别追

病毒！别追我

你 的 电 脑 被 攻 击 了 吗

无线网络安全防护策略

WiFi上网安全

手机等智能终端安全

01 WiFi上网安全

2016/12/18

背景

WiFi是一种允许电子设备连接到一个无线局域网的传输技术，遵循IEEE802.11标准。目前使用WiFi无线网络存在重大的安全隐患，一方面是公共场所的无密码WiFi热点，很可能就是钓鱼陷阱；另一方面是网民家里的无线路由器如果设置不合理，很可能被恶意攻击者轻松攻破，攻击者除了免费享用网络带宽外，还可以登录无线路由器的管理后台，这样网民在家里通过WiFi连接无线网，进行微信、QQ、甚至网银登录，很可能在毫不知情的情况下，面临个人敏感信息遭盗取风险，甚至遭受直接的经济损失。

策 略

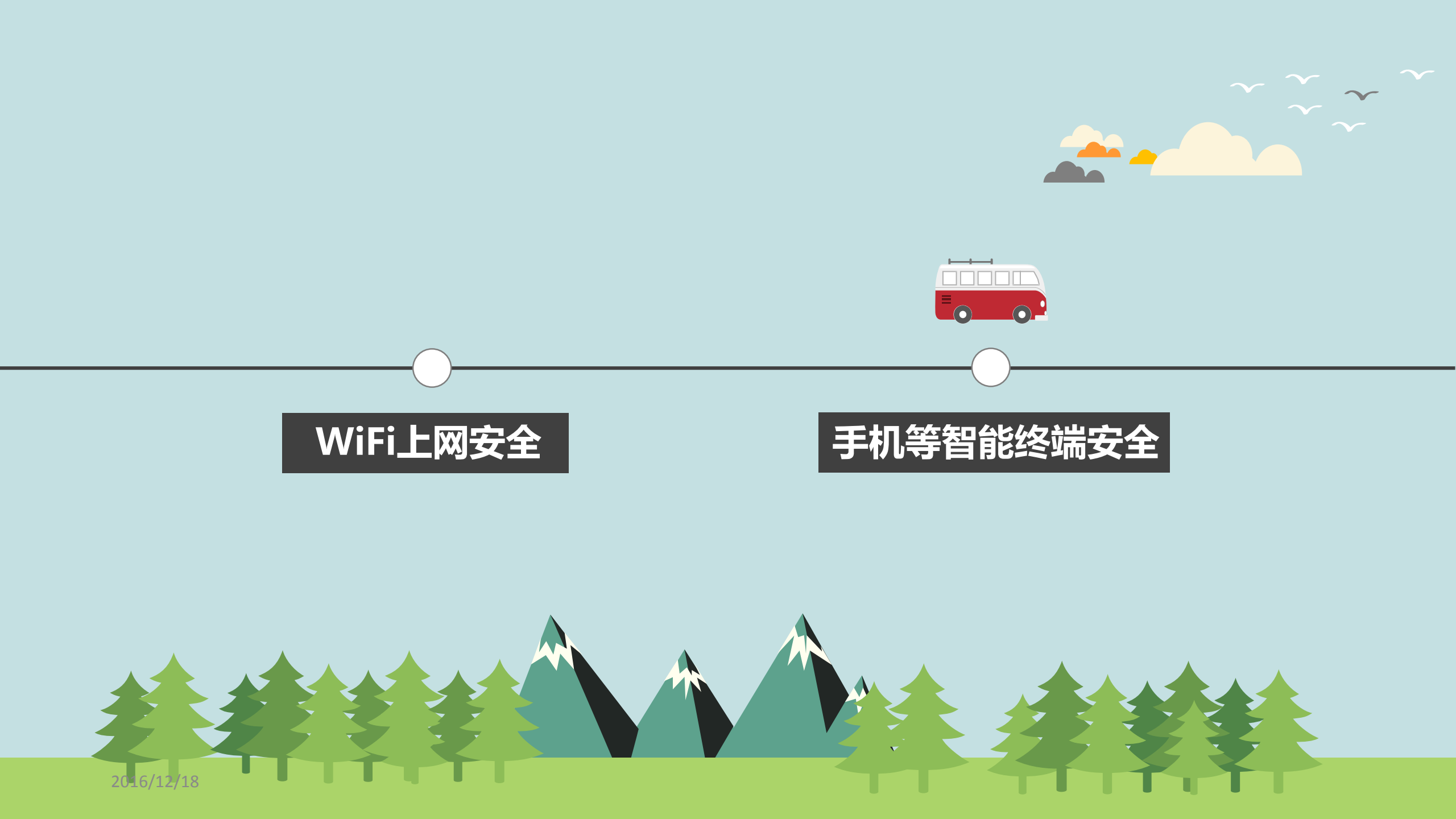
无密码WiFi的安全防范策略：

- 尽量不使用公共场所提供的无密码的WiFi无线网络；
- 不要在无密码WiFi网络环境下进行与资金有关的银行转账与支付等操作。

策 略

家庭WiFi的安全防范策略：

- 路由器管理后台的登录账号、密码，不要使用默认的admin，启用时更改为字母加数字的高强度密码；
- WiFi设置要选择WPA/WPA2加密认证方式；
- WiFi密码要使用相对复杂的密码，可提高黑客破解的难度。


WiFi上网安全
手机等智能终端安全

02 手机等智能终端安全

背景

智能手机和平板电脑等移动智能终端已融入了我们的生活，大家也越来越依赖智能手机。但手机支付漏洞、手机远程定位、手机信息泄露等安全问题屡见不鲜。智能手机强大的上网功能和部分用户不安全的上网习惯，给了手机病毒、木马乘虚而入的机会，短信彩信、邮件等也是手机病毒传播感染的重要途径。

策 略

安全防范策略：

- 设置手机锁屏密码，以防手机遗失时，被不法之徒轻易获得通讯录、文件等重要信息；
- 不要轻易点击打开别人在QQ、微信、短信、邮件中发来的链接地址；
- 平时关闭手机的自动搜索无线网络功能，仅在需要时开启；

策 略

安全防范策略：

- 在手机的QQ、微信等应用程序中关闭地理定位功能；
- 经常为智能手机做数据备份。
- 在正规的通信运营商处维修手机，防止手机被植入病毒木马程序。

谢谢观看