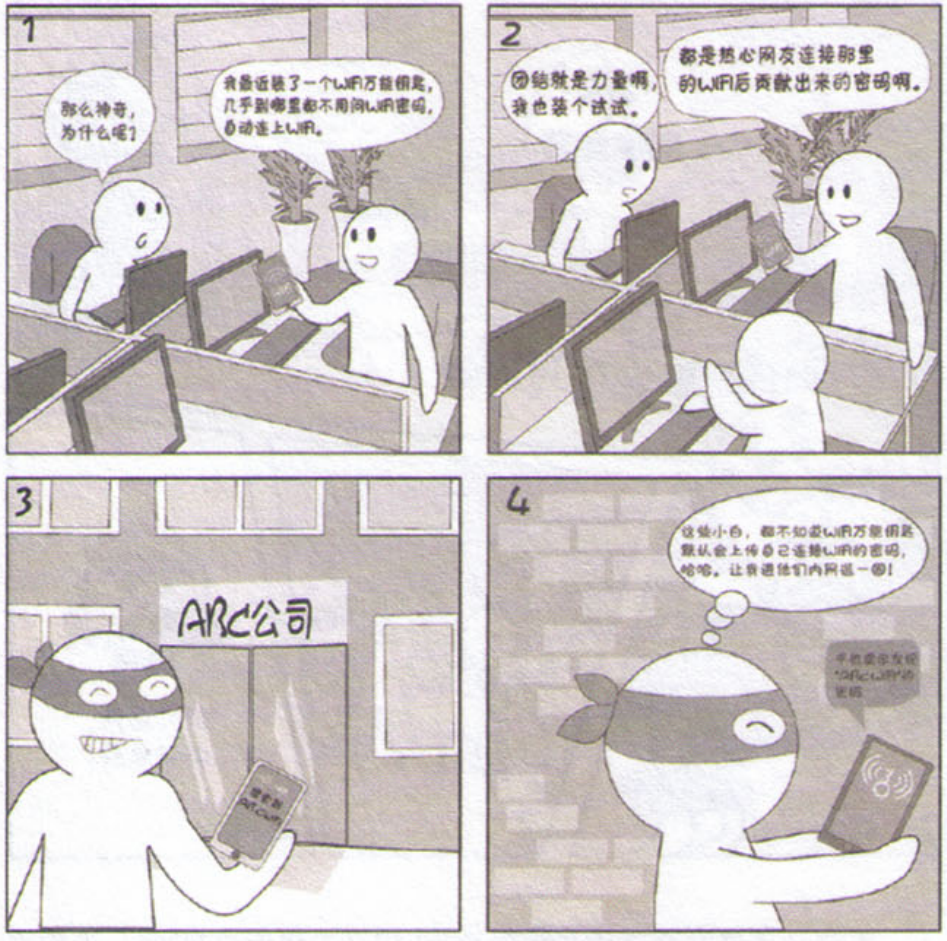


一些手机在搜索到不是同一个 WIFI 热点但名称相同的 WIFI 时也会自动使用保存的密码连接，这就给黑客以可乘之机。

小编温馨提示：

- 日常不用 WIFI 时关闭手机和笔记本的无线局域网功能，以防自动连接恶意 WIFI
- 当手机和笔记本连上 WIFI 后，留意连接到的 WIFI 热点名称

WIFI 万能钥匙



手机上的 WIFI 万能钥匙类的 APP 在安装后默认设置会自动上传你所连接的 WIFI 的密码。这些密码一般不会明文给出，只会在连接 WIFI 时自动输入，但曾爆出漏洞用一个 APP 能读出检测到 WIFI 的密码，这样就可以用笔记本接入 WIFI 使用更强大的攻击工具了。

小编温馨提示：

- 建议不要使用 WIFI 万能钥匙类 APP
- 如果必须使用建议关掉自动上传密码功能

WIFI 安全口诀：

- 公共场合连 WIFI，名称一定确认好；
- 私搭路由要审批，安全设置莫忘记；
- 无密 WIFI 不要连，安全支付用 4G；
- WIFI 不用要关闭，万能钥匙请回避。