网络安全意识 | 无形之刃，最为致命。

WiFi安全现如今已经是老生常谈的问题了，笔者也查阅了很多相关文章，提出的解决方案一般如下三种：

1.不要连接公共WIFI。

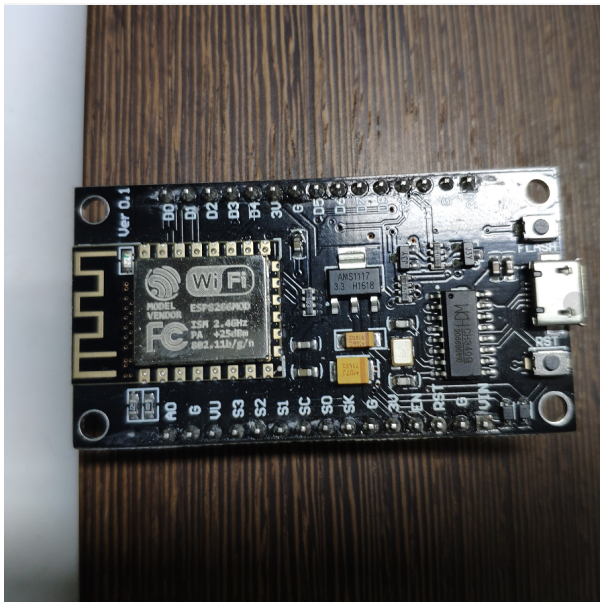
2.开发者使用更安全的HTTPS协议传输数据。

3.办公WIFI的话将内网和访客分开。

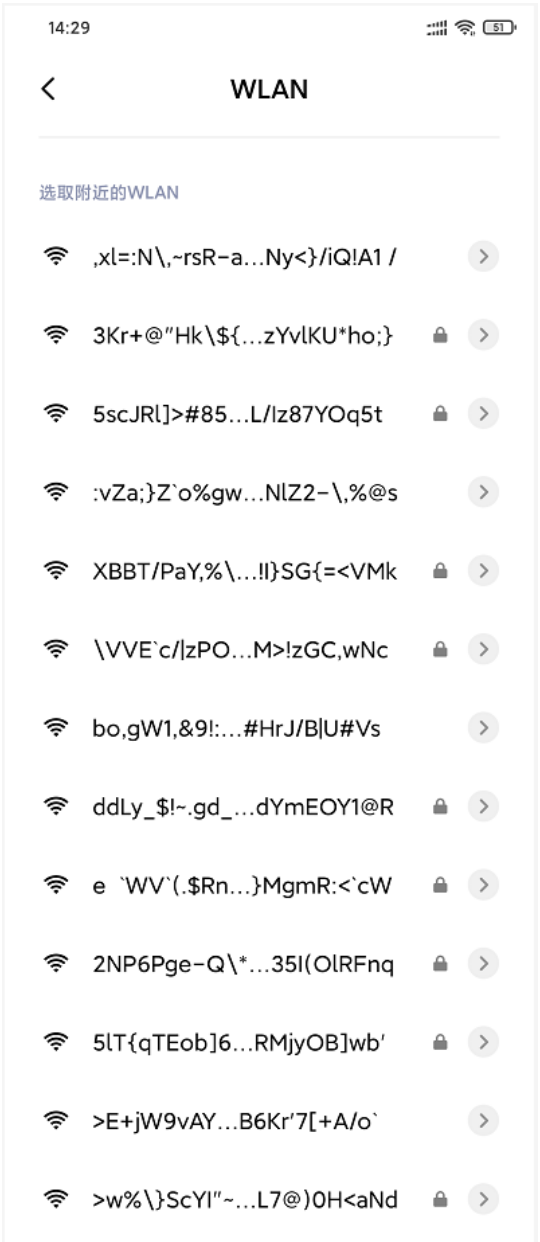
诚然这些方法可以避免一些安全隐患，但是一刀切的禁止连接公共WIFI，实在是有些因噎废食的意味。即便开发者使用了HTTPS协议，但如果没有进行双向校验的话，仍然存在**中间人攻击**的风险，而大多数情况下开发者因为运行速度的原因，并不会采用这种方式。访客WiFi如果自身网络设备存在安全问题，即使与办公网络分开，通过网络设备一样可以轻而易举的进入内网。

世面已经有太多告诉我们不应该做什么事情的文章了，笔者希望本系列文章能告诉我们普通人在碰到时应该做什么，以及在不得不使用开放WiFi时如何将自身的风险降到最低。

这是一个名叫ESP8266的WiFi开发模块，淘宝售价仅为14.8元，插上充电宝就可以启动。



它的效果？它可以生产大量随机WiFi SSID广播，让你找不到其他WIFI。



它会扫描周围所有WiFi查看什么设备进行了连接。

```
[===== Stations =====]
ID MAC               Ch Name            Vendor   Pkts     AP                                Last Seen Selected
=============================================================================================================
 0 58:94:6b:33:a4:f4  4                 IntelCor       48 [redacted]                        <1sec
 1 50:2b:73:cb:af:af 11                 TendaTec       13 HUAWEI-5HXHAN                    <1sec
 2 50:2b:73:c8:b1:4d 11                 TendaTec        8 HUAWEI-5HXHAN                    <1sec
 3 b0:59:47:55:8b:e1 13                 Shenzhen        8 *HIDDEN*                         <1sec
 4 f4:6a:92:b3:bc:23 11                 Shenzhen        4 HUAWEI-5HXHAN                    <1min
 5 f4:6a:92:b3:a8:bc 11                 Shenzhen        2 HUAWEI-5HXHAN                    <1sec
 6 50:2b:73:cb:af:9b 11                 TendaTec        2 HUAWEI-5HXHAN                    <1min
 7 04:79:70:03:d2:b6 11                 HuaweiTe        1 SXRS                             <1min
 8 20:f4:1b:cb:06:ba 11                 Shenzhen        1 HUAWEI-5HXHAN                    <1min
=============================================================================================================
```

而如果它被用来作恶。首先他会克隆大量目标WiFi SSID，然后在向连接目标WiFi的设备发送解除认证帧来关闭设备的连接，使其掉线。用户再次输入密码连接WiFi时便已经落入早已准备好的天罗地网。因为几乎没有人可以在这么多一模一样的列表里分辨出真实的WiFi。

在连接WiFi时，如果发现**大量重复或随机WiFi名出现**时，我们应该有所警觉。对于这种移动式神出鬼没的钓鱼WiFi威胁，生活中有可能遇到的情况比较少，而比较多的，泄露WiFi密码的方式还有两种，一种是自己不经意之间，通过**某APP**分享出去，这里就不点名了；第二种就是由于人为的原因。

笔者目前在某公寓租住，公寓给每户都配备了独立的路由器，但是不允许住户更改密码，美其名曰方便维修和管理。每户的WiFi默认密码都是房间号输两遍，比如笔者门牌号是0721，WiFi密码就是07210721，无线路由器的默认密码都是123123。笔者就此事向管家进行沟通，并说明安全隐患，得到的答复是：”你被黑客攻击了，关我什么事“。无奈之下，只好回去更改了自己的WiFi以及路由器密码，过上了用自己家的WiFi看电视，用楼上的WiFi下载的生活。

更危险的是，因为路由器没有更改密码，所以就可以随便的登录到大多数住户的管理页面，只需轻轻选择远程Web管理权限，便可在千里之外进行控制。

在这里建议大家，WiFi的安全性，由于目前智能设备的增加大大提高了其暴露后的攻击面。WiFi密码这个东西若是自用一般不要分享出去，如有被泄露可的能应及时更改。如果需要向外提供WiFi,应该与自家设备所连接的分开。至于路由器管理密码更应该牢牢的掌握在自己的手中，以免在不经意之间沦为肉鸡。

这里给大家提出几个关于WiFi安全的小建议：

对一般人来说：

- 路由器管理后台设置强密码，防止弱口令被登录。
- 关闭使用pin码登录，指的是WPS功能，只需输入数字就可登录。
- 启用WPA加密，不用已经过时的WEP加密。
- 如果特别注重安全的话可以对SSID进行隐藏。

- 不安装某APP进行WiFi密码分享。

这些就可以满足大多数人的安全需求了，在办公安全那篇里会对办公WiFi提出安全性更高的建议。

上述文章讲的都是使用个人WiFi所要注意的事情，而在酒店、饭店、机场甚至于高铁与飞机上目前都提供了公共WiFi来使用，其安全性又如何进行保障呢？

2017年的冬天，笔者和同学去北京参加一场安全技能比赛。北京的冬天很冷，比赛结束后，就一起在主办方安排的酒店休息。那时正值吃鸡如日中天，同学耐不住寂寞，连上酒店WiFi便准备Chicken Dinner。打了没多久电脑突然黑屏了，重启后发现所有硬盘都被格式化了。一是因为格式化硬盘这种事情实在太过分，二是因为电脑上确实存着与某涉密部门的项目，一怒之下便报了警。北京的出警速度很快，不一会儿，一个民警带着两个辅警赶到了酒店。询问过后，也属实无奈，一是无法确定到底是何人进行了攻击，不可能一个房间一个房间的去查；二是也不是所有民警都具备网络取证的能力。诚然连我们这些和安全接触较多的学生也不具备这个追踪能力，何苦相互为难。所幸的是项目有备份，格式化的硬盘使用恢复软件可以恢复绝大多数的数据。

事后我们分析这次攻击，酒店Wifi并没有进行隔离，所有连接进来的人都暴露在其中、可能是工具里有后门、未开防护软件、补丁没有打到最新。

总结经验教训得出了如下几点：

- 公共WiFi该用还是要用，用的是尽量避免敏感操作（登录、转账）。现如今流量也不是很贵，建议出门在外敏感操作还是使用流量，相信运营商。
- 敏感设备，存储了重要文件或者数据的设备就不要连接公共WiFi。同理手机热点是一个不错的解决方法。
- 一个整个酒店都用同一个WiFi在一般情况下的安全性都要比每个房间独立WiFi的安全性要低，连接前做好权衡。
- 大多数采用手机认证的公共WiFi会绑定IP和手机号方便出事后进行溯源相比之下会更安全一些，但是目前对于日志的保存情况我们也不要报太多的希望。