

银发族S.U.R.E.技能系列

工作坊二：如何查证电邮和信息的真伪

叶若诗

外展服务馆员
国家图书馆管理局



工作坊大纲

- S.U.R.E.是什么?
- 钓鱼电邮
- 如何辨识钓鱼电邮
- 可疑信息
- 如何辨识可疑信息
- 如何查证可疑信息
- 总结

S.U.R.E.是什么?

S.U.R.E.是什么?

- 请点击下面的链接以了解更多S.U.R.E.的详情!

<https://sure.nlb.gov.sg/blog/seniors/sn0022>

钓鱼电邮

如何辨识钓鱼电邮

如何辨识钓鱼电邮

1. 钓鱼电邮通常看起来是由知名企业或机构发送的，例如银行、网上节目提供商、手机服务提供商、网上购物平台、网上付款平台、社交软件网站等
2. 钓鱼电邮通常会利用一个虚构的原因，要求收信者点击一个链接，然后连接到企业或机构的网站，然后在网站上输入自己的个人资料或敏感资讯。钓鱼电邮也可能指示收信者下载电邮中的附件，一旦收信者点开附件，里头的恶意软件便会下载到收信者的电脑系统里
3. 钓鱼电邮通常都会以胁迫的语气要求收信者迅速点击链接，或下载附件
4. 钓鱼电邮的行文通常都有文法，或英文拼字上的多个错误；语气也显得煽情夸张；或者内容缺乏连贯性，这些都是钓鱼电邮的迹象。因为真正由企业或机构发送的正规电邮一般行文流畅、文法和拼字正确、前后连贯，并且语气严肃诚恳

收到钓鱼电邮该怎么办

1. 不要回复、不要点击任何链接或图像、不要下载并点开任何附件、绝对不能提供个人资料或敏感资讯，例如用户名和密码、银行账号、信用卡号等。最好立刻删掉
2. 如果您想到企业或银行的网站查询，应该打开网页浏览器，在上头的网址栏里输入网址。不要点击可疑电邮里的任何链接，因为它们极可能把你连接到钓鱼网站
3. 如果您不肯定是否收到钓鱼电邮，可以拨打能信赖的电话号码到银行或机构查询，例如从银行的纸本来信，或网站上获取的电话号码。不要拨打可疑电邮里的任何联系号码。您也可以到搜索网站上查看有没有类似内容的钓鱼电邮已经被举报了
4. 向被冒充的企业/银行，或执法机构检举该钓鱼电邮。您也应该给自己的电脑系统安装防毒软件，并且定期更新，这样系统才能更有效地过滤附有恶意软件的电邮

可疑信息

可疑信息的特征

1. 内容笼统简略，缺乏细节
2. 利用煽动性字眼、偏见或刻板印象来扭曲事实
3. 耸人听闻，以刺激收信人动指转发，散播开来

如何辨识可疑信息

如何辨识可疑信息

1. 查实该则信息的可靠性

- 这则信息是否来自一个可信的源头？
- 信息的作者是这个课题的专家或权威吗？
- 搜索主流信息来源，如报章、电视和电台，对所质疑的信息进行多方查证
- 如果您不肯定，请向家人询问

如何辨识可疑信息

2. 查看信息是否带有可疑迹象

- 所引用的网址是错误的
- 语句所使用的文法或英文拼字错误百出
- 所提到的事件或涉事人物、时间和地点都很简略笼统，缺乏细节
- 内容煽情、形容夸张——所提出的计划、价格等，往往优惠得令人不敢置信

收到可疑信息该怎么办

1. 在点击“分享”按钮把信息转发出去之前，请先想一想

- 请勿在一知半解的情况下，随意转发，让不实信息散播开来

2. 成为打击不实信息的一份子

- 通知不实信息的转发者该则信息是虚假的；您也可以向被冒充的企业或执法机构检举该则不实信息正在网上或社交群组间流传

如何查证可疑信息

如何查证可疑信息

- **使用信息查证网站**

例如：

1. Black Dot Research (<https://blackdotresearch.sg/factcheck/articles/>)
2. Factually (<https://www.gov.sg/factually>)

- **查找多个新闻资讯管道**

看看其他主流的新闻资讯管道是否也报道了同一则信息。如果没有，那这则信息很有可能是虚构的

例如：

1. 国家图书馆管理局的电子报网站 (<https://eresources.nlb.gov.sg>)
2. Google新闻 (<https://news.google.com.sg>)

总结

- 注意电邮的地址和链接的网址是否与发送电邮的企业、银行、机构等相符合
- 注意电邮或信息的文法和英文拼字是否错误百出，语气是否煽情夸张，或带胁迫性，以及前后文是否连贯
- 搜索主流信息来源，对所质疑的信息进行多方查证
- 向被冒充的企业，或执法机构检举钓鱼电邮，或不实信息
- 在转发前请先利用S.U.R.E.的四个步骤查证信息



网址: sure.nlb.gov.sg
电邮: sure@nlb.gov.sg

感谢您的阅览

