

# OUCH!

## 本期导读

- 自动填充
- Cc: / Bcc:
- 分发列表
- 情感 & 隐私

## 关于邮件的注意事项

### 概览

电子邮件已经成为我们私人或职业交流的主要手段之一。然而，在使用电子邮件的时候，我们经常可能会成为我们自己的敌人。本期，我们将探讨人们经常邮件使用过程中最容易犯的错误，以及如何日常生活中避免它们。

### 客座编辑

Eric Cole博士 (@drericcole) 是SANS技术研究所的活跃成员，并在SANS与学生们一起工作，参与教学和课件的维护和开发。他是SANS的讲师和课程作者，还是行业内的实践领袖，提供前沿的网络安全咨询。

### 自动填充

自动填充是大多数邮件客户端中的常见功能。当你敲入收件人的名字的时候，你的邮件软件会自动为你选择对方的邮件地址。这样一来，你就不需要记住联系人的地址，只需要记住收件人的姓名就行了。自动填充的问题在于，如果你有些名字相似的联系人的话，那么客户端就很容易选错地址。比如，你想将你所在组织的所有财务信息发送给你的会计同事Fred Smith，自动填充却选择成了你的邻居Fred Johnson。结果是，你把敏感信息发送给了没有得到授权的人。为了防止此类情况发生，在点“发送”前，一定要再检查一下名字和电邮地址。

### Cc / Bcc

大多数邮件客户端除了收件人 (To) 以外还有两个选项，即抄送 (Cc) 和密送 (Bcc)。“Cc”全称为“Carbon copy”，意思是让他人接收副本；“Bcc”代表“Blind carbon copy”，它和“Cc”很像，但是被“Bcc”的人对其他人不可见。这两个选项都可能给你造成麻烦。如果某个人给你发了

## 关于邮件的注意事项

一封附带抄送人的邮件，你就得确定回复的时候是否要回复给包括抄送人在内的所有人。如果你的回复包含敏感信息，一定不要使用“回复全部”这一选项，因为它会把所有人包括进来。关于“Bcc”问题又是另外一回事儿了。在发送敏感邮件的时候，你可能想要给某人密送一份，比如给你的老板。然而，如果你的老板使用了“回复全部”选项，那么所有收件人都会知道，你当初给老板密送了一份。

### 分发列表

分发列表是由单个电邮地址代表的一系列电邮地址，有时也称作邮件列表或群组名。例如，你有一个分发列表，叫做group@example.com，当你像这个地址发送邮件的时候，消息会分发到该群组里面的所有人，数百甚至数千人。当向分发列表发送邮件的时候要格外小心，因为你一下子可能将这条消息发送给了好多人。除此以外，回复某个属于分发列表的邮箱的时候也要十分小心。你或许只是想回复给单个发送者，但是，如果你这时又点了“回复全部”，那么你就将整个分发列表都包括进来了，这意味着即时不是上千也有数百的人现在可能就在阅读你的私人邮件。自动填充要是选择了一个分发列表你就危险了，你原本可能只想发给一个人，比如你的同事Carl (carl@example.com)，但是自动填充可能误认为要将其发送给你订阅的一个关于汽车的分发列表了。

### 情感

当你处于情绪波动的状态时，不要发送邮件。如果你处在一个情绪化状态，那么你发送的邮件可能会在未来给你造成伤害，可能会让你失去一个朋友或者一份工作取而代之的是，花一点时间，冷静地整



邮件没有“撤销”键。不管什么时候，发送邮件前都应该慢下来，检查一下内容和收件人有没有什么问题。

## 关于邮件的注意事项

理一下你的思路。如果你想排遣一下沮丧的心情，确保你没有针对任何人，然后再去以说话的口吻用键盘记录下你的切身感受，给你自己泡杯茶也是不错的选择。当你回来的时候，删除这封邮件，从头再来；或者找个人在电话上聊聊，因为有时候仅凭邮件是很难确定语调和意图的。

### 隐私

最后，记住，传统的电子邮件基本上没有任何隐私保护，任何接触到它的人都可以读到。除此之外，和电话或者个人谈话不同，邮件一旦被发送出去，就脱离了你的控制范围。你的邮件很容易就能被转发给他人，放在公共论坛上，并且甚至可能永远在网上存在下去。如果你有一个特别隐私的事儿要交流，不如拿起电话吧。同样重要的是，在很多国家，电子邮件可以作为法庭证据。最后，如果你用办公电脑发邮件，记住，你的雇主可能有权监控甚至查看你的邮件，这其中可能还包括你的私人邮件，如果你用办公电脑来登录你的个人邮箱账号的话。如果你对公司邮件隐私存疑的话，咨询你的上司。

### 了解更多

订阅OUCH! 安全意识月刊，访问OUCH! 过往存档，了解更多关于SANS安全意识解决方案的信息，请访问：<http://www.securingthehuman.org>

### 相关资源

- OUCH! 邮件钓鱼攻击：<http://www.securingthehuman.org/ouch/2013#february2013>
- OUCH! 钓鱼式攻击：<http://www.securingthehuman.org/ouch/2013#july2013>
- 常见的安全术语：<http://www.securingthehuman.org/resources/security-terms>

OUCH! 由SANS Securing The Human出版，根据 "[知识共享许可协议3.0 \(署名-非商业使用-禁止演绎\)](#)" 发行。你可以在不对其进行修改的前提下，自由传播这份新闻简报或在你的安全意识课程中使用它。了解翻译或更多信息，请联系：[ouch@securingthehuman.org](mailto:ouch@securingthehuman.org)。

编委：Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis

翻译：成自豪