网络钓鱼安全提示

保障您自己以及其他人免受网络钓鱼攻击，避免对其他人构成意想不到的伤害。如下建议可以帮助您识别并避免钓鱼邮件的陷阱。

您应该做些什么

- 只在您知晓来源以及是在您预料之中的情况下打开附件。
  - 若是在您的预料之中的话，请在打开前先联络相关机构以及验证邮件。
- 若邮件内容通过可怕的后果来诱导您点击链接，您可通过不同的渠道对它进行验证。
- 在点击任何链接前，将鼠标停留在链接上以及阅读完整的网址以便检验该链接是否是真实的。
- 将链接直接输入游览器而不是点击它们。
- 虽然邮件是来自一位所认识的人，也要验证可疑邮件的发送者。
  - 此类邮件的邮件域很可能不是真实的。

您应该避免做些什么

- 避免打开拥有附件，可点击链接的未知邮件，奖励邮件，恐吓邮件以及威胁邮件。
  - 越吸引人的奖励 = 攻击的机率越高。
  - 忽略此类邮件，除非获得奖励是您预料之内。
- 避免游览看起来可疑的网站。
- 不要蓄意使用，散布或创建病毒，蠕虫或其他恶意软件。
- 不要中断或改变您的电脑/手提电脑所安排好自动病毒扫描的设置。

- 对于那些显示需要紧急或立即行动的未知邮件保持警惕。
  - 与IT 团队/安全团队验证此类邮件。
- 寻找是否有以下的问题：
  - 不良的邮件格式
  - 模糊的标志/横幅
  - 不良的拼写/语法
  - 一般的问候/信息

- 避免将个人资料或者与ABI相关的敏感资料分享至邮件或者网上表格中。
- 避免打开已经标志为垃圾邮件的邮件。
  - ABI拥有过滤以及将邮件标志为垃圾邮件的工具。

记得及时报告以下事项：

- 可疑邮件
- 病毒/恶意软件事件

经常报告任何此类网络钓鱼活动至

soc-support@ab-inbev.com