《邮件安全须知》

如有发现有异常登录或者发信的账号，建议立即将其进行锁定或者让其尽快修改密码，并即刻查看和修改相关配置，参考如下：

1、在确认邮箱被盗的情况下，建议开启二次验证和客户端专用密码。开启二次验证功能后，网页版登录邮箱需要使用**对应的设备验证才**能进行授权登录上去，如果您认为频繁授权太麻烦，您可以在授权时选择信任设备。第三方客户端（例如 outlook、foxmail）等软件登录邮箱使用使用客户专用密码进行登录，客户端专用密码是在网页版随机生成的 16 位密码，只在生成时可见。建议您需要设置第三方客户端时在登录网页版进行生成，生成后复制到第三方客户端，不要保留在本地。
2、建议检查个人设置》邮件分类》来信分类中是否存在非本人设置的自动转发，以免后续邮件被泄露。
3、建议检查个人设置》收发信设置》自动转发中是否存在非本人设置的自动转发，以免后续邮件被泄露。
4、建议检查个人设置》高级功能》共享邮箱是否存在非本人设置的共享账号，以免后续邮件被泄露。
5、您可以在管理员后台》用户管理点击对应用户》ip 绑定中绑定用户登录 ip，其他 ip 将无法登录该账号或者在管理后台》安全管理》登录限制策略中对域内邮箱批量限制 ip 登录
6、建议电脑杀毒后再修改邮箱密码，以免由于电脑中毒导致密码泄露

开启二次验证后就算您的密码被泄露，那么别人登录您的邮箱同样需要经过您绑定的论客 APP 授权或者短信验证码才能成功登录上去，开启二次验证功能步骤如下：
1、管理员开启二次验证功能设置权限
路径：管理员后台》安全管理》密码策略》将当登录或信息修改时选择为用户自定义

2、用户登录网页版邮箱，将账号绑定论客 APP 或者短信验证
路径：个人设置》安全设置》二次验证设置》选择 APP 授权或者短信验证，进行绑定即可

另附【如何安全使用邮箱】：

1、将邮箱密码设定为高强度密码，即字母加数字组合，10 位以上的密码。（不要使用 123456 等密码，可使用形如：xom23qy5bi1x5 这种随机的数字字母密码）；
2、立即对此邮箱所使用的机器进行全面杀毒。
3、不要在 WEB 页面上保留邮箱的密码。
4、每天请登陆到 webmail，点击"自助查询"-"登陆查询" 看看有没有异常 ip 成功登录过邮箱的记录，如果有登录成功的记录，说明密码已经泄露了，一定要及时修改，同时在修改好密码后，观察下是否还有被成功登录的记录，如果有观察下登录成功前的错误次数，如果登录失败很多次后登录成功，多说明是通过暴力

破解的，请设定密码时一定使用高强度密码；如果登录失败次数很少就又成功登录您的邮箱，那么说明您的电脑很可能是中毒了，一定要杀毒。
关于如何查询自己的公网 IP，可以登录 www.ip138.com，可以自动帮您检测。
5、如有需要，建议可以开通 IP 登录限制，登陆邮箱管理员后台—安全管理——IP 登陆限制下可以设置，可以设置允许登陆的 IP，亦可以将 IP 列入黑名单。
6、密码过期功能，定期修改密码。 登录到 webmail—设置—密码—密码有效期；
7、设置组织密码强度检查，联系渠道开通组织策略和组织参数设置后，客户在管理员后台—系统管理—组织设定下可以设置。
8、开通自动转发提醒，联系渠道开通组织策略和组织参数设置即可。
9，系统有防猜策略，同一 IP 下，如果一个账号 10 分钟内密码错误次数超过 10 次，系统会自动挂起该 IP 的登录

10，如有使用客户端(如 outlook\foxmail 等)，可登录网页邮箱在设置中心—账号信息，开启客户端专用密码，专用密码是自动生成的，强度级别高。
11，绑定安全登录二次验证在手机。路径：设置中心—安全登录二次验证。

——