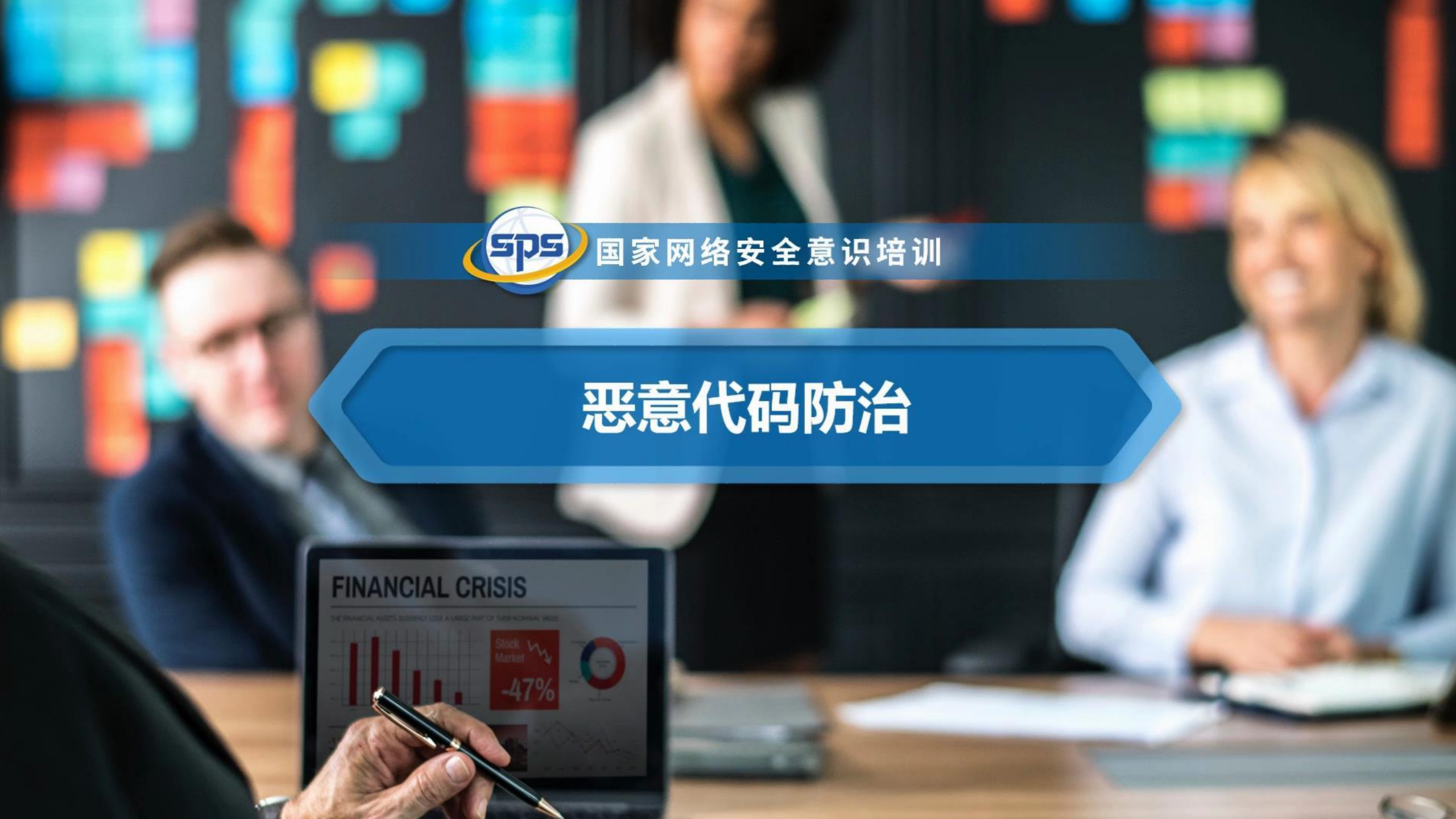
ISAT网络安全意识

第1课 恶意代码防护



国家网络安全意识培训

恶意代码防治

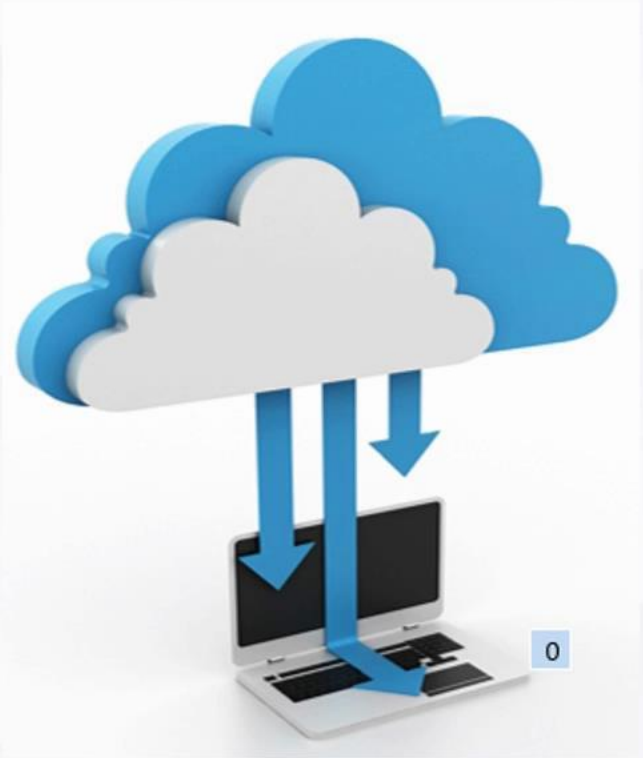
什么是恶意代码

恶意代码是没有有效作用，但会干扰或破坏计算机系统及网络功能的程序、代码或一组指令。

表现形式

- 计算机病毒
- 蠕虫病毒
- 木马程序
- 后门程序
- 流氓软件
- 逻辑炸弹
- ……

恶意代码是怎么进入你的系统的



- 通过文件传播
- 通过移动存储
- 通过网络传播
  - 网页
  - 电子邮件
  - 即时通讯
- 通过软件漏洞传播
- 攻击者主动放置

恶意代码传播方式—文件传播

感染文件

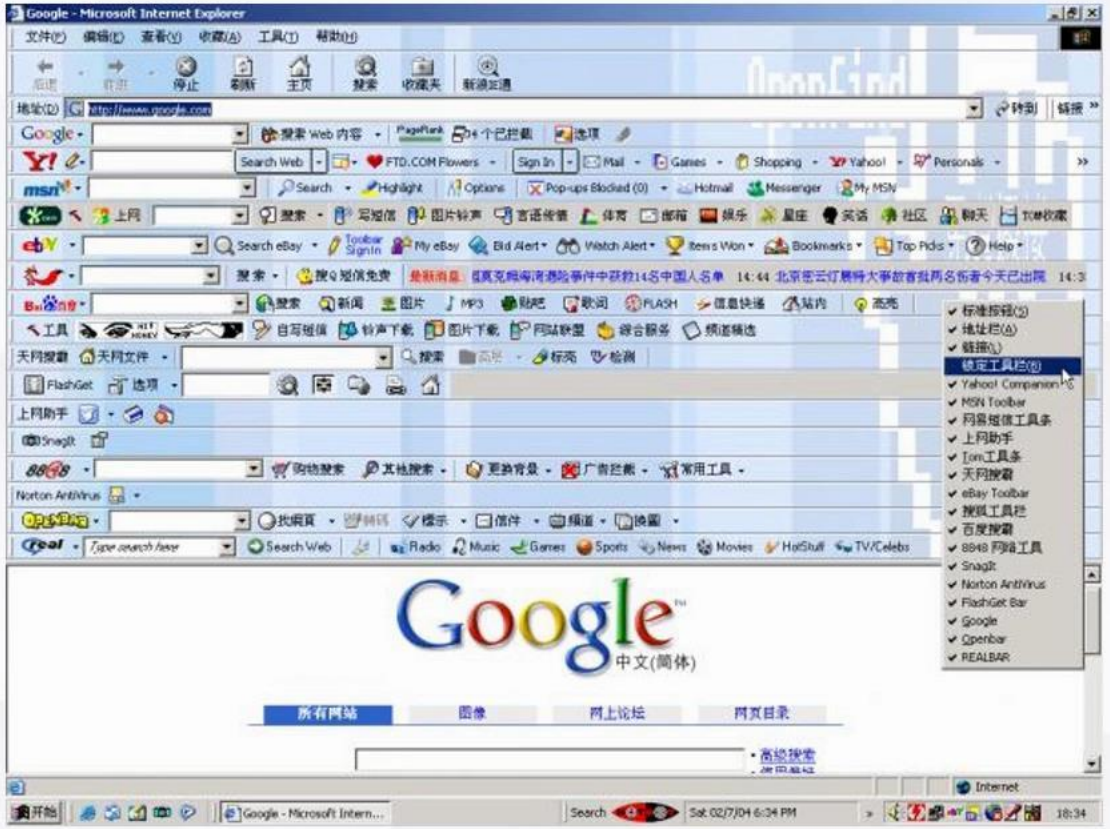
- 宏病毒（附着在Word、Excel、PPT等办公文档）
- 二进制病毒（附着在安装程序等可执行程序）

软件捆绑

- 强制安装：在安装其他软件时被强制安装上
- 默认安装：在安装其他软件时被默认安装上

防护措施

- 杀毒软件
- 选择可靠软件



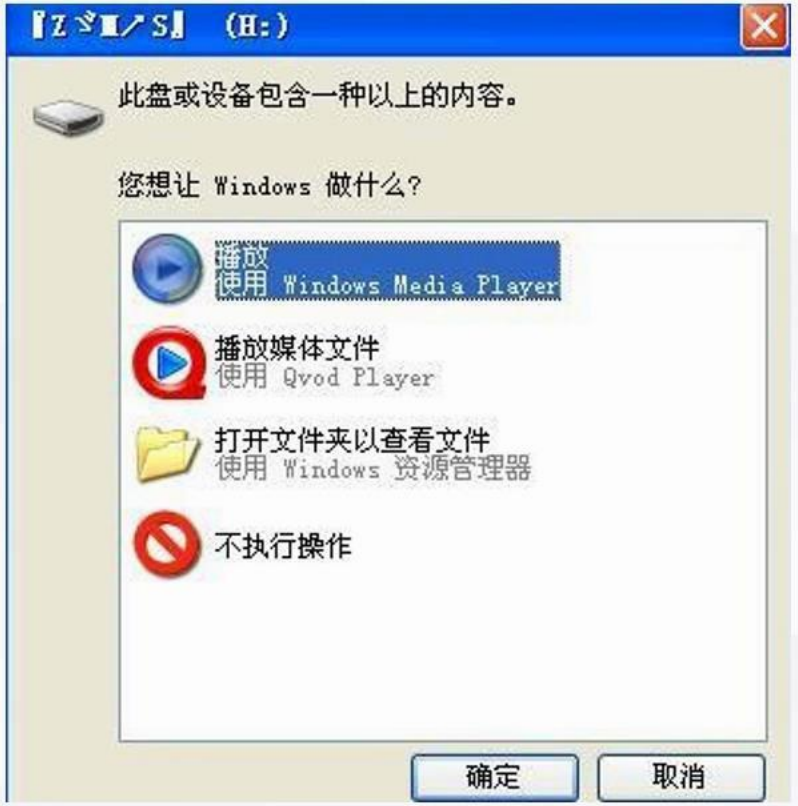
恶意代码传播方式—移动存储（U盘）

U盘病毒利用 Windows默认提供的“自动播放”功能

- 为方便用户而设计，自动执行移动存储中的指定文件
- 恶意代码（木马程序、蠕虫）将自身复制到U盘上，并设置为需要自动执行的程序，实现随U盘进行传播。

防护措施

- 修改系统设置，关闭自动播放功能
- 设置位置：组策略编辑器

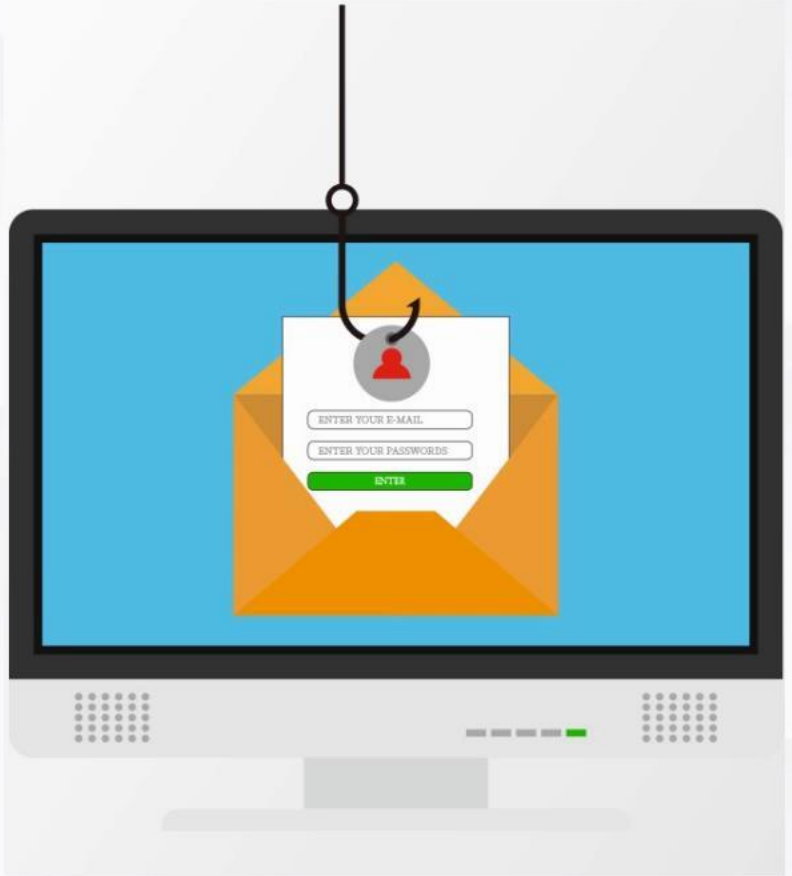


恶意代码传播方式—网页

- 利用浏览器的漏洞，用户访问网页时木马下载并安装到用户计算机上。
- 利用软件的漏洞，例如广泛使用的flash player等，在页面加载过程中将恶意代码下载并安装到用户计算机上。
- 恶意代码伪装成网页上的正常资源，例如用户需要下载的软件。

恶意代码传播方式—邮件

- **利用社会工程学诱骗用户打开附件**
  - 欺骗性邮件主题
  - 吸引人的邮件主题
- **利用系统及邮件客户端漏洞自动执行附件**
  - 尼姆达（畸形邮件MIME头漏洞）
- **防护措施**
  - 安全补丁
  - 安全意识



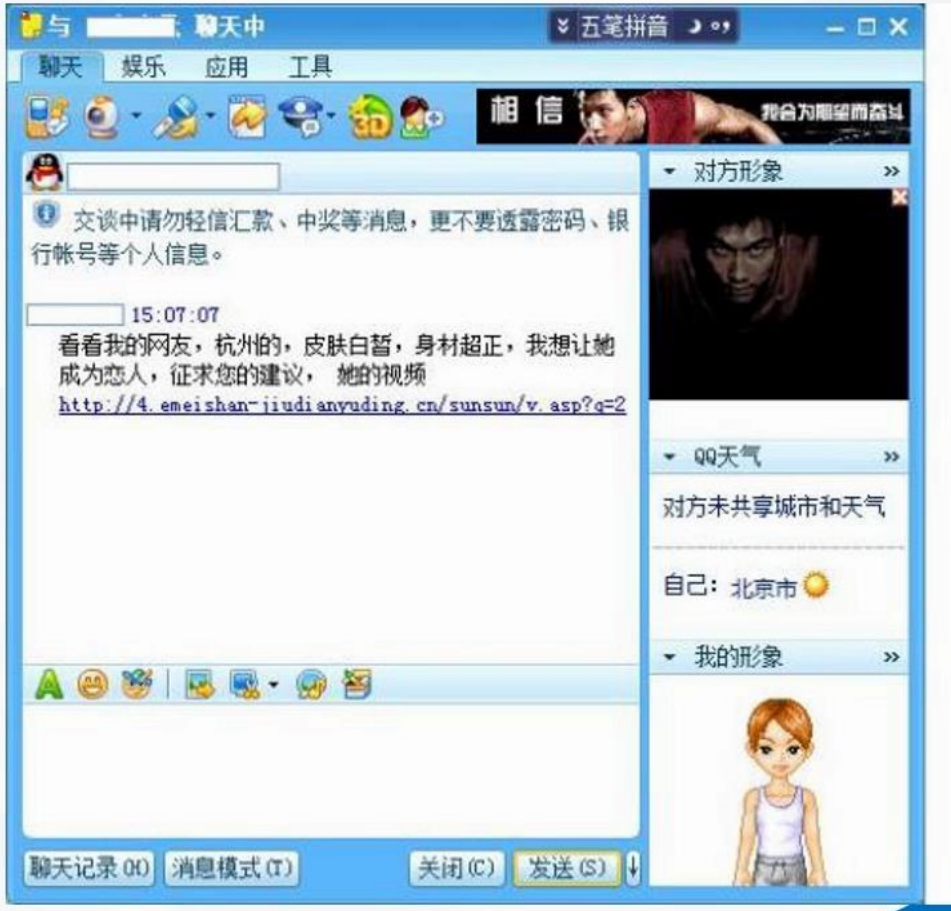
恶意代码传播方式—即时通讯

即时通讯

- 伪装即时通讯中的用户向其联系人发送消息，使用欺骗性或诱惑性字眼。

P2P下载

- 伪造成有效资源进行传播



恶意代码传播方式—主动放置

攻击者获得权限后主动放入的恶意代码

- 木马程序
- 后门程序
- 逻辑炸弹
- ……

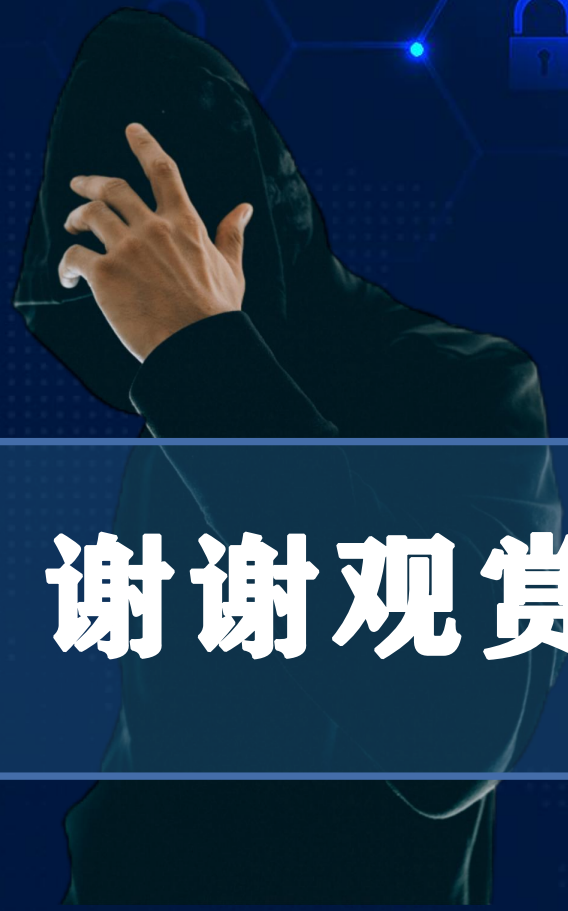
防护措施

- 防病毒
- 安全审计

恶意代码防治

- 定期检查系统更新并及时安装系统补丁
- 安装并配置好系统上的防病毒软件
- 我的杀毒软件每天都更新病毒库
- 不认识人发来的链接、二维码不随意访问
- 即使认识人发来的链接，也确认后再访问
- 我只在软件官网下载软件

树立网安意识
构筑网络空间安全人民防线



谢谢观赏