Continguts Formatius
de Suport al Projecte acTIC

Nivell C-1: Cultura, participació i civisme digital

Mòdul 4: Avaluació de la informació i nocions de seguretat

1. OBJECTIUS

- Conèixer i aplicar les mesures bàsiques de seguretat de la informació
- Fer un ús eficient i segur d'Internet, i avaluar la informació obtinguda

2. AVALUACIO DE LA INFORMACIO D'INTERNET

Actualment tothom pot accedir a Internet i publicar-hi qualsevol tipus d'informació. Per aquest motiu, hem de ser capaços d'avaluar si aquesta informació és fiable i segura.

L'autoria

Una de les claus a l'hora d'avaluar una informació consisteix a saber qui publica el contingut, si el lloc que visitem és d'una institució (una entitat educativa, una empresa comercial, una associació sense ànim de lucre, etc.) o bé d'un particular.

El segon aspecte a considerar és si podem posar-nos en contacte amb el responsable del contingut (si es tracta d'un autor que firma l'article dintre d'un lloc web que conté més informació), o si a la pàgina web hi ha algun enllaç que permeti comunicar-nos amb la institució o entitat que publica els continguts.

Portada de la web de l'Enciclopèdia Catalana, on es pot apreciar a la part inferior els enllaços a les dades de contacte de la institució

El tercer aspecte és veure si la informació està actualitzada; es pot comprovar, per exemple, mitjançant la darrera data de publicació del contingut.

El quart aspecte és avaluar si la informació és creïble, o bé si es tracta d'una informació publicitària o que intenta persuadir d'alguna cosa el lector.

La qualitat dels enllaços

Molts llocs inclouen enllaços. Hem de comprovar si els enllaços estan actius i si presenten els continguts amb una informació actualitzada. Per exemple, si una pàgina web enllaça freqüentment amb altres pàgines que mostren un missatge d'error, pot significar que aquesta pàgina no s'ha actualitzat o revisat des de fa temps.

Si una pàgina web enllaça freqüentment amb altres pàgines que mostren un missatge d'error, pot significar que aquesta pàgina no s'ha actualitzat o revisat des de fa temps

També hem de tenir en compte si els enllaços estan relacionats amb el contingut del lloc original.

El disseny del lloc

Una bona pàgina d'inici ha de presentar un resum del contingut del lloc web i una guia o índex sobre com accedir-hi.

Un dels aspectes que cal que considerem és si la navegació dintre del lloc és clara i coherent i si és fàcil de trobar-hi allò que cerquem; per exemple, és molt convenient que disposi d'un plànol de navegació o esquema de les diferents seccions que conté (un mapa web).

També hem de considerar si hi ha elements multimèdia i si aporten informació de qualitat al lloc.

Una altra manera d'avaluar la informació que ofereix un lloc web és tenir en compte les valoracions que els usuaris fan de determinades pàgines relacionades amb la informació (per exemple, les valoracions de cases rurals per part dels clients en webs de viatges) o les referències que, en blocs específics, es donen sobre un determinat tema.

3. SUPLANTACIÓ D'IDENTITAT I PROGRAMARI MALICIÓS

Quan naveguem per Internet o fem servir el correu electrònic, cal ser molt prudents, ja que de vegades podem ensopegar amb programari maliciós capaç d'afectar el nostre ordinador o que impliqui altres riscos. Tot i que es tracta d'un perill que es pot prevenir, abans de res hem de saber de quin tipus d'amenaça es tracta.

Els gestors de correu electrònic poden ser atacats no per aconseguir informació del servidor o obtenir-ne el control, sinó per difondre indiscriminadament correus de publicitat no desitjada (anomenada "correu brossa" o "spam") o bé virus, amb la intenció de propagar-los al major nombre possible de comptes de correu.

Les amenaces al correu electrònic

Es classifiquen en dos tipus:

- La recepció de correus electrònics amb virus, cucs electrònics i troians com a arxius adjunts. Quan s'obre l'arxiu, el virus s'executa i infecta l'ordinador, o bé infecta altres equips tot enviant-los correus electrònics.
- Els enganys (també anomenats "pesca electrònica" o "phishing")

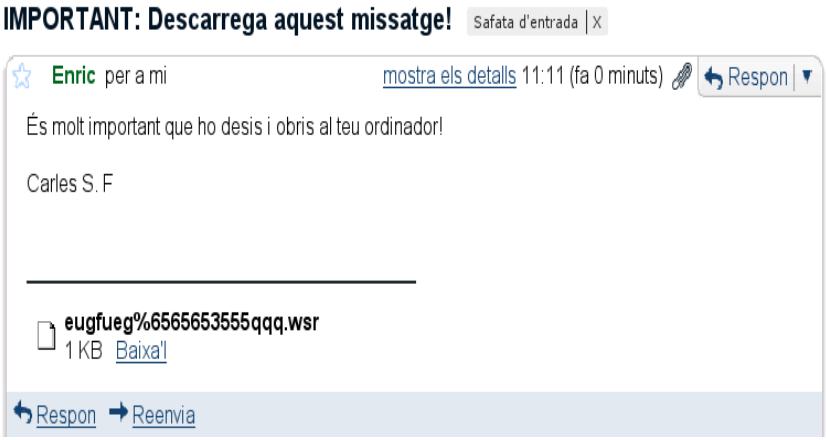
Al missatge de correu electrònic rebut, ens indiquen o demanen que realitzem alguna acció, com visitar una adreça web, en la qual hem d'introduir dades confidencials com ara el nom d'usuari i la contrasenya. Un exemple d'aquest tipus d'engany són aquells correus electrònics que semblen emesos per la nostra entitat financera, i mitjançant els quals se'ns pretén avisar que hi ha algun problema de seguretat amb el nostre compte.

Com podem saber si el correu és un engany? Ens fixarem en els aspectes següents:

- El remitent: L'adreça de correu electrònic (en aquest cas, suposadament, el suport tècnic del banc) no dóna prou informació per assegurar la seva credibilitat. Al final de l'adreça, en lloc de les inicials o el nom de l'entitat,

hi apareix un compte gratuït de correu electrònic, com per exemple Hotmail, Gmail, etc.

- El destinatari: Les empreses gestionen de forma personalitzada la comunicació amb el client, i, per tant, el nom del destinatari ha de coincidir amb la seva adreça. -
- L'enllaç a la suposada pàgina web de l'entitat financera: Si ens hi fixem, veurem que es troba a la part superior del navegador web, a la barra d'adreces, i comença per http://. Si el seu inici no coincideix amb el nom de l'entitat, probablement es tracti d'un lloc web fraudulent.

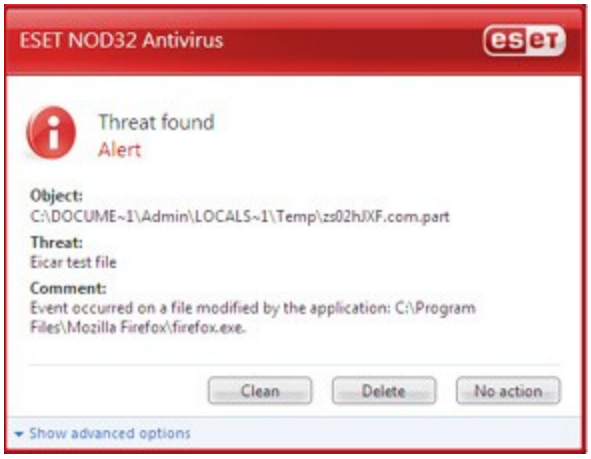


De vegades fins i tot un remitent conegut per nosaltres pot semblar l'autor d'un missatge que contingui un adjunt perillós

Codis maliciosos

Els navegadors d'Internet (Mozilla, Opera, Internet Explorer, etc.) també poden ser, ocasionalment, objecte d'atacs. En visitar pàgines web, els navegadors sovint permeten l'execució i instal·lació automàtica d'uns components que s'anomenen "connectors" (o *plugins* en anglès).

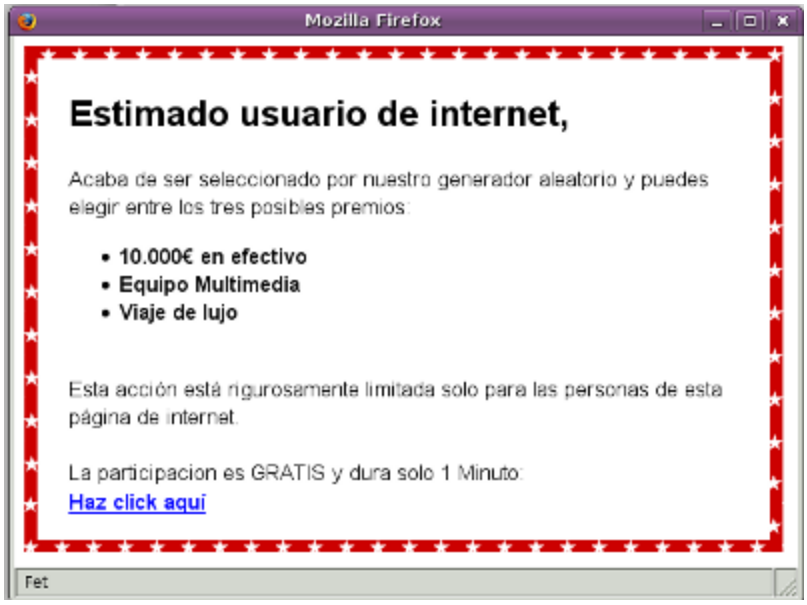
Aquests connectors són inclosos als navegadors per veure o millorar la visualització de determinats arxius. Però alguns d'aquests components de vegades poden dur un codi maliciós que permet la instal·lació de programes que emplenen l'ordinador de publicitat mentre estem navegant, o que, fins i tot, poden introduir-hi un virus. Cal estar molt atents als advertiments que sovint ens ofereix el navegador quan accedim a aquest tipus de pàgines web.



Exemple de pantalla flotant de programari que alerta sobre la detecció d'una amenaça per al sistema mentre es navega per Internet

Altres connectors poden instal·lar programes que obtenen informació de l'ordinador, com ara el "programari espia" (també anomenat *spyware*), o que poden activar processos en l'ordinador sense que ens n'adonem, per tal que treballi amb finalitats delictives quan el deixem encès.

Hi ha d'altres connectors o reclams a pàgines web que poden omplir la pantalla de finestres emergents amb publicitat mentre naveguem per Internet.



Exemple de reclam publicitari no desitjat.

Algunes coses que podem fer per evitar aquestes intrusions de codis maliciosos són:

- No obrir mai els arxius adjunts a un correu electrònic si desconeixem el que contenen o qui ho envia.
- Instal·lar programari de protecció (antivirus).
- Determinar filtres de seguretat al maquinari de navegació o del correu electrònic.

4. SEGURETAT DE LA INFORMACIÓ

Una xarxa telemàtica és una xarxa d'equips informàtics que es comuniquen entre ells. La xarxa Internet està formada per la unió de xarxes telemàtiques de proveïdors de serveis d'accés i d'interconnexió, que gestionen els paquets de dades (la informació) que nosaltres enviem i rebem.

Aquesta estructura en xarxa pot patir el risc d'accessos no autoritzats als nostres equips informàtics i a la nostra informació. Aquests riscos, que normalment poden ser previnguts, es divideixen en dues categories: riscos relacionats amb la informació i riscos relacionats amb els sistemes (dels ordinadors i equips informàtics).

Riscos relacionats amb la informació

La informació que s'intercanvien dos ordinadors connectats a una xarxa pot patir les amenaces següents:

A la confidencialitat: Algú no autoritzat accedeix a la informació que enviem per la xarxa a un altre usuari, tot interceptant el nostre canal de comunicació (el cable o la xarxa sense fil) mitjançant un programari que permet capturar els nostres paquets de dades.

- A la integritat de la informació: S'intercepten els nostres paquets de dades per modificar-ne la informació. D'aquesta manera, es pot enganyar el destinatari de la informació i fer que dugui a terme una acció diferent a la desitjada.
- A l'autenticitat: Consisteix a enviar informació falsa a un destinatari, suplantant la identitat d'una altra persona.
- Pèrdua d'anonimat: L'obtenció de les nostres dades (per exemple, el número de la targeta de crèdit) o d'una decisió (el vot electrònic) que és confidencial, per utilitzar-les de forma no autoritzada.

De vegades poden interceptar-se paquets de dades per modificar-ne la informació

Riscos relacionats amb els sistemes

Són atacs a qualsevol element que forma part de la xarxa de comunicacions (cables, ones, etc.) i als sistemes finals (ordinadors i altres dispositius informàtics). Es classifiquen de la manera següent:

- Denegació de servei: Es bloqueja el sistema perquè no es pugui utilitzar o per empitjorar el servei, introduint interferències al senyal o bloquejant el servidor amb l'enviament de molta informació generada automàticament.
- Atac d'intrusió: S'entra en un sistema de forma no autoritzada per aconseguir informació confidencial, per modificar o destruir informació, per executar un programari maliciós o bé per utilitzar l'equip amb la finalitat d'atacar altres sistemes.

Per evitar aquest tipus d'amenaces, disposem de diferents programes antivirus (McCafee, Panda, NOD32, etc.), programari de tallafocs per controlar el flux de dades i programes antiespies que es poden instal·lar a l'ordinador o bé als servidors.

Exemple de programa tallafocs per controlar el flux de dades entre ordinadors

5. ENLLAÇOS RELACIONATS.

Avaluació de la informació d'Internet

Internet, ajuda o perjudici? http://blocs.xtec.cat/filotermes/2007/12/13/internet-ajuda-o-perjudici-sandra-garcia/

Suplantació d'identitat i programari maliciós

Portal per a la prevenció de fraus per Internet (en castellà)
http://www.identidadrobada.com

Informació sobre pesca electrònica de l'Associació d'Internautes (en castellà)
http://seguridad.internautas.org/

Seguretat de la informació

Secció sobre virus i seguretat de la informació del bloc Informàtica.cat
http://www.informatica.cat

Classificació de virus informàtics (en castellà) http://www.network-press.org/?virus_informaticos_concepto