如何才能识别钓鱼邮件，从而加强安全防护：

请牢记任何一封询问你账号密码，跳转外部链接的都是钓鱼邮件，都是不可信的，请立刻举报它为垃圾邮件后删除！并且不要点击邮件中的任何链接及附件！

骗子惯用的钓鱼邮件招数：

1、盗用官网图片，伪造知名域名或公司域名，甚至完全盗用官网或用户常用联系人的特定信息，仿冒可信邮件。提供一个虚假的理由诱导用户提交邮箱账号和密码或诱导用户支付，邮件通常包含某个理由。

例如：

“ 我们正在更新升级邮箱账号中心。 ”

“ 我们正在删除不活跃用户 ”

“ 订单款项已打入你的支付宝账号，请进入查收 ”

“ 我的汇款账号已更新，请将款项打入我的新账号中 ”

“ 邮箱密码到期通知 ”

“ 警报：存储空间不足 ”

2、邮件的主题会吸引用户的注意力，而且通常都显得急迫，非常可怕或非常诱人

以下是一些常见的例子：

“ 邮件账号异常使用警报！请立即进入检查 ”

“ 账号检测到安全隐患 “ 或者 “ 需要核实您的信息否则账号将被关闭！！！！ ”

“ 您参加的双11购物狂欢节，中奖一部iphone6请提交个人信息，以便邮寄奖品 ”

“ 通知各部门 ”

3、伪装发件人、伪装可信的链接地址是骗子最常用的方式，请一定细心检查。

乍一看，用户像是收到了可信用户或可信网站的官方邮件，但是如果仔细检查发件地址，或通过查看邮件原文就知道它是假的。通常，骗子们只是使用某个相似的邮件账号假冒来发送邮件。或者使用非常类似的

链接地址骗取收件人点击。

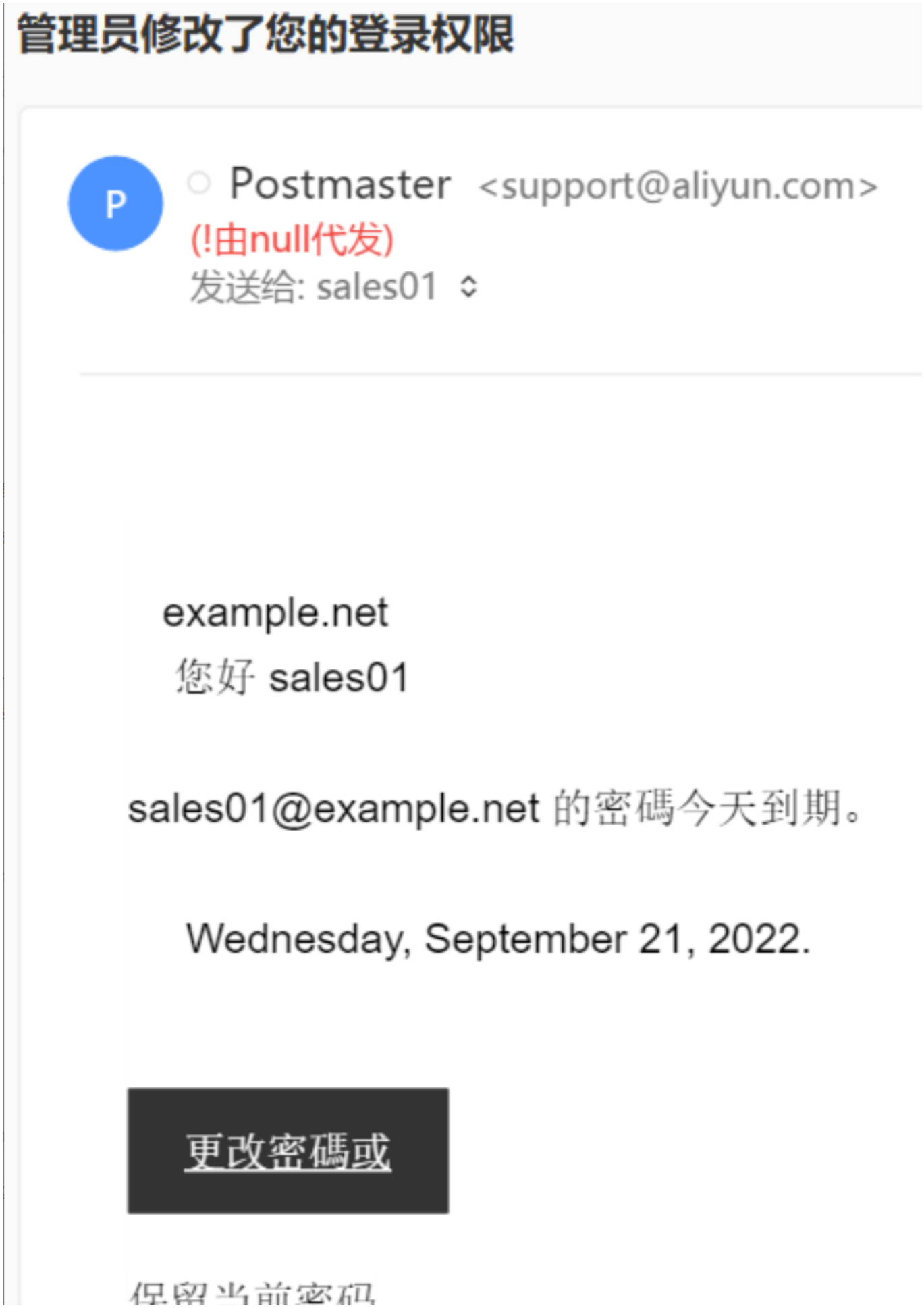
例如：

您的客户邮箱是hellenliu@ali.com□骗子伪装的发件人是helleneliu@all.com□

可信官方网站的服务地址是http://taobao.com/，邮件中连接实际上是http://taoboa.com/*□

“ 管理员修改了您的登录权限 ”

Last update: 2023/11/15 09:55	邮箱小知识:钓鱼邮件防护安全指南	http://wiki.chicmax.net/doku.php?id=%E9%82%AE%E7%AE%B1%E5%B0%8F%E7%9F%A5%E8%AF%86:%E9%92%93%E9%B1%BC%E9%82%AE%E4%BB%B6%E9%98%B2%E6%8A%A4%E5%AE%89%E5%85%A8%E6%8C%87%E5%8D%97


管理员修改了您的登录权限
P
Postmaster <support@aliyun.com>
(!由null代发)
发送给: sales01
example.net
您好 sales01
sales01@example.net 的密碼今天到期。
Wednesday, September 21, 2022.
更改密碼或
保留当前密码

4、通过邮件附件诱骗。

骗子通过邮件诱骗你点击下载附件。它可能是侦查软件或木马病毒，一旦你点击下载该附件，欺诈者可以盗取你的密码，并控制你的邮箱。虽然我们的邮箱系统已经提供了附件病毒扫描功能，但是仍难免有漏网之鱼，仍请你切记勿随意点击附件下载。

“重要通知”

5、诈骗邮件中通常将你称作是“尊敬的客户”或“尊敬的用户”，而不是你的真实姓名，通过此项可以简单排查可疑的钓鱼邮件。

6、邮件内容中附带图片伪装无法显示，诱使用户点击，误导用户提交账户密码

以下这些方法可以帮助你保护账号安全，预防账号密码被盗：

1. 任何邮件向你索要账号密码信息，都请立即举报删除。

2. 如果你想要证实邮件的真实性，请手动输入这家公司的URL而不是点击邮件中嵌入的链接。

3. 不要使用简单的密码，增加密码复杂性，养成定期更换密码的习惯。

4. 备用几套常用密码，不要在各种网络服务中使用相同的密码。

5. 不让PC自动“保存账号密码“，尤其在公共场所（网吧、酒店等）。

6. 不随意在第三方网站输入你的邮箱账户账号和密码，提高防范意识。

7. 实在无法确认的邮件，直接联系信息部进行确认。

8. 即便是个人电脑，也要定期在所有已登录站点手动强制注销进行安全退出。

9. 建议启用邮箱登录二次认证以及标准客户端专属密码，防止账户密码泄露被不法分子利用。

任何技术手段都无法100%杜绝钓鱼邮件的产生，开展组织内用户的岗前和定期培训，以及垃圾邮件发送演练，有利于员工增强识别防范意识，防范于未然。