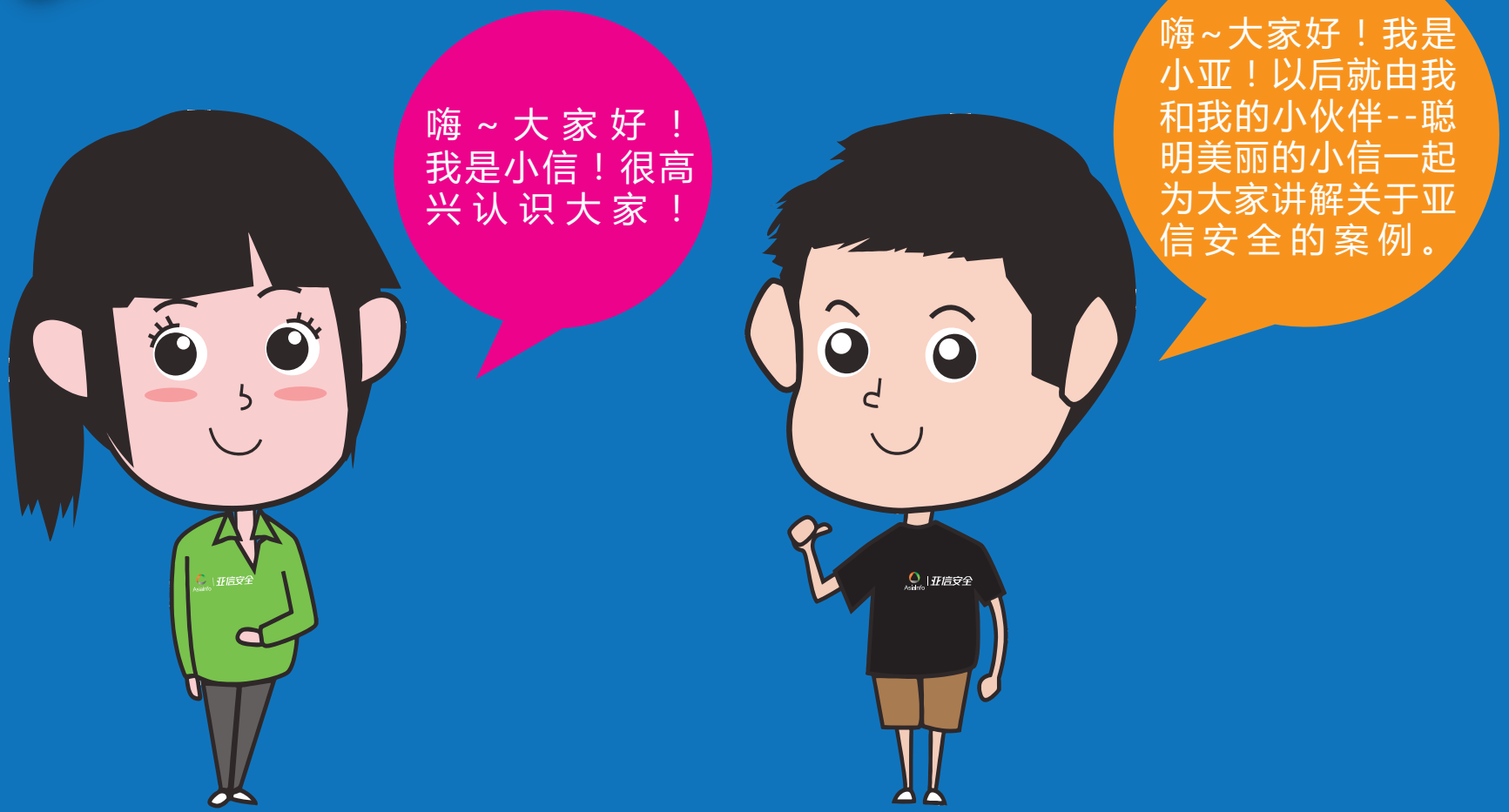
AsiaInfo | 亚信安全

警惕勒索软件已在安卓手机上出现！！

防范手机应用的重要性！



受到勒索软件攻击的国家分布图

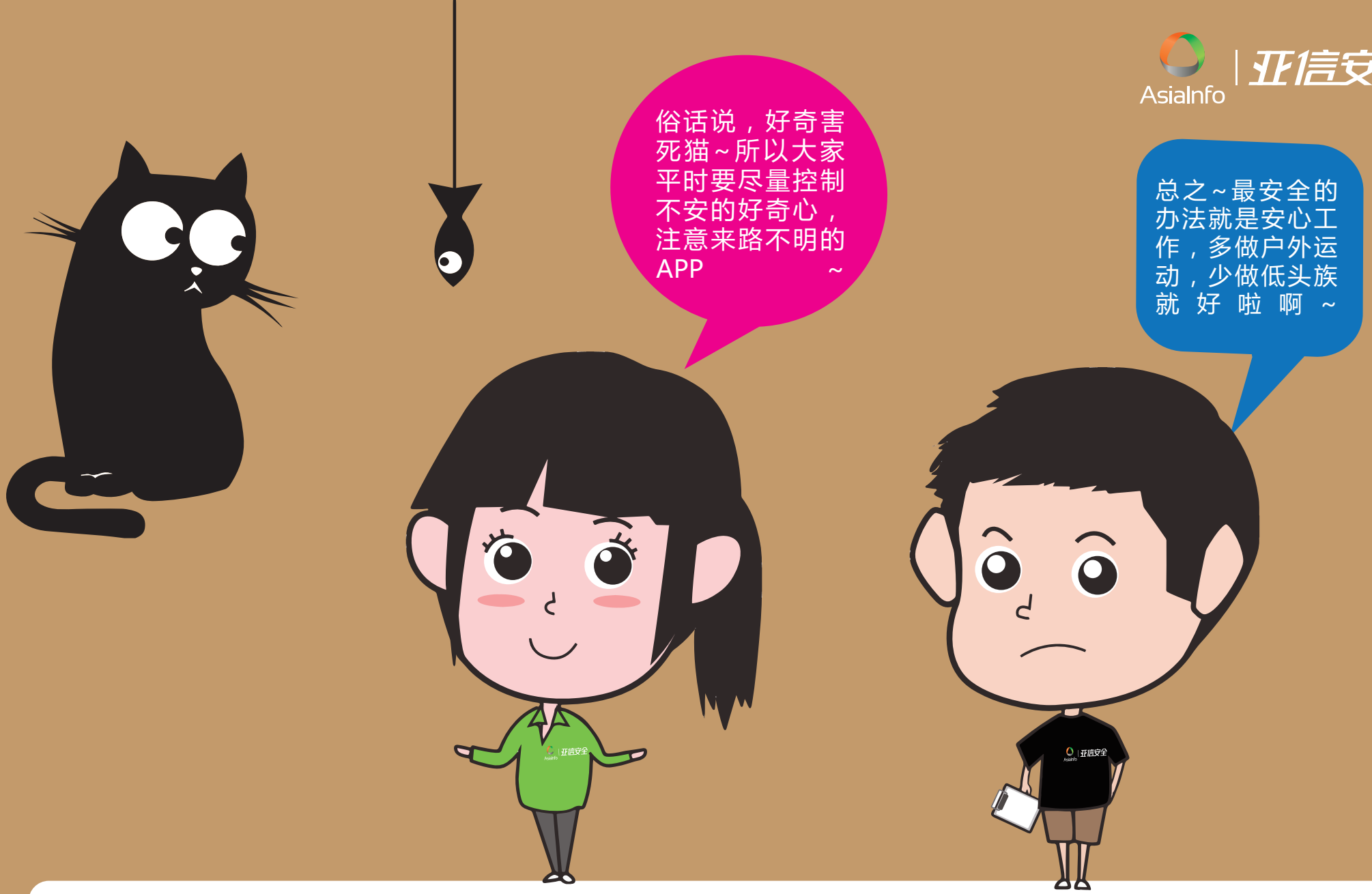
勒索病毒如同瘟疫一样疯狂的向全球蔓延，仅18个月时间，勒索病毒就占据了安全领域的大部分版图，不论是数量还是破坏力都达到了惊人程度。亚信安全研究院调查显示，2016年6月Android勒索病毒威胁比2015年4月增长了15倍！网络犯罪集团现在已把矛头指向另一目标：Android移动端平台。

移动设备勒索病毒如何威胁受害用户？

勒索病毒的可怕之处在于，不管你的台式机还是移动设备只要被它锁住或加密文档，那么你只有向黑客支付赎金的份儿。如果你不照做，犯罪者会将你被感染的文档、照片或视频文件统统删除，严重情况会让你永远无法使用电脑或移动设备。亚信安全研究院在2014年4月首次发现了移动勒索病毒的样本，这种病毒变种体以锁住手机屏幕的方式要挟用户支付赎金，一旦受害者拒不支付，它将完全控制移动设备的执行指令，直接迫使用户购买新的手机。有时它也会冒充监督部门或执法机关，在手机屏幕上显示调查令来逼迫用户缴付“罚款”，总之，越能装饰自身强势身份，黑客就越是乐此不疲，而最终被恐吓勒索的则是那些受骗的用户。

移动设备勒索病毒的扩散根源在哪里？

通常情况下，移动勒索病毒喜欢冒充常用的应用程序、热门游戏、Flash播放程序、视频教程、系统更新程序加载到用户系统里，他们大多来自非官方的APP下载资源中。此外，用手机登陆网站论坛、浏览情色网站或是点击简讯中的垃圾链接都有可能遭到勒索病毒的攻击。



移动设备勒索病毒威胁不断加大，如何有效进行防范？

首先，就像上面提到的情形，不在那些非法的APP平台下载软件，浏览网站时尽量控制自己的好奇心，不点击未知页面或链接，以免涉入感染源。