El treball diari en les nostres entitats i associacions passa sovint per realitzar un munt de tràmits i gestions electròniques. Enviar correus electrònics als nostres associats, realitzar tràmits o preparar els nostres butlletins son tasques que no estan exemptes de convertir-se en **pràctiques de risc informàtic**. Però, què significa això del **virus informàtic**? Què puc fer per evitar aquests riscos?

Quan parlem de **seguretat en informàtica** ens referim a aquelles **mesures que podem prendre per evitar patir qualsevol mena d'acció malintencionada** contra el nostre ordinador. Des d'intentar robar-nos dades personals, omplir la nostra pantalla d'anuncis o danyar el nostre equip, aquestes accions són, sovint, portades a terme per programari maliciós, conegut genèricament com a virus. Aquests programes són difosos a través dels correus electrònics, enganxats en fitxers adjunts o amagats en un llapis de memòria USB, s'instal·laran en el nostre equip sense el nostre permís.

En aquest recurs aprendrem **quines són les principals amenaces per als nostres equips** i com podem actuar per evitar-les i defensar-nos.

Les amenaces informàtiques: tinc un virus?

Un virus informàtic és un programa que s'ha realitzat amb l'objectiu de modificar el funcionament normal d'un equip, sigui esborrant arxius, modificant el sistema operatiu o enviant dades personals als creadors del programa. Tot i que és l'amenaça informàtica més coneguda, sovint anomenem virus allò que no ho és. Farem servir la paraula ***malware*** per descriure a aquells programes maliciosos (de l'anglès ***mal****icious soft****ware***).

Però també cal recordar que les amenaces no són provocades només per aquests programes, sovint l'engany o els usuaris/àries inexperts/es es converteixen en la més gran de les nostres vulnerabilitats!

Virus i cucs: malware infecciós

Un **virus informàtic** és un programa que té com a objectiu **modificar el funcionament d'un ordinador**, **sense el coneixement de l'usuari/ària**. Al executar aquest programa, aquest **es propaga infectant a altres programes**,

de la mateixa manera que ho faria un virus biològic.

El funcionament d'un virus es basa en substituir els arxius executables d'un programa sa o del sistema operatiu per a altres infectats amb el seu codi, alterant el bon funcionament de l'equip. El seu objectiu pot ser el d'entorpir les tasques, però sovint poden amagar altres objectius com eliminar dades o fitxers vitals per al sistema operatiu.

Es denomina **cuc informàtic** el programa que és capaç de **duplicar-se a sí mateix**. El seu principal objectiu és el d'infectar a la major part d'usuaris/àries possibles, però també pot tenir objectius nocius.

A diferència dels virus, **els cucs no modifiquen els arxius de cap programa**, sinó que s'allotgen en la memòria del sistema i es van duplicant. A la llarga, es detecten els cucs quan, a causa de la seva incontrolada replicació, **consumeixen els recursos del sistema**, fent que les tasques més habituals es tornin increïblement lentes.

Aprofita les vulnerabilitats d'una xarxa per infectar altres equips, sent aquest el seu màxim objectiu. Per això, sovint generen problemes de connexió, ja que per propagar-se utilitzen molt ample de banda.

Una altra diferència destacable entre cucs i virus és que el virus necessita la intervenció de l'usuari per propagar-se (cal que algú executi l'arxiu infectat), mentre que el cuc es propaga automàticament. Les infeccions trameses a través del correu electrònic, per tant, són virus (necessiten que s'obri el correu per executar-se).

Malware que s'amaga: troians, rootkits i la porta del darrera

Si el principal objectiu d'un *malware* és destruir parts dels sistema que ha infectat, quant més temps tingui per realitzar aquesta tasca més possibilitat tindrà per fer-la correctament. Amb aquest objectiu, hi ha diversos tipus de programari maliciós que intentarà mantenir-se invisible el màxim temps possible.

Comencem amb els **troians**. La idea d'aquests programes prové de la història del Cavall de Troia explicada en l'Odissea d'Homer. En aquesta versió contemporània, **el troià es presenta a l'usuari com si fos un programa legítim** i inofensiu que, al ser executat per l'usuari, modifica els sistema operatiu.

Pot desenvolupar diverses tasques, però la més comú és la d'obrir **portes del darrera** en el nostre ordinador, donant la possibilitats que un tercer usuari no autoritzat controli el nostre sistema operatiu o copii les nostres dades personals (contrasenyes desades en el navegador, etc..).

Estrictament parlant, un troià no és un virus, ja que no té la capacitat de propagar la infecció a altres sistemes per si mateix. Les seves conseqüències, però, són igualment fatals, fet pel qual ens hem de defensar igualment d'aquests programes.

Els **rootkits** ajuden també en aquesta tasca. Aquests són programes destinats a **esborrar qualsevol rastre deixat dintre d'un sistema infectat**, permetent que un *malware* es mantingui ocult a l'usuari. Per exemple, un rootkit evita que un procés maliciós fos visible en la llista de processos del sistema o que els seus arxius es mantinguin ocults en el navegador de fitxers, de la mateixa manera que pot contenir estatègies per evitar ser esborrat del sistema.

L'ús de portes del darrera i de rootkits no s'efectua només des dels atacants informàtics. Empreses de software han plantejat l'ús de les portes del darrera com una manera d'ajudar als usuaris/àries inexperts/es, fent servir l'administració remota dels sistema operatiu, i algunes distribuïdores discogràfiques han fet servir rootkits per mantenir la protecció anticòpia d'alguns CDs de música.

Amb l'objectiu de fer diners

Tot i que molts virus i cucs han estat creats com a simple exercici informàtic (per explorar les vulnerabilitats d'un sistema operatiu) la majoria estan fets amb l'objectiu de treure'n beneficis. Ja sigui amb fins publicitaris o amb voluntat d'obtenir il·lícitament dades personals, aquest programari buscarà traure el màxim profit del nostre ordinador.

Comencem per l'anomenat ***spyware***. El programari espia és un tipus de programa troià que s'instal·la a un ordinador (host) amb l'objectiu de **recollir dades personals del seu propietari** i enviar-les a empreses publicitàries o altres institucions interessades. Les dades que acostuma a recollir són el correu electrònic, la llibreta de contactes, les pàgines web visitades, temps que s'ha passat l'usuari visitant-la, els fitxers que s'ha descarregat, i tota la informació que un usuari pugui intercanviar en una web: formularis web, números de targetes de crèdit i comtes de banc, contrasenyes...

En concret, els **keyloggers** i els **stealers** són els programes creats específicament per **robar la informació personal**. Mentre el keylogger captura les pulsacions del teclat, el stealer intentarà fer-se amb la informació desada en els fitxers protegits del nostre sistema, on s'allotgen les contrasenyes o altres credencials privades.

Els programes spyware envien aquesta informació fent servir la connexió a Internet, de manera que consumeixen molt ample de banda, reduint la velocitat de transferència de dades.

Sovint, aprofitant la connexió a Internet, adjuntat en un correu electrònic o fent-se passar per programari legítim es pot instal·lar **adware**. Aquests programes s'executen automàticament i mostren missatges publicitaris, fent servir finestres emergents que dificulten l'ús de l'ordinador. En alguns casos, les versions gratuïtes de programes propietaris inclouen adware, per eliminar les molèsties que aquest causa cal fer-se amb la versió de pagament.

Alguns programes adware han rebut crítiques ja que recollien i feien seguiment de la informació personal de l'usuari, actuant com ho faria un spyware.

També cal vigilar amb...

Tot i que no entrin dintre de la categoria de programari maliciós, hi ha un seguit de **pràctiques que poden suposar un perill per als usuaris/àries d'ordinadors**, sobretot si no es tenen present les conseqüències que poden tenir.

El **correu brossa**, conegut com **spam**, és una tècnica de venta directa consistent en fer enviaments massius de correus electrònics sense el consentiment de les persones que el reben. Poden arribar al volum de saturar una bústia de correu electrònic o de fer passat desapercebuts correus legítims, i sovint mostren publicitat enganyosa o fraudulenta.

En aquest sentit, cal anar amb compte amb els **hoax**, també dit falsa alarma o senzillament enganys. Aquests correus són la versió digital de les llegendes urbanes, històries en les que es **barregen referents reals amb ficcions per fer caure al lector en un engany**. Els més benignes poden senzillament demanar que reenviïs el correu, altres poden detallar instruccions precises perquè esborris un fitxer vital del sistema operatiu fent-te creure que és un virus.

Finalment, una altra pràctica amb la que cal estar alerta és el **phishing**. Aquesta és una **estafa cibernètica** en què l'estafador intentarà aconseguir dades privades (tals com el número de la targeta de crèdit, en número de seguretat...) fent-se passar per membre de l'empresa fent servir una comunicació aparentment oficial.

Defensem-nos!

Cal tenir present que aquests programes malintencionats aprofiten els forats del nostre sistema operatiu per fer la seva tasca. Com que la seva voluntat és danyar el màxim d'ordinadors possibles, és lògic que estiguin dissenyats per atacar el sistema operatiu majoritari en el mercat: les diferents versions de Windows fabricades per Microsoft. Aquest fet no vol dir que no existeixi malware per a Mac OS o GNU/Linux, però és molt minoritari.

Sigui quin sigui els sistema operatiu que fem servir, convé que seguim els següents passos de protecció:

- **No fer servir l'usuari administrador del sistema** per a altres tasques que no siguin les d'administració. La major part de Sistemes Operatius permeten crear usuaris “sense permisos” per poder realitzar tasques del dia a dia.
- **Mantenir el Sistema actualitzat**. A través de les diverses actualitzacions que ofereixen els programadors del nostre Sistema es corregeixen errades i forats de seguretat, tornant el nostre ordinador més segur davant de possibles atacs.
- **Instal·lar un antivirus** actualitzat que ens ajudin a defensar-nos.

Podem trobar diverses opcions, quina escollir? Hi ha vàries opcions comercials que ens protegiran, però si la nostra entitat és petita i no disposa de grans recursos, podem fer servir les versions gratuïtes que ens ofereixen algunes d'aquestes opcions. Aquestes versions acostumen a oferir menys prestacions (sense suport, o sense filtre anti-spam...) però protegiran igualment al nostre ordinador.

- Avast! Free Antivirus Aquest antivirus, elaborat per una comunitat de desenvolupadors txecs, posa a disposició de l'usuari domèstic una **bona, robusta i gratuïta solució de seguretat informàtica**, oferint a empreses i institucions solucions de pagament adaptades a les seves necessitats.
  La versió gratuïta per a Windows ens ofereix una protecció antivirus així com anti-spyware, de la mateixa manera que ho ofereix en la versió per a GNU/Linux.
  La versió bàsica per a Mac OS, però, és de pagament.
- Una altra opció que podem considerar és AVG Antivirus. De la mateixa manera que ho fa l'anterior opció, AVG ofereix una **versió bàsica gratuïta per a usuaris domèstics**, que ens protegeix dels virus i troians. Per a usuaris pro (empreses i professionals) ofereix a més protecció per a phishing, anti-spam, protecció de la identitat, anti-rootkits, etc.
  AVG ens ofereix la seva protecció tant si fem servir GNU/Linux com si fem servir alguna versió de Microsoft Windows, però no ofereix protecció per a usuaris de Mac OS.

Cal recordar que la principal defensa en matèria de seguretat informàtica està a les mans dels mateixos usuaris. Seguir unes senzilles pautes reduirà considerablement el nostre risc:

-

Fer servir un **usuari sense permisos d'administració** en el nostre sistema operatiu.

- **Canviar la nostra contrasenya** del correu electrònic amb regularitat, evitant fer servir paraules massa senzilles d'endevinar.
- **No obrir mai un fitxer enviat per correu electrònic** de remitent desconegut (acceptaries un caramel d'algú que no coneixes?)
- Comprovar que qualsevol arxiu nou no estigui infectat, **passant-hi l'antivirus**. Si no tenim permisos per instal·lar-ne, podem comprovar que l'arxiu estigui sa fent servir alguna utilitat per analitzar fitxers on-line.
- Comprovar que el nostre antivirus estigui actualitzat.
- **No enviar les nostres dades personals per correu electrònic**, encara que ens ho estigui demanant una empresa de confiança.
- **Configurar el nostre navegador** perquè eviti les finestres emergents i denegui les galetes (cookies) de tercers.

I **mantén-te informat**! Trobaràs molta informació d'interès a la web del Centre de seguretat de la Informació de Catalunya o a la web del Instituto Nacional de Tecnologías de la Comunicación.