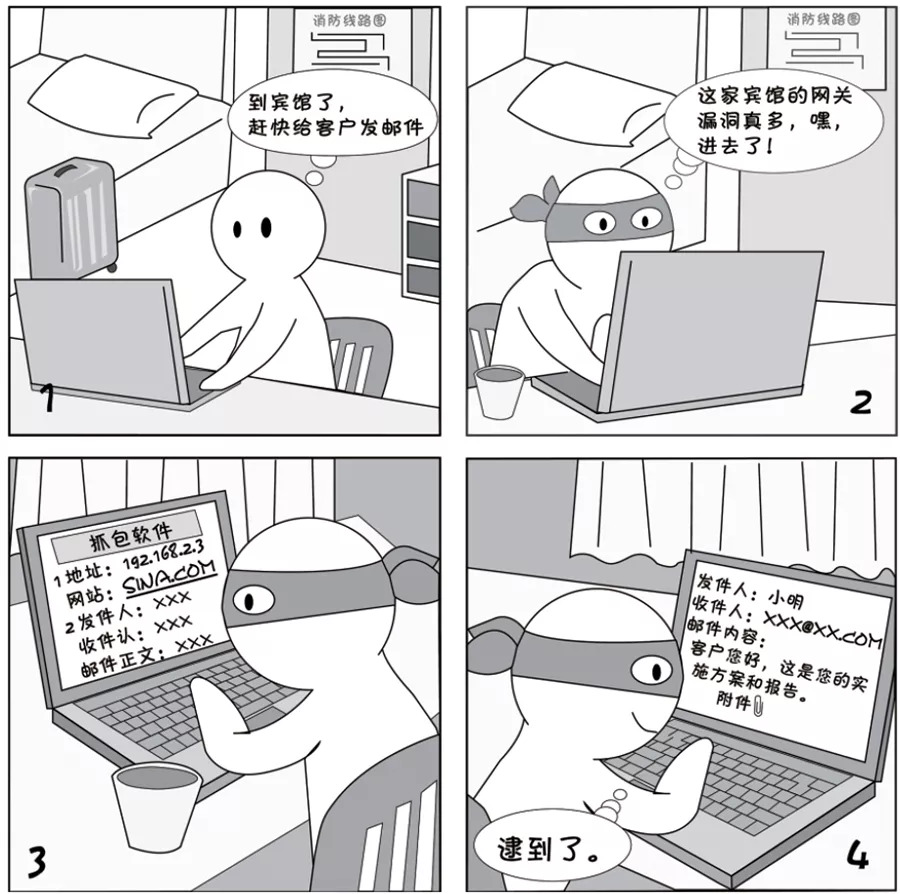
**2018国家网络安全宣传周系列动漫②邮件安全篇**

电子邮件，人们几乎天天发、天天收。网络信息化时代，电子邮件已经成为常用通信工具，而且也成了企业内部主要的沟通工具。

然而，邮件安全问题也日益突出，逐渐成为电信诈骗、勒索软件攻击的重灾区。如何让邮件更安全？下面这组漫画，大家可以学习一下。

* **传输加密**

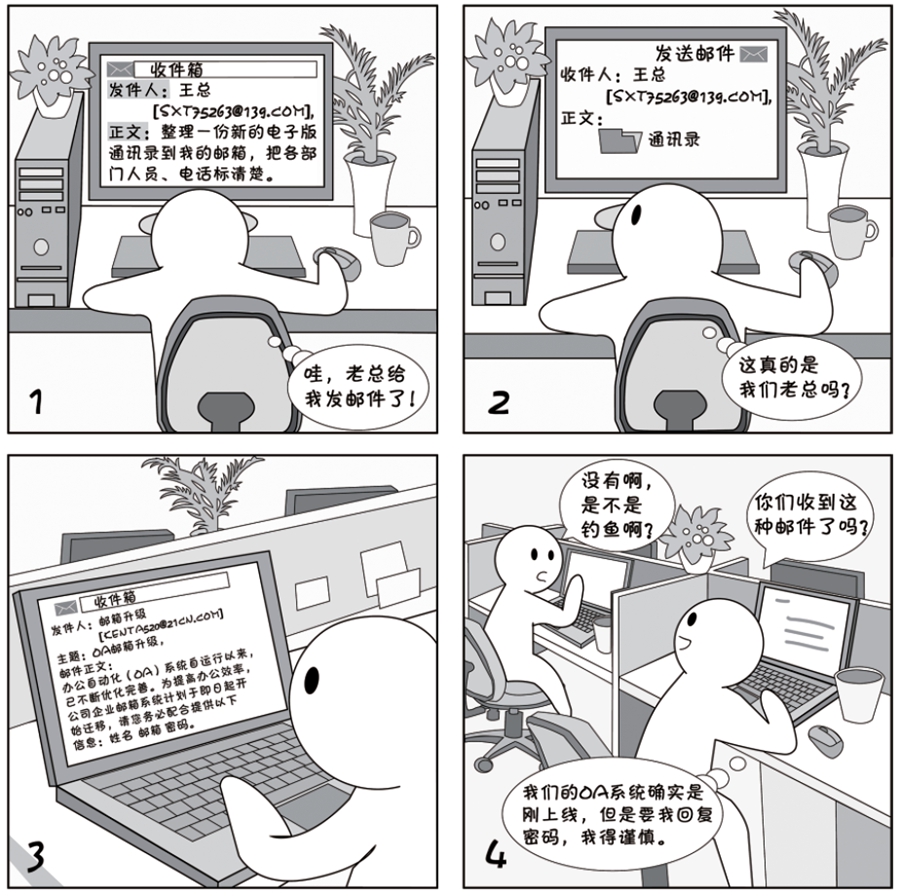


**【现象】**

一些宾馆或公共网络的安全性较差，黑客很容易入侵到其网关设备并监控网络流量，如果收发邮件没有加密，黑客抓到这些数据包后很容易还原出邮件正文和附件。

**【建议】**

* 收发敏感邮件时要确保传输通道是加密的
* WEB邮箱的传输是否加密要看URL（网页地址）是HTTP还是HTTPS，带S说明是加密传输
* 用邮件客户端的加密设置一般为在发送和接收服务器设置处勾选SSL
* **钓鱼附件**

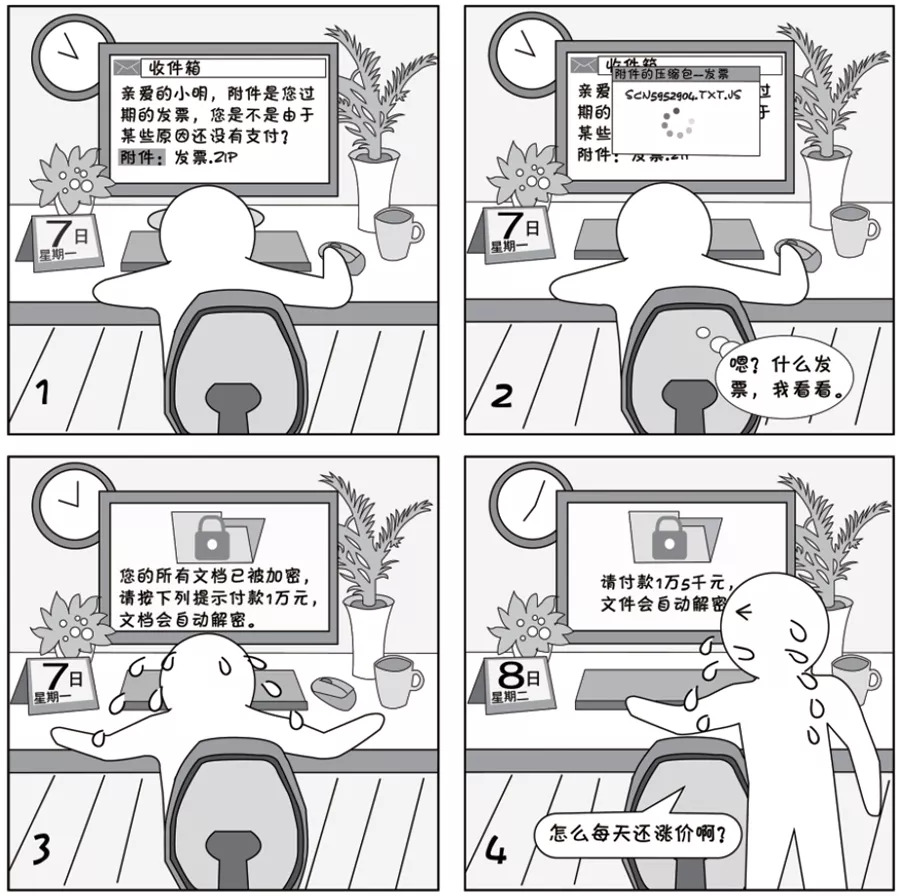


**【现象】**

钓鱼邮件种类繁多，利用邮件骗取回复敏感信息是最简单和常见的钓鱼方式。

**【建议】**

* 望：看邮件发件人地址、签名等信息，是否是你的熟人，是否是系统邮箱，是否是可疑的地址
* 闻：多听周围人的看法，骗子不会骗到所有人
* 问：打电话与相关人员直接确认是最保险的
* 切：懂一些电脑的技术人员可以查一下发件人的真实IP地址、分析一下邮件头内容
* **附件病毒**

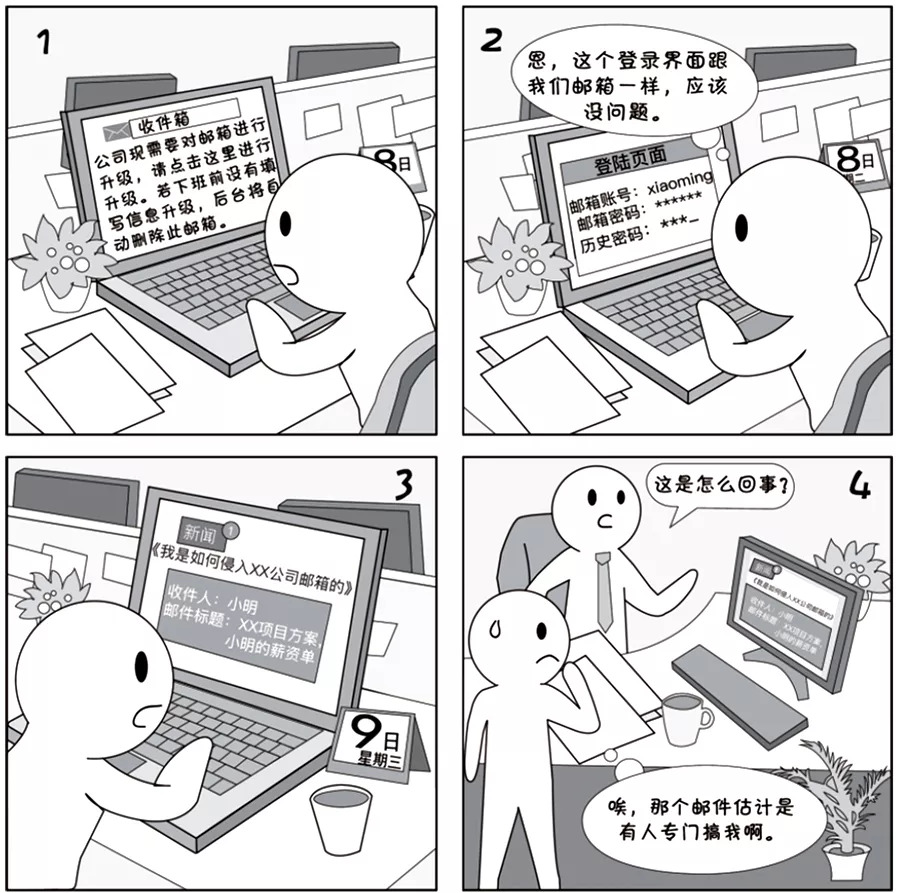


**【现象】**

流行的勒索病毒邮件多为英文邮件，主题和正文诱导用户打开附件。这种病毒对文档的加密强度很高，可以说是无法破解，只有付款才能解密文档。

**【建议】**

* 必须要装但不要完全相信防病毒软件
* 确保自己的邮件客户端禁止访问执行文件，可以自己给自己发一个.exe 后缀的文件测试一下
* 所有类型的文件都可能带病毒，不仅仅是exe/js/bat 为后缀的可执行文件，非可执行文件的利用难度较高，需要利用相关漏洞
* **恶意链接**



**【现象】**

包含链接并链接向钓鱼页面的邮件比较具有迷惑性，因为让受害者看到了与真实登录界面几乎一模一样的网页，受害者就会放低戒心，输入用户名和密码。邮件中的链接也可能直接指向一个挂马页面，打开后直接就会中木马。

**【建议】**

* 遇到索要敏感信息的邮件首先要保持冷静、提高警惕
* 若对邮件所说内容不知情，请勿点击链接，直接电话向发件人确认
* 邮件安全总结



**<邮件安全口诀>**

邮件传输要加密，黑客截获难破译

各种附件谨慎点，可执行文件风险高

默认浏览器非IE，陌生链接勿点击

遇事冷静莫慌张，电话确认是法宝