# 安全培训

安全培训是比较通用性质的，进行任何方面的安全建设都需要安全培训，培训内容不同而已。

不涉及具体安全项目的建设，通用性的安全培训也是可以搞的。比如安全意识培训，保密意识培训，法律法规培训。

可以将通用的安全培训加入到新员工入职培训，提高大家的安全意识，帮助大家更好的识别与处理电脑服务器异常，邮件诈骗，社工等网络攻击。

建设常态化的机制，对特定部门进行特定的安全培训，比如安全开发培训，安全测试培训。

再就是安全方面建设工作的时候进行安全培训，比如数据安全培训，办公安全保密的培训。

可以将培训做成视频，做成线上的形式，根据培训内容出考试题，需要考试通过。

## 针对产品经理的培训

为什么要收集安全需求进行安全评估

法律法规，对APP行为的规定

对数据使用的规定

等等

## 针对开发的培训

为什么要学习安全编码规范

法律法规，对APP行为的规定

## 针对测试的培训

为什么要有安全测试，如何与安全测试进行流程配合

## 全员的培训

法律法规

公司规定

安全意识

1. 弱口令，通用密码，密码泄露，密码纸条保存。
2. 系统更新及杀毒软件。一个主动关闭，一个是无人维护的设备。
3. 软件下载，电脑及手机。从邮件下载东西，登录网站。关闭杀毒不要关。升级flash。
4. 共享WIFI软件，公共WIFI。
5. 社工诈骗。社工库，钓鱼，冒充权威，冒充小白，冒充同事（安全组，审计组，监察组）。
6. 第三方托管的信息泄露：公司人员将代码信息等上传到GitHub。
7. 使用公司服务器搭建个人站点：个人CMS漏洞。或者将公司信息资产放到自己个人博客上。
8. 盗窃，泄密，买卖行为。法律。