

# 钓鱼邮件自卫指南

## 识别与报告钓鱼邮件指南

钓鱼邮件会伪装成银行、社交网站、朋友甚至是老板的消息。它们看起来合法无害，但通常包含可以证明其恶意性质的线索

如果您收到一封可能存在钓鱼迹象的电子邮件，或者只是觉得不对劲，请不要犹豫，立刻向您的 IT 和安全部门报告。他们会非常高兴在钓鱼邮件产生实际损失前阻止欺诈行为

### 永远不要

点击可疑电子邮件中的链接，按钮或图标。它可能会诱导您到看起来合法却是精心布置的恶意网站  
打开附件，除非你真的知道里面是什么，否则其中可能包含恶意软件  
“确认”或“验证”密码，帐号，社会安全号码，出生日期或任何其他机密信息

### 始终要

忽略可疑电子邮件中的链接。打开浏览器，搜索发送该邮件的组织/公司，并查看与电子邮件中的信息是否一致  
立即报告一封疑似钓鱼的电子邮件，或者只是觉得某封邮件不对劲也要立刻报告

联系人的名字或电子邮件地址不熟悉，或者公司并非合作的公司

发送和回复的地址不同

截止日期、感叹号、全部大写

带有可疑的、意料之外的附件

尴尬的措辞与拼写错误

要求输入个人或凭据信息（如密码）

伪装的链接或与将鼠标悬停在其上时显示的 URL 不匹配的链接

From: KeyserSoze@MegalithBankSecurity.com

Reply to: Security@MeglithBank.com

ACTION REQUIRED: VERIFY YOUR TRANSACTIONS IMMEDIATELY!

Suspect\_Transactions.zip

Dear Client: The Megalith Bank security team has detected a problem with transactions in account 8793004-8816. A pattern of unusual withdrawals were made in the past 24 hours. Please open the attached document for a list of the suspect transactions.

ALERT! We encourage you to immediately click on the secure URL below, enter your username and account password, and confirm or challenge these transactions.

<https://www.MegalithBank.com/security/login.html>

If you do not take immediate action, we may be forced to suspend all withdrawals from this account until these issues are resolved.

Sincerely,

Account Security Team, Megalith Bank