社交工程

高雄餐旅大學
黃士育

OUTLINE

何謂社交工程？

1. 社交工程說明

2. 社交工程常見的攻擊方式

3. 如何預防社交工程的發生?

社交工程說明

社交工程 (Social Engineering) 係利用人性弱點，應用簡單的溝通和欺騙技倆，以獲取帳號、密碼、身分證字號或其他機敏資料，來突破校園的資通安全防護，遂行其非法的存取、破壞行為。

範圍相當廣泛，一般在報章雜誌上經常看見之詐騙手法，或是親身經歷的詐騙電話，另外還有利用好奇心來使人上鉤等都是屬於社交工程之應用

社交工程常見的攻擊方式

個人對社交工程的輕忽，給予不法份子有機可乘的機會，將構成校園資通安全的漏洞，其結果輕則影響個人權益，重則威脅校園資通安全，實不可不慎。瞭解社交工程的各種攻擊方式，有助於個人防範各種攻擊事件，以下列示常見的社交工程攻擊方式以供參考

1. 利用電話佯裝資訊人員，騙取帳號及密碼

1.1 利用電話佯裝使用者，騙取帳號及密碼

2. 偽裝委外廠商之維護人員或上級單位人員，乘機騙取帳號及密碼

3.利用電子郵件誘騙使用者登入偽裝之網站以騙取帳號及密碼，如網路釣魚

4.利用電子郵件誘騙使用者開啟檔案、圖片，以植入惡意程式、暗中收集機敏性資料

5.利用提供工具、檔案、圖片為幌子，誘騙使用者下載，如偽裝的修補程式 、p2p 下載軟體、工具軟體等，乘機植入惡意程式、暗中收集機敏性資料

6.利用即時通訊軟體如 MSN，偽裝親友來訊，誘騙點選來訊中之連結後中毒

7.在facebook上分享好康連結，讓使用者點選後中毒

實例分享

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Phishing Email Example

Subject: E-Mail Account Upgrading of XXX Webmail @2012

Welcome To XXX Webmail
Dear Email subscriber

We would like to inform you that we are currently carrying out scheduled maintenance and upgrade of our account service and as a result of this your accounts have to be upgraded.

. . . . . .

Login :

Password:

. . . . . .

Phishing Email Example

Subject: Account Update !!!

This is to inform you that you have exceeded your email quota limit of 325MB
and you need to increase your email quota limit because in less than 48 hours
your email will be disable. Increase your email quota limit and continue to
use your webmail account.

To increase your email quota limit to 2.2GB, , you must reply to (xxx@gmx.com) this email immediately and enter your account details below.

Username: (**********)
Password: (**********)
Date Of Birth(**********)

各個地方出現__連結

網站:

facebook
google+
plunk
.....

e-mail:

附檔中的小遊戲
好康連結
spam

如何預防社交工程的發生?

社交工程雖然利用人性弱點來騙取機敏資料，讓人覺得防不勝防，但如果能隨時提高警覺，不未經確認即轉寄資料、不開啟來路不明的電子郵件及附加檔案、不連結及登入未經確認的網站、不下載非法軟體及檔案，就能避免社交工程的攻擊傷害

開啟郵件的處理

關閉郵件預覽就不會有問題??

關閉圖片預覽就不會有問題??

windows update才是最重要的

建議使用 WSUS

所有軟体的update 如Adobe PDF Reader、Flash、Real player、Codec...等

宣導郵件

一、依據教育部98年11月12日台電字第0980185062A號函辦理。
二、「教育部98年度學術機構分組防範惡意電子郵件社交工程演練計畫」結果報告:依測試結果, 信件點閱率以趣味類的點選率最高，以測試信件標題為開玩笑語句或是可笑圖片等內容，通常最吸引長時間上班受測者目光而較被密集點選。而點選連結下載遊戲程式或開啟來路不明文件並在主機執行，容易感染病毒或被種植木馬，也可能被駭客入侵並成為攻擊跳板，造成嚴重資安問題。
三、建議各位同仁, 並勿開啟任何來路不明的電子郵件或連結下載遊戲程式。

圖資館網路應用組　敬啟

謝謝聆聽!!