

# 網絡意識





## 前言和致謝

現代資訊技術給21世紀的生活帶來超常便利的同時，其迅速發展的緊密連接也有其至暗的一面。

我們所有人都對現代資訊技術的黑暗面有所瞭解。事實上我們中的一些人，儘管出發點是好的，但也曾淪為那些狡猾線民的獵物，那些人意圖欺騙我們，或者破壞我們的事務，不論是什麼動機促使他們這樣做。

近年來，船舶經營中網路意識的需求越來越成為行業的焦點。該焦點必然反應了船舶以及用於操縱船舶的電子系統的日益增長的技術複雜性。複雜性的提高經常-但不是總是一意味著出現差錯的可能性也擴大，尤其是如果出現問題的系統人機界面不能應對維護誠信的需要。

因此，儘管船舶管理中船舶技術自動化的程度越來越高，不論在海上還是在陸上，但是人的因素仍然是保證資訊技術系統的可靠性以及保護IT系統不遭受外部操控和破壞的關鍵因素。

正如序言中提到的，自2021年1月1日起，網路安全的重要性將通過ISM規則的發證要求得到承認，規則將考慮網路風險管理。許多實際問題將與船員的網路意識，以及他們在船期間使用IT系統進行交流或者其他活動的能力有關。

在這種背景下，我們希望本篇《網路意識》可以以一種通俗易懂而令人難忘的形式，幫助我們的會員以及會員的雇員掌握一些實用技巧，規避因網路安全環境和船舶在網路方面的弱點對船舶造成的各種風險，保障船舶安全。

非常感謝Dr. William Moore, Ms. Danielle Centeno以及Shipowners Claims Bureau, Inc.的IT團隊，感謝他們以獨特的熱情和活力推動美國保賠協會的這一最新舉措。同樣感謝Mr. John Steventon，他的藝術才華與他捕捉圖像中複雜想法的能力相匹配，這些想法因其巧妙的圖形表達而可以理解。

Joseph E. M. Hughes  
主席&首席執行官  
Shipowners Claims Bureau, Inc.  
Managers of the American Club



## 序言

網路意識的主要受眾是海員。存在常見且基本的維護海員個人設備以及船上系統網路安全的最佳做法。這些常見的最佳做法中，許多不僅適用於家中，也同樣適用於船上。

海員必須形成一定的網路風險和謹慎意識，這對他們的個人生活和職業生活都至關重要。雖然2017年的國際海事組織決議儘“鼓勵”網絡風險管理應當符合規定，但是也要理解網絡安全對於每一項業務以及海事資產和運營的安全、完整性和可靠性都至關重要。在實踐中，這意味著公司必須對其資訊技術系統環境（包括用於操作船舶的系統）進行風險評估，並發佈程式來管理所有網路安全風險，包括那些影響船舶海員的網路安全風險。

與外部世界，特別是與朋友和家人的溝通和社會交流對於現代海員來說是司空見慣的。從人的角度來看，他們的網路健康是整體健康和個人健康的關鍵組成部分。不過需要重點理解的是，保護自己並確保船舶安全的責任不受損害。這些共同目標是通過採取良好的個人網路安全做法來實現的。我們希望海員能夠從網路意識中獲得有用的資訊，以提醒他們能簡單做到保護自己和船舶安全。

William H. Moore, Dr. Eng.

高級副總裁

Shipowners Claims Bureau, Inc., Managers

American Steamship Owners Mutual Protection & Indemnity  
Association, Inc.

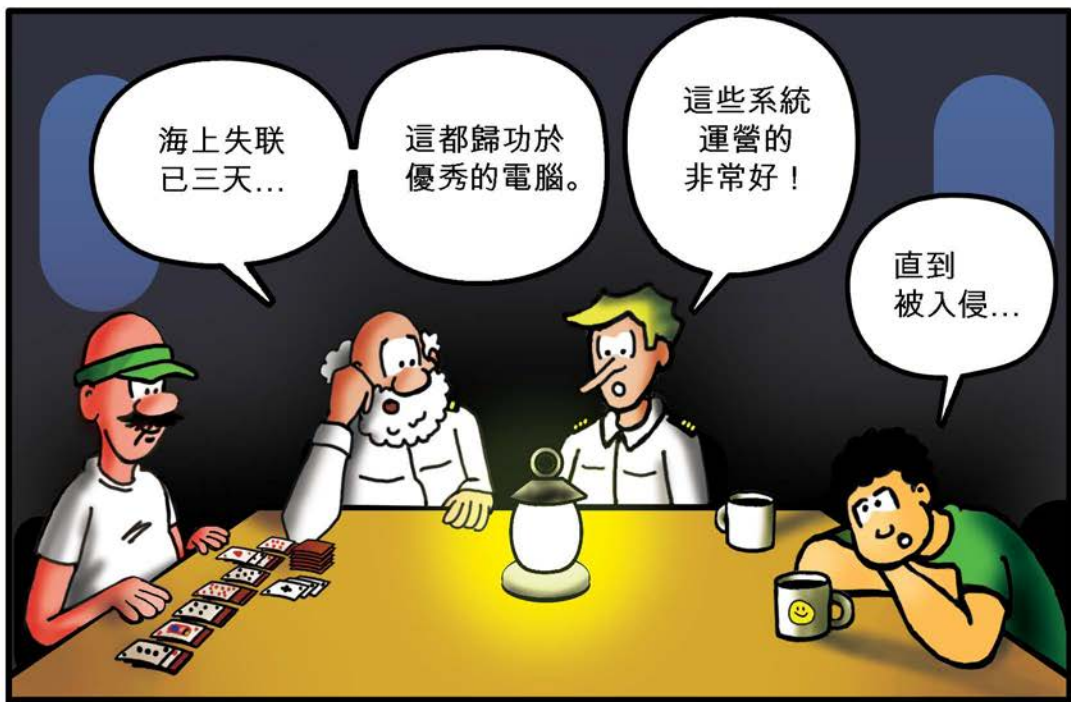
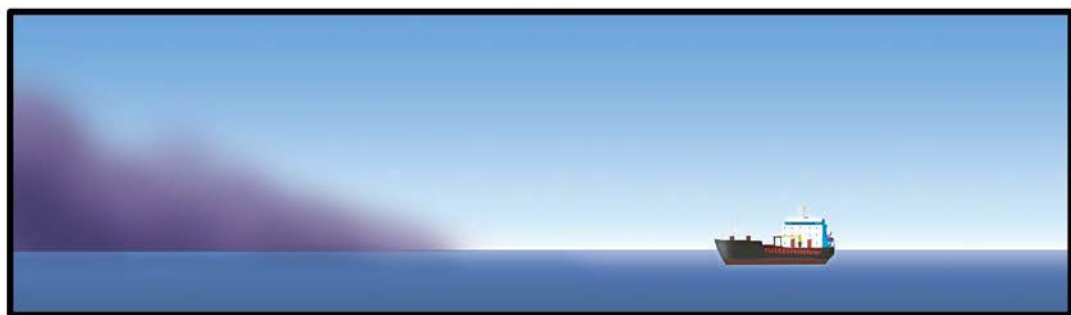
Ms. Danielle Centeno

副總裁助理

Shipowners Claims Bureau, Inc., Managers

American Steamship Owners Mutual Protection & Indemnity  
Association, Inc.

# 網絡意識



兩周後...

## 網絡安全風險評估

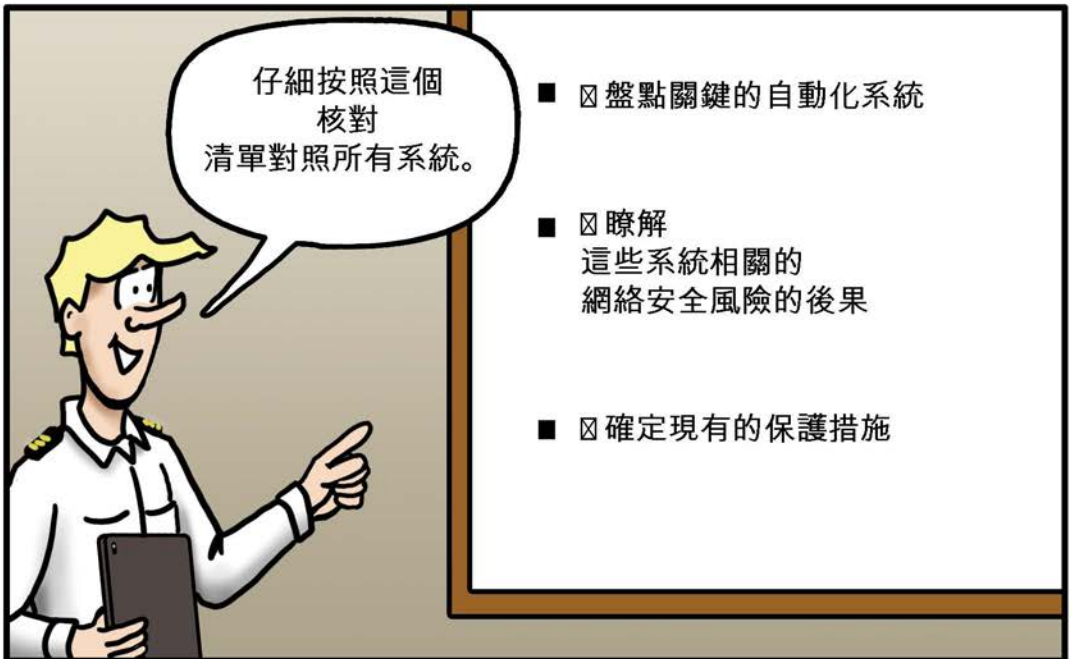


## 識別關鍵系統

### 考慮網橋系統



網橋有很多系統，有些針對解決外部干涉很有幫助。



# 識別關鍵系統

## 推進及機器系統



## 甚至貨物管理系統



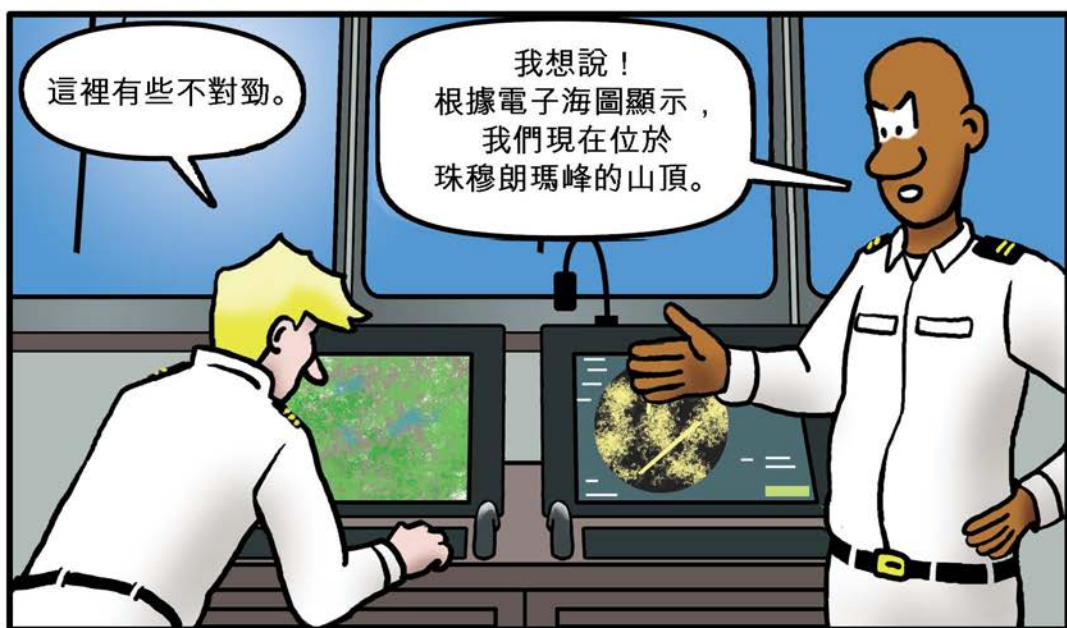


# 識別關鍵系統

## 通訊及警報系統



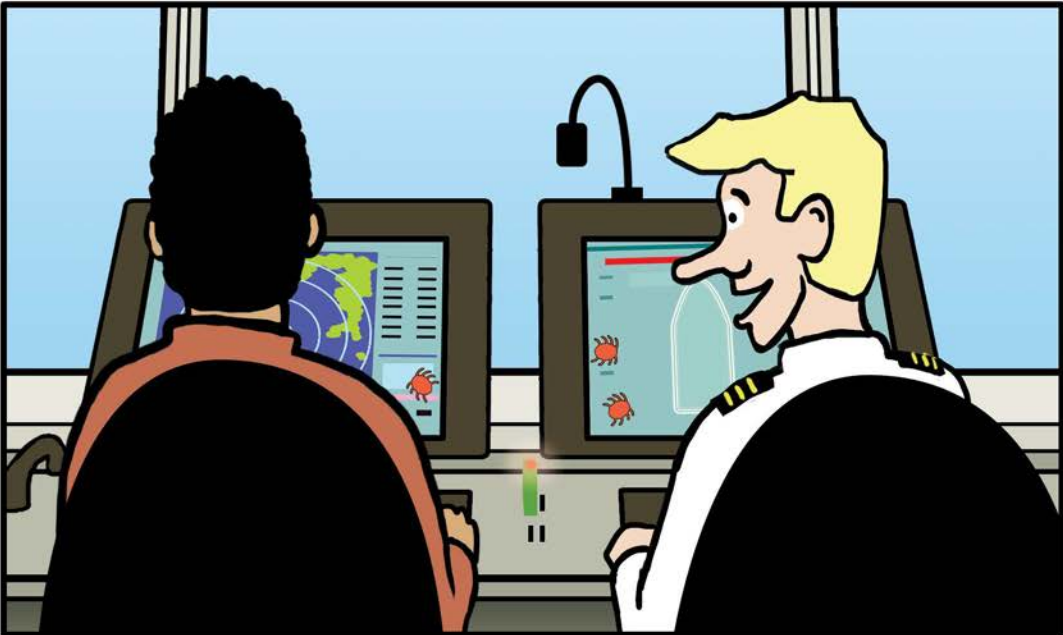
我們提到全球定位系統了麼？



確定了一個關鍵系統，我們就需要去尋找潛在的風險。

# 識別風險

這些是內部風險，通常由人為失誤、過失或缺少相關意識造成。



以及很多外部風險，比如由激進、犯罪和臨時起意造成。

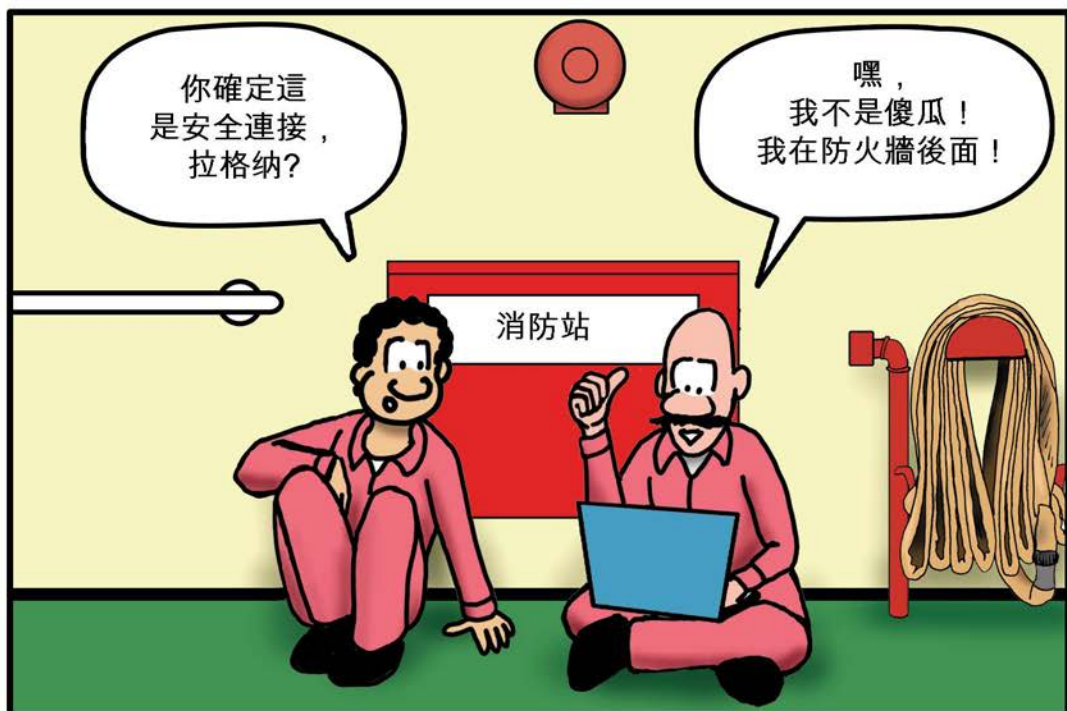
# 威脅者

這些團體會威脅船舶的安全。



## 識別漏洞

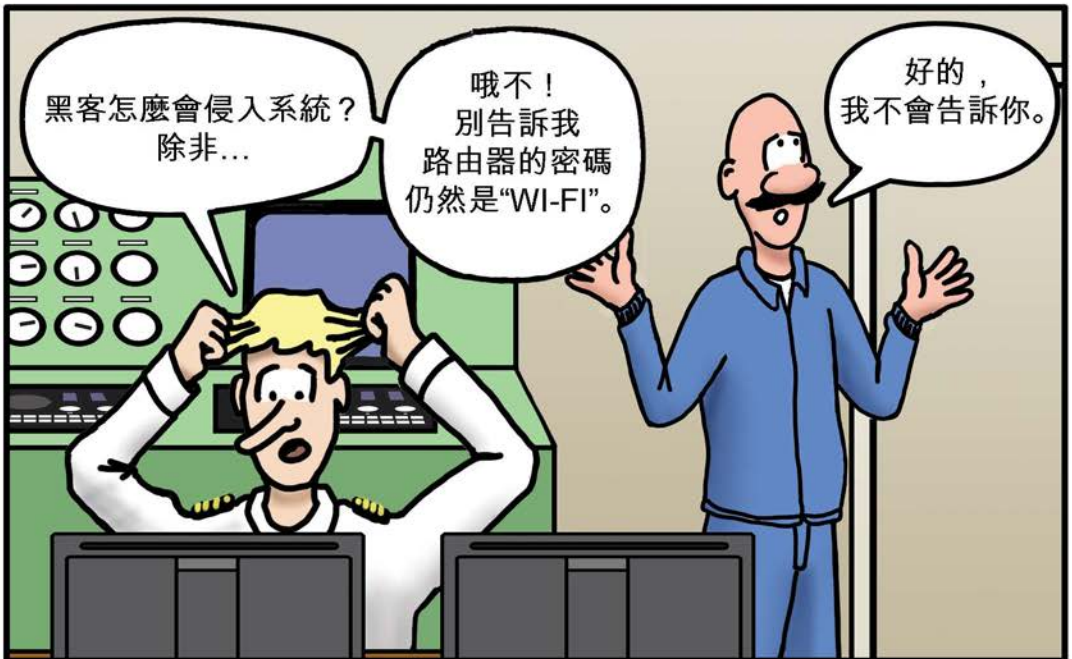
### 識別已經存在的控件



常見的網絡漏洞可能包括舊的操作系統，  
缺少或過時的殺毒軟件和未打補丁的資訊技術系統。



常見的錯誤可能會涉及未更改或未公開的存儲密碼。



審查所有船員的做法可以避免很多預期問題。

## 電子通訊：最好的實踐

和乔治一樣，務必謹慎。



使用長密碼。  
密碼應為14位以上，  
包括至少一個數字，  
一個大寫字母和一個符號  
( 比如，\$, @, ?, # )



只有受信賴的供應商提供的  
個人設備和USB驅動器  
才可以上船。



在個人設備上安裝、  
註冊和更新殺毒軟件、  
防間諜軟件和防火牆軟件包。

## 別和拉格納一樣粗心



對外部下載和電子郵件持懷疑態度。  
驗證非預期郵件的真實性。  
特別是那些帶有附件或連接的郵件。



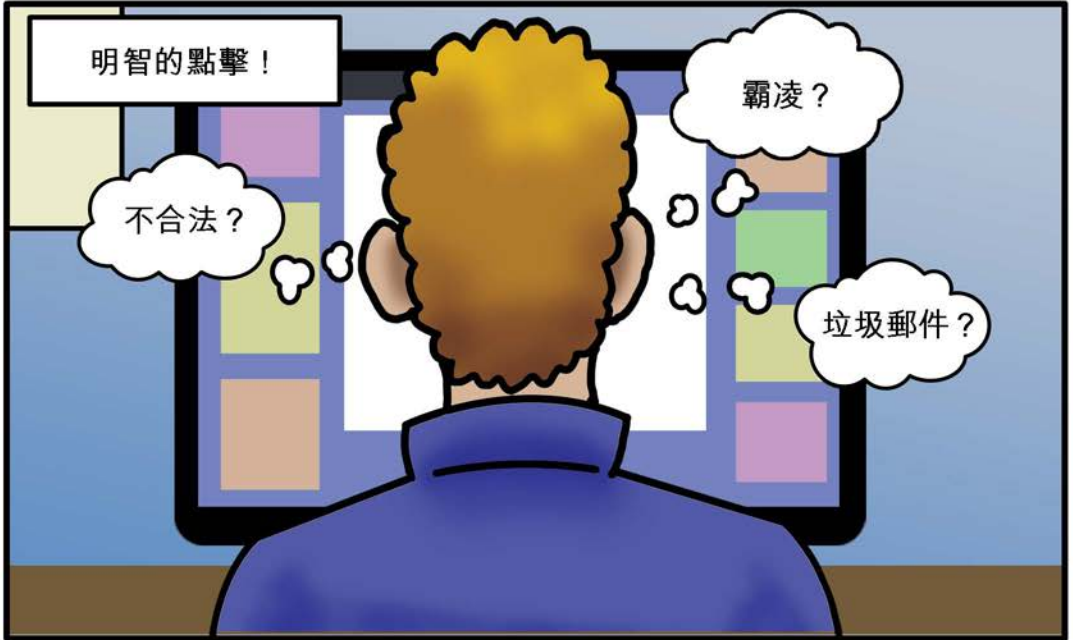
在船舶無人看管的時候，  
個人和船用設備都必須鎖屏。



僅使用您公司獨用的，  
加密且安全的WIFI。

## 網絡健康注意事項

網絡健康代表積極的幸福感，負責任的行為以及互聯網用戶的良好選擇。



謹慎對待你在網上遇到和信任的人！  
試圖欺詐的人可能會用你的銀行帳戶信息、  
信用卡信息或身份證號碼來竊取你的信息。





存在與網路連接有關的個人風險因素，  
包括移動設備的不當使用和過度使用...



保持你在社交媒體上的記錄和行為積極且專業，  
尤其是與工作有關的內容！






保持對說明如何正確使用系統的網路安全程序  
以及他們的維護程序的更新及現成可用



程式還應確定組織內部以及在每個服務提供者辦公室內部網路安全聯絡人。

**聯絡人**

		
<p>Carrie Lotsastuff Cargo Systems Carrie@Cargos_R_us.com 1-800- CAR RYIT</p>	<p>Iona Lotaboats Navigation Equipment IL@navequipteam.com 1-800-NAV TEAM</p>	<p>Loudon Cleer Auto Alarms Loudon@AlarmMe.com 1-800-ALA RMME</p>

## 勒索軟體的威脅

勒索軟體是一種被設計用來加密您的檔或者將您的電腦完全鎖起來，直至您支付一定數額的費用的惡意軟體。



勒索軟體一般通過陷阱連結或者郵件附件傳播。

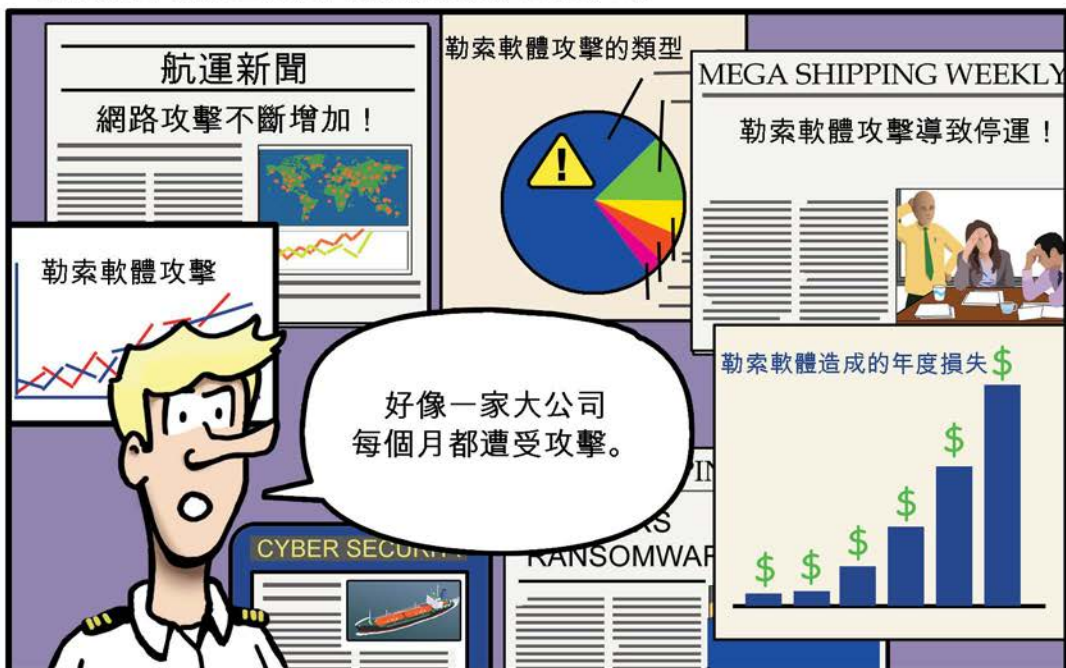


勒索軟體是一種非常可怕的，從個人到大型公司都可能遭遇的攻擊。

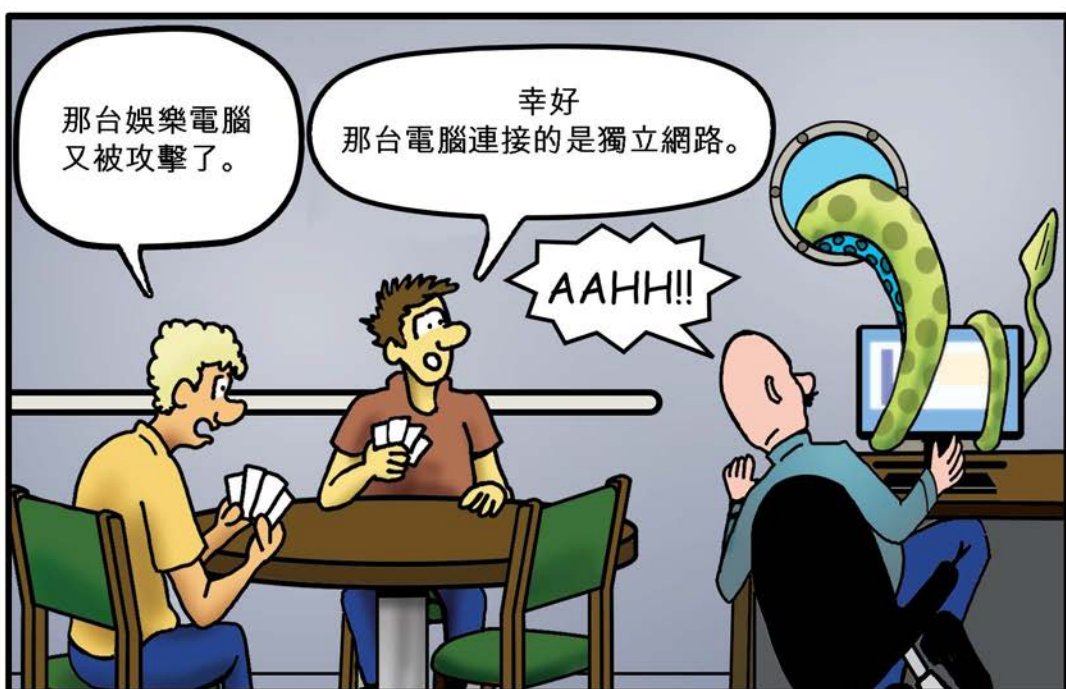


## 勒索軟體概述

勒索軟體可能是破壞性最強的網路攻擊形式。



如果你懷疑有勒索軟體攻擊，請立即向您的主管報告！  
預防是最好的防禦措施！



## 勒索軟體：如何發現它

勒索軟體和其它病毒一般通過看起來合法的陷阱連結或者郵件附件傳播。

你如何識別  
潛在的  
惡意電子郵件？



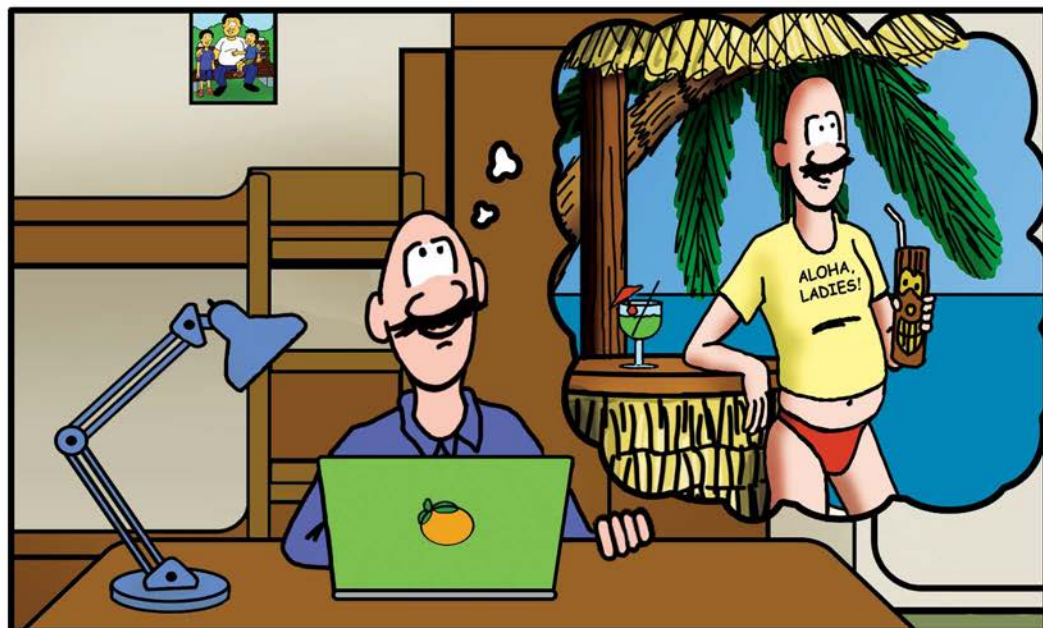
Subject: You win 50% off your next trip!  
From: Vacations R Us <Joe@VacationsRu5.com >

Dear Valued Costumer,  
50% off your next trip - Click [HERE](#) to  
redeem this coupon.

[www.GOTCHA.com/stealinfo](http://www.GOTCHA.com/stealinfo)

To unsubscribe , please click [HERE](#)

- 電子郵件功能變數名稱與網站不匹配。警惕諸如@y0utube.com或paypa1.com之類的數位或拼寫錯誤。
- 合法公司將使用您的真實姓名。
- 滑鼠懸停在連結上不要點擊，就會顯示出該連結的真實網址。如果其真實網址與郵件的內容不匹配，不要相信這個連結！



## 如何抵御勒索软件。

对那些主动发来的  
或者意料之外的邮件  
保持警惕。



注意高风险附件文件类型，  
比如说exe, scr, 和zip  
这些需要下载的文件。

Subject: Your Refund

From: Tax Department <Security@TakeYoMoney.com>

 2019Receipt.zip

Please find the attached Tax Receipt with  
your \$30,000 refund.

**FAKE**

- 真实的公司不会随意向你发送带有附件的邮件。  
而是会指引你从他们的官网上下载文件。
- 网络罪犯一般在报税季或者购物季行动，  
这些邮件也往往与报税或者购物有关。

电子邮件诈骗正变得越来越老练。

我们在打开并下载电子邮件附件时必须保持警惕、理智和聪明。

防御和应急计划  
是您在网络事件中的救星。

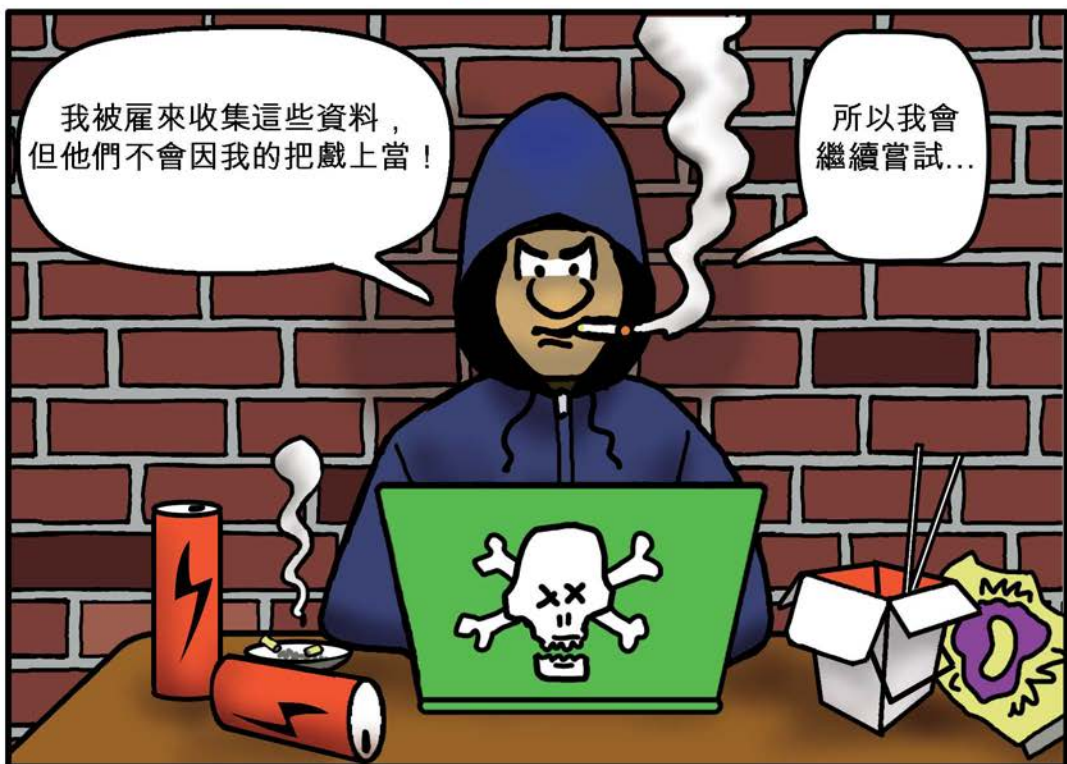


## 應急計畫

你無法預知所有的事情，但知道事情出現差錯後如何應對非常重要。











AMERICAN STEAMSHIP OWNERS MUTUAL  
PROTECTION & INDEMNITY ASSOCIATION, INC.

**SHIPOWNERS CLAIMS BUREAU, INC., MANAGER**

One Battery Park Plaza, 31st Floor  
New York, New York 10004 USA

TEL +1 212 847 4500  
FAX +1 212 847 4599  
WEB [www.american-club.com](http://www.american-club.com)  
EMAIL [info@american-club.com](mailto:info@american-club.com)

2100 West Loop South, Suite 1525  
Houston, TX 77027 USA

TEL +1 346 223 9900  
EMAIL [claims@american-club.com](mailto:claims@american-club.com)

**SHIPOWNERS CLAIMS BUREAU (UK) LTD.**

78-79 Leadenhall Street  
London EC3A 3DH United Kingdom

TEL +44 20 7709 1390  
EMAIL [claims@scb-uk.com](mailto:claims@scb-uk.com)

**SHIPOWNERS CLAIMS BUREAU (HELLAS), INC.**

Filellinon 1-3 - 3rd Floor  
Piraeus 185 36 Greece

TEL +30 210 429 4990 1 2 3  
FAX +30 210 429 4187 8  
EMAIL [claims@scb-hellas.com](mailto:claims@scb-hellas.com)

**SCB MANAGEMENT CONSULTING SERVICES, LTD.**

The Workstation, 28th Floor  
43 Lyndhurst Terrace  
Central, Hong Kong SAR, People's Republic of China

TEL +852 3905 2150  
EMAIL [hkinfo@scbmcs.com](mailto:hkinfo@scbmcs.com)

**SCB MANAGEMENT CONSULTING (CHINA) CO., LTD.**

Room 905, Cross Tower  
No. 318 Fuzhou Road  
Shanghai 200001, People's Republic of China

TEL +86 21 3366 5000  
FAX +86 21 3366 6100  
EMAIL [claims@scbmcs.com](mailto:claims@scbmcs.com)

