

新北市 科技領域 教學示例

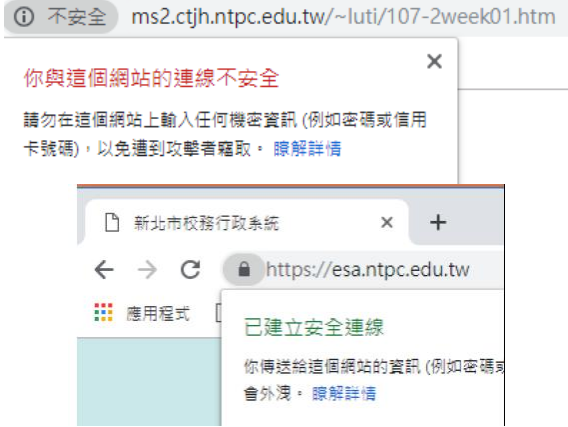
(一) 教案概述

單元名稱	資安小達人		
領域/科目別	科技領域/資訊科技		
教學對象	國中7年級	教學時數	共 2 節， 90 分鐘
教學資源	筆、電腦、網路、瀏覽器		
學習目標	能了解網路資訊安全防護概念 能了解密碼管理及強度概念 能了解凱薩密碼編碼概念 能了解網頁加密與未加密之差異性		
先備知識	1.基本英文 26 個字母認識及順序 2.瀏覽器使用		
可融入之領域/議題	實質內涵	法治教育議題	
	所融入之學習重點	理解法律與治的意義；習得實體程序基本知能追求人權保障與公平正義的價值。	
與課程綱要的對應	核心素養	J-B2 具備善用科技、資訊與媒體以增進學習的素養，並察覺、思辨人與科技、資訊、媒體的互動關係。 J-C2 具備利他與合群的知能與態度，並培育相互合作及與人和諧互動的素養。	
	學習表現	運 a-IV -2 能了解資訊科技相關之法律、倫理及社會議題，以保護自己與尊重他人。	
	學習內容	資H-IV-3資訊安全。	
課程架構	<div><div>資訊安全概念(2 節)</div><div><div>網路安全-防火牆及密碼強度與管理概念及其生活上應用(1 節)</div><div>網路安全-密碼學與安全傳輸協定概念及其生活上應用(1 節)</div></div></div>		

教學活動 (名稱)	教學內容 (含時間分配)	備註 (如學習單等、教學資源)															
第一節活動一	<p>引起動機 (10 分鐘)</p> <p>1.播放資訊安全新聞事件。</p> <p>2.老師引導提問:</p> <p>Q1:思考一下:資訊世界帶給我們新視野雖有新契機但也有新威脅.請問有何威脅?</p> <p>Q2:思考一下:在此新聞中這名電腦高手是幾歲?他是何種身份?他真的是駭客嗎?</p>	<p>資訊安全新聞事件</p> <p>ATM 爆漏洞 一銀被盜領7千萬</p> <p>https://youtu.be/6lnEd-cJpxo</p> <p>19歲駭客抓 FB 漏洞 30秒刪創辦入貼文</p> <p>https://youtu.be/IQFETpqt9Uk</p> <p>(並備妥離線版本)</p> <p>教學網站</p> <p>https://bit.ly/2GXfEcE</p>															
第一節活動二	<p>資訊安全概論(10 分鐘)</p> <p>1.老師以表格說明危害資訊安全的原因</p> <table border="1"> <thead> <tr> <th>資訊安全的威脅</th><th>惡意</th><th>非人為、無意</th></tr> </thead> <tbody> <tr> <td>硬體破壞</td><td>竊盜、搗毀</td><td>自然災害、儲存媒體損毀</td></tr> <tr> <td>資料破壞</td><td>資料竄改、資料增刪、系統性更動資料</td><td>程式師無能、不小心、遺漏</td></tr> <tr> <td>資料外洩</td><td>資料複製、網路截取、詐騙</td><td>不小心</td></tr> <tr> <td>網路入侵</td><td>竊取資料、破壞、將受侵電腦作為犯罪工具</td><td>—</td></tr> </tbody> </table> <p>2.資訊安全的防範</p> <ul style="list-style-type: none"> ● 網路安全 ● 系統(電腦)安全 <p>3.網路安全</p> <ul style="list-style-type: none"> ● 防火牆(Firewall) ● 隱私及識別 <p>4.老師解釋防火牆及隱私及識別的涵義</p> <p>(1)先以大樓間的防火巷為例。</p> <p>(2)再以圖解說明防火牆，它是一項協助確保資訊安全的裝置，會依照特定的規則，允許或是限制傳輸的資料通過。可能是一台專屬的硬體或是架設在一般硬體上的軟體。</p> <p>(3)隱私及識別是指資料或訊息在網路傳遞時是否被人攔截或非法讀取其運用的網路技術為加密及</p>	資訊安全的威脅	惡意	非人為、無意	硬體破壞	竊盜、搗毀	自然災害、儲存媒體損毀	資料破壞	資料竄改、資料增刪、系統性更動資料	程式師無能、不小心、遺漏	資料外洩	資料複製、網路截取、詐騙	不小心	網路入侵	竊取資料、破壞、將受侵電腦作為犯罪工具	—	<p>教學網站</p> <p>https://bit.ly/2GXfEcE</p> <p>學習單</p>
資訊安全的威脅	惡意	非人為、無意															
硬體破壞	竊盜、搗毀	自然災害、儲存媒體損毀															
資料破壞	資料竄改、資料增刪、系統性更動資料	程式師無能、不小心、遺漏															
資料外洩	資料複製、網路截取、詐騙	不小心															
網路入侵	竊取資料、破壞、將受侵電腦作為犯罪工具	—															

	解密。	
第一節活動三	防火牆設定(10 分鐘) 1.學生觀看作業系統防火牆設定教學影片。 2.學生實際操作防火牆設定。 3.老師課間巡堂釋疑。	Windows 作業系統防火牆設定教學影片 https://youtu.be/yA-Zn3ONI94 教學網站 https://bit.ly/2GXfEcE 學習單
第一節活動四	密碼強度(Strong Password) (10 分鐘) 1.老師提問最容易被破解的密碼為何? 2.老師播放 SplashData 評出的2018年最容易被破解的密碼。 3.學生觀看破解你的密碼要花多少時間影片? 4.學生進入 HOW SECURE IS MY PASSWORD 網站實際演練。 5.老師說明優質(強壯、複雜)密碼設定原則: (1)設定至少 8 個字元的密碼。 (2)避免重複或連號的字母、數字。(aaacbb、112233)。 (3)使用數字、英文字母大小寫、符號穿插的字串。(a、A、^&*]、)。 6.老師說明密碼管理重點: (1)至少三個月更換一次密碼。 (2)避免重複設定已用過的密碼。 (3)避免使用字典查詢得到的字串,意即常見之單字。 (4)避免使用太過複雜,自己也記不住的密碼。 (5)不可用明文方式記載密碼。 (6)不要告訴別人,不可用電子郵件或經由他人轉交密碼,不要在公用電腦上(如:機場、車站、網咖等)輸入密碼並儲存於公用電腦上。	破解你的密碼要花多少時間? https://youtu.be/D-mjdV2EbLU 2018 年最糟糕網路密碼榜資料與影片 https://bit.ly/2Hj1HWE https://vimeo.com/306043630 HOW SECURE IS MY PASSWORD? https://howsecureismypassword.net/ 教學網站 https://bit.ly/2GXfEcE 學習單
第一節活動五	資訊安全小結1(5 分鐘) 1.老師針對今天上課的內容進行總結及複習。 2.老師詢問學生對今天上課內容是否有疑問。	
第二節活動一	引起動機(10 分鐘) 1.播放阿里巴巴與四十大盜影片(看到3分36秒即可)。 2.老師引導提問: (1)阿里巴巴是怎麼知道密語的? (2)這個密語相當是我們網路世界的什麼?	觀看阿里巴巴與四十大盜影片(看到3分36秒即可) https://youtu.be/A9iiuykkRcM
第二節活動	與密碼共舞(5 分鐘) 1.複習隱私及識別是指資料或訊息在網路傳遞時	教學網站 https://bit.ly/2GXfEcE

<p>動二</p>	<p>是否被人攔截或非法讀取其運用的網路技術為加密及解密。</p> <p>2.老師圖解說明「密碼學」概念。</p> <div data-bbox="284 338 935 562" data-label="Diagram"> </div> <p>圖 13：一般所指的密碼系統架構</p> <p>圖片引用:雲端的守護神 ~資訊安全之密碼學初探 資訊安全之密碼學初探 蘇淵源 教師 (國立新港藝術高級中學)</p>	
<p>第二節 活動三</p>	<p>凱薩密碼(Caesar cipher) (15 分鐘)</p> <ol style="list-style-type: none"> 1.學生觀看凱薩密碼原理影片。 2.凱薩密碼練習輔助工具網站操作(分組練習)。 3.老師提問凱薩密碼有何缺點。 4.學生討論。 	<p>The Caesar cipher Journey into cryptography Computer Science Khan Academy https://youtu.be/sMOZf4GN3oc</p> <p>凱撒密碼練習輔助工具網站 https://www.xarg.org/tools/caesar-cipher/ https://www.cryptoclub.org/ http://ctf.ssleye.com/caesar.html 學習單</p> <p>教學網站 https://bit.ly/2GXfEcE</p>
<p>第二節 活動四</p>	<p>安全傳輸協定-SSL (10 分鐘)</p> <ol style="list-style-type: none"> 1,老師說明如何知道線上購物網站是可靠的運用-的網路技術-安全傳輸協定 SSL。 2. SSL(Secure Sockets Layer)是瀏覽器及網頁伺服器之間以加解密方式溝通的安全技術標準，這個溝通過程確保了所有在伺服器與瀏覽器之間通過資料的私密性與完整性。 3.http 開頭的網頁，在網際網路上是明碼在傳遞的，若有傳送機密資料(如網站登入密碼、金融卡卡號等)，則有可能被有心人士竊取。因此常見的大型網站(如 google.FB..等)的登入頁面都會用 SSL 加密，即網址為 https 開頭。 4.觀察與討論瀏覽器網址列前方標示的安全與不安全圖示 	<p>教學網站 https://bit.ly/2GXfEcE</p> <p>呂老師教學網站 http://ms2.ctjh.ntpc.edu.tw/~luti/</p> <p>新北市校務行政系統網站 https://esa.ntpc.edu.tw/</p> <p>學習單</p>

	 <p>5.老師提問學生:是否可舉一些你常去的網站說明其網頁是否有加密呢?</p>	
第二節 活動五	<p>資訊安全小結2(5 分鐘)</p> <ol style="list-style-type: none"> 1.老師針對今天上課的內容進行總結及複習。 2.老師詢問學生對今天上課內容是否有疑問。 	
參考資料	<p>資訊安全新聞事件</p> <p>ATM 爆漏洞 一銀被盜領7千萬 https://youtu.be/6lnEd-cJpxo</p> <p>19歲駭客抓 FB 漏洞 30秒刪創辦人貼文 https://youtu.be/IQFETpqt9Uk</p> <p>Windows 作業系統防火牆設定 教學影片 https://youtu.be/yA-Zn3ONI94</p> <p>破解你的密碼要花多少時間? https://youtu.be/D-mjdV2EbLU</p> <p>2018 年最糟糕網路密碼榜資料與影片 https://bit.ly/2Hj1HWE https://vimeo.com/306043630</p> <p>HOW SECURE IS MY PASSWORD? https://howsecureismypassword.net/</p> <p>阿里巴巴與四十大盜影片 (看到3分36秒即可) https://youtu.be/A9iiuykkRcM</p> <p>The Caesar cipher Journey into cryptography Computer Science Khan Academy https://youtu.be/sMOZf4GN3oc</p> <p>凱撒密碼練習輔助工具網站</p> <ul style="list-style-type: none"> ● https://www.xarg.org/tools/caesar-cipher/ ● https://www.cryptoclub.org/ ● http://ctf.ssleye.com/caesar.html <p>新北市校務行政系統網站 https://esa.ntpc.edu.tw/</p> <p>教學網站</p> <ul style="list-style-type: none"> ● https://bit.ly/2GXfEcE ● http://ms2.ctjh.ntpc.edu.tw/~luti/ 	

(二) 評量活動

評量目標	1.能完成學習單。 2.能參與分組討論。 3.能網路資訊安全防護概念 4.能了解密碼管理及強度概念 5.能舉例說明常用的網站那些網頁是有加密 6.能利用網路資源了解凱薩密碼編碼概念
評量工具	學習單

資安小達人學習單

1.小華立志成為一名電腦資訊安全工程師，請協助她判斷下列何者對於資訊安全的描述是否為真。(是非題.真寫T.假寫F)

(1)危害資訊安全的原因，一定是人為破壞。

(2)防火牆，它是一項協助確保資訊安全的裝置，會依照特定的規則，允許或是限制傳輸的資料通過，它一定是一台的硬體裝置。

(3)密碼管理重點是不要告訴別人，不可用電子郵件或經由他人轉交密碼。

(4)資料或訊息在網路傳遞時是否被人攔截或非法讀取其運用的網路技術為加密及解密。

(5)線上購物蝦皮購物網其網址為<https://shopee.tw/>，其中<https://>代表該網站使用安全傳輸協定SSL(Secure Sockets Layer)。

A:(1) (2) (3) (4) (5)

2.ABC網站的會員密碼必須符合下列三項規則

a.限8-12個字元長度

b.只能使用英文大小寫字母.0-9的數字.特殊符號(@_-)

c.必須包含1個大寫字母

小花正在註冊成為ABC網站會員，想了4組密碼，哪一個密碼可以使用？

(1)Flower.123 (2)99flower (3)Flower_123 (4)-Flower123qazx

A:

3.凱撒密碼是廣為人知的代換密碼。為了用凱撒密碼法加密訊息，每個明文的字母將會被其位置的後3個字母替代。因此字母A將會被字母D替代、字母B將會被字母E替代、字母C將會被字母F替代等，最後，X、Y和Z將分別的被替代成A、B和C。例如，"WIKIPEDIA"將被加密成"ZLNLSHGLD"。凱撒把字母向後移"3"位。

明文字母表：A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

密文字母表：D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

(1)位移量是3的話 明文：HELLO → 密文是：_____

(2)位移量是3的話 密文：love → 明文是：_____

(3)根據凱薩密碼原理SPNF可以還原成ROME，其偏移量是_____(提示1~25)