**TIPUS ATACANT**

- **Crackers o hackers de barret negre:** el terme hacker es utilitzat per referir-se a qualsevol intrús en un sistema, sense tenir en compte la finalitat de l’atac. Les persones que trenquen les barreres de seguretat dels sistemes amb fins malintencionats se'ls anomena  **cracker** que prové de **Criminal hACKER**.

**- Phreakers**: són experts en **telefonia**. Són coneguts com els **phone crackers**, que busquen un benefici econòmic sabotejant les xarxes telefòniques per realitzar **trucades gratuïtes.**

**- Ciberterroristes**: són experts en **informàtica** i en **intrusisme** a la xarxa, que posen els seus coneixements al servei de països **i organitzacions per l’espionatge o sabotatge informàtic.**

**- Programadors de virus**: creen **petits programes que danyen** , que per un o altre motiu **arriben a la xarxa** i es **distribueixen amb rapidesa** ocasionant **danys en els sistemes o en la informació guardada en aquests.**

- **Carders**: ataquen els sistemes de **targetes**, especialment els **caixers automàtics**.

**- Sniffers**: ho podríem traduir com a **cotilla**, són les persones que es dediquen a **escoltar el trànsit de la xarxa**, per intentar **recomposar i desxifrar els missatges** que circulen per la xarxa.

**Lammers**: nois joves que sense grans coneixements informàtics, es creuen verdaders hackers i ho fan creure als membres de les seves colles. Aquests només **s’han descarregat eines o programes d’Internet** per realitzar atacs informàtics i els han posat en marxa **sense saber com funcionen**.

**- Newbie**: són els hacker **novatos**, comencen a aprendre i van superant els primers reptes per arribar a ser verdaders hackers.

**Luser**: és el terme que utilitzen els atacants per referir-se a **l’usuari** que serà **atacat.** És la abreviatura de **Local User**

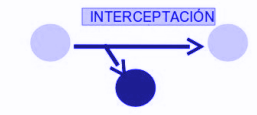
**TIPUS ATAC:**

**- Interrupció**: aquest tipus d’atac vulnera la disponibilitat d’un recurs dels sistema o de la xarxa. El recurs no podrà ser utilitzat.

* **Exemple,** l’apagament manual de qualsevol recurs



**- Intercepció**: ataca la confidencialitat. Un intrús accedeix a la informació guardada al nostre sistema o al que hem transmès per la xarxa

* **Exemples**, captura d’informació en la xarxa o copia d’arxius no autoritzats.

**- Modificació**: ataca l’objectiu d’integritat. Les dades han estat manipulades per personal no autoritzat en algun moment entre la seva creació i l’arribada al destinatari

* Exemples, les modificacions de programes per a que realitzin accions diferents a les propostes originalment, DNS spoofing, etc.



**- Fabricació**: aquest tipus d’atac vulnera la autenticitat. Es tracta de modificacions destinades a aconseguir que el producte final sigui similar a l’atacat de forma que sigui difícil distingir-lo de l’original.

* Exemple, el phishing.



Un altre tipus de classificació es pot realitzar en funció de la forma d’actuar dels atacs

**- Spoofing o suplantació de la identitat**: la tècnica de spoofing s’utilitza en **xarxes ethernet commutades** (xarxes que fan ús de switch). Aquest atac consisteix en falsejar alguna dada d’un PC atacat.

Tipus:

**Arp spoofing o arp poisoning**, consisteix en **enganyar a la taula arp** que els equips guarden en memòria.

Amb aquesta tècnica d’engany podem **fer creure a un PC atacat que l’adreça física d’un altre PC, també atacat de la xarxa, és la del PC del atacant.**

Aconseguint així que tot el trànsit de xarxa entre els dos PC atacats passi per un PC de l’atacant;

**DNS spoofing o engany de DNS**, consisteix en **falsejar la resposta del servidor DN**S sobre una petició i donar-li una adreça IP diferent a la real.

És a dir, que quan un PC atacat **demana** per exemple **la IP de www.elmeubanc.cat** al seu servidor DNS, l’equip atacan**t falsejarà el paquet de dades de les DNS** amb la resposta i li pot enganyar donant-li la IP d’un altre equip qualsevol.

Així e**nlloc de connectar-se al seu banc es connectaria a un altre PC** diferent podent falsejar la pàgina d’entrada de la seva banca electrònica i capturant les seves claus d’accés a la mateixa.

**- Sniffing o anàlisis de trànsit:** consisteix en **escoltar el trànsit de la xarxa**. (En xarxes d’àrea local que utilitzen el HUB com a medi d’interconnexió entre els equips)

Aquesta tècnica es converteix en un joc de nens; com sabem, els hubs o concentradors repeteixen tota la informació rebuda per cada un dels seus ports.

**NO - Connexió no autoritzada a equips i servidors:** consisteix en descobrir diferents **forats en la seguretat** d’un sistema informàtic **i establir-hi una connexió no autoritzada.**

Ja sigui perquè hem descobert les contrasenyes d’alguns usuaris, o bé utilitzant aplicacions malware que aprofiten les portes de darrera o forats per permetre l’accés a l’equip des de l’exterior.

**- Enginyeria social:** Consisteix en **obtenir informació secreta d’una persona** o organisme per utilitzar-la posteriorment amb finalitat maliciosa. Habitualment els enginyers socials utilitzen el correu electrònic, pàgines Web falses, el correu ordinari o el telèfon per dur a terme els seus plans.

Exemples, són el phishing i l’ús d’una màquina atacada per l’enviament d’spam.

**- Phishing:** és una tècnica d’engany a l’usuari, que adquireix informació confidencial del mateix **suplantant la identitat d’altres** persones, organismes o pàgines WEB d’Internet.

Un dels mètodes de Phishing més utilitzats avui en dia consisteix en penjar a Internet una pàgina que es copia idèntica d’alguna altra, como pot ser la d’alguna entitat financera o banc.

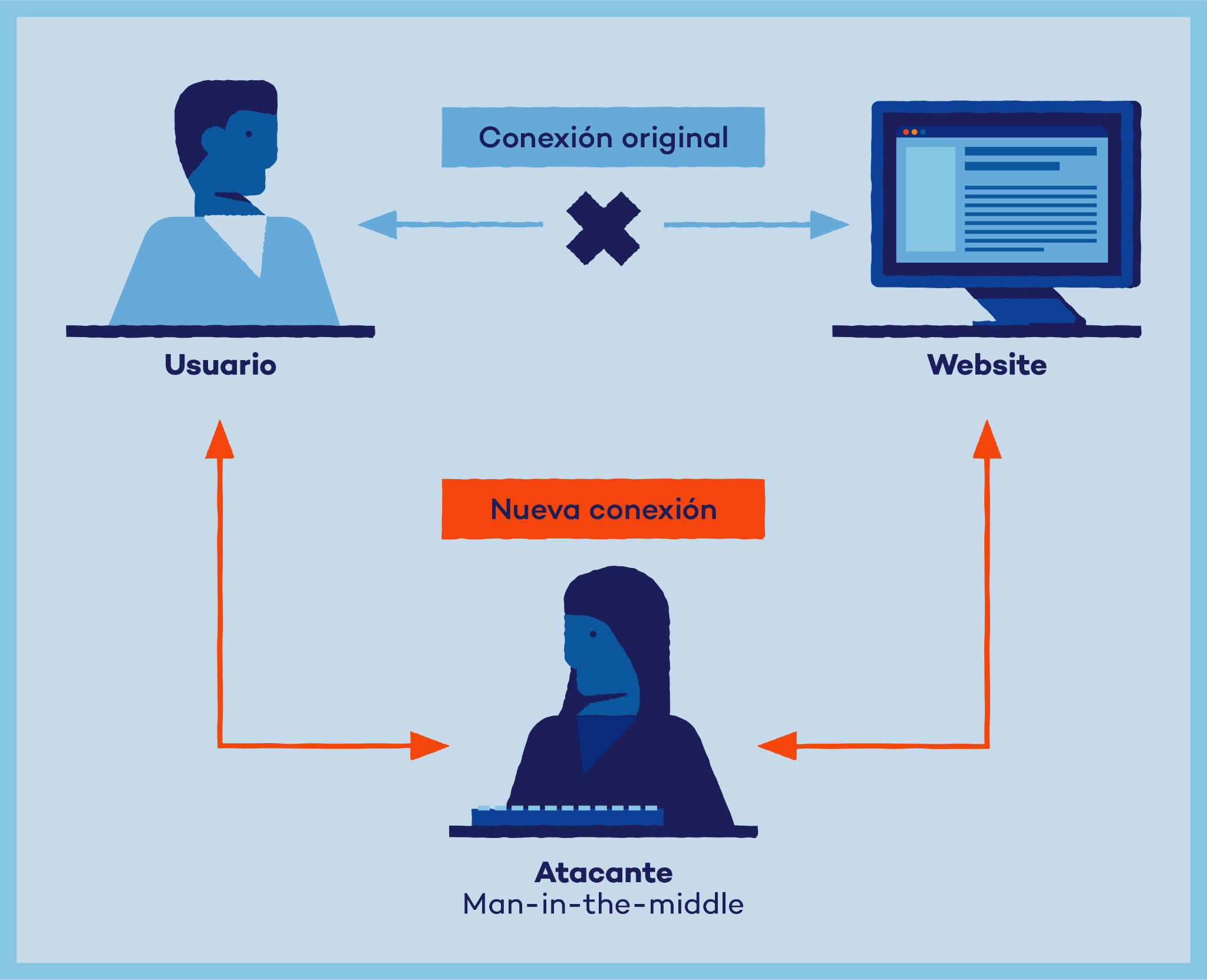
Si algú confon aquesta pàgina falsa amb l’original i introdueix en ella les seves dades personal com poden ser el número de targeta o PIN de la mateixa, aquests números se’ls envia directament als creadors de l’estafa,

**La URL té una petita diferència** que a primera vista no es nota però que obligatòriament ha de tenir.

**Inundació de peticions SYN:** consisteix en **fer una petició d’establiment de connexió** a un servidor **i no respondre a la seva acceptació de connexió**, bé sigui perquè s’ha falsejat el paquet de petició amb una IP falsa o per alguna altra causa.

Aquest tipus d’atac provoca una **saturació en les connexions obertes del servidor**, de tal forma que si aquestes són molt elevades poden arribar a produir un coll d’ampolla del servei ofert amb la conseqüent denegació de servei.

Man in the middle



**TIPUS MALWARE**

**Virus** és un **codi maliciós** incrustat en el codi normal d’un programa amfitrió. El virus es **propaga d’un ordinador a un altre**, però per fer-ho **necessita la intervenció humana.**

Només poden existir en un equip dins d’un altre fitxer, generalment executable: .exe, .src, .bat

Pot afectar al funcionament del software, del hardware i a les propietats de la informació, causar un impacte des de lleu a molt greu, depenent del seu objectiu

**Bomba lògica.** Programa o part d’un programa que s’instal·la en un ordinador i **no s’executa fins que es compleix una determinada condició**, per exemple, ser una data concreta, execució d’un arxiu determinat, etc.

**Hoax** Missatge electrònic enviat per un conegut que **intenta fer creure al destinatari alguna cosa que és falsa**, com alertar de virus inexistents, notícies amb contingut enganyós, etc. i sol·licitant ser reenviat a tots els contactes.

**Clicker**. **Readreça les pàgina d’Internet** a les que intenta accedir l’usuari, d’aquesta forma aconsegueix aumentar el número de visites a la pàgina redireccionada.

**Spwyware Roba informació de l’equip per enviar-la a un servidor remot.** El tipus d’informació obtinguda varia segons el tipus d’espia. Als espies que roben informació bancària se’ls anomena “troians bancaris”.

**Keyloggers:** S’utilitza com eina maliciosa per **conèixer tot el que un usuari escriu a través del teclat**, fins hi tot a vegades registren captures de pantalla de l’equip. Per aconseguir aquests objectius existeixen eines hardware i software.

Els perifèrics dissenyats per aquesta finalitat poden ser des d’un teclat amb l’aparença idèntica a un de normal però que conté una **memòria no volàtil** on guarda la informació escrita o bé mitjançant un petit dispositiu que es connecta entre el port de l’ordinador (USB o PS2) i un teclat.

**Els cucs** **són un subtipus de virus**, que es propaguin per la xarxa. Es diferencien en que aquestos **no necessiten la intervenció de l’usuar**i, ja que no s’adjunten a cap programa, sinó que **són distribuïts per la xarxa** consumint en la gran majoria dels casos un gran ample de xarxa o poden arribar a bloquejar l’equip infectat. Es fan **propietaris dels serveis encarregats de la transmissió de dades**

**Els troians** són **aplicacions aparentment inofensives** que faciliten en la majoria dels casos l’accés remot als equips infectats.

Aquestes aplicacions es poden amagar en arxius adjunts en els missatges que enviem per la xarxa. Poden arribar al nostre sistema:

* Descarregat per un altre programa maliciós
* Descarregat sense el consentiment de l’usuari al visitar una pàgina web maliciosa
* Dintre d’un altre programa que simuli ser inofensiu

**Un subtipus de troià és el backdoor**, un programa **client-servidor que obre una porta a l’equip client a través de la qual el servidor pren possessió de l’equip com si fos propi**, el que li permet tenir accés a tots els seus recursos, programes, contrasenyes i correu electrònic, algunes vegades en mode vigilància i altres per modificar la informació. Els equips poden **infectar-se si executen algun programa trampa**, generalment rebut com adjunt d’un correu electrònic o descarregat d’Internet. Igualment pot ser instal·lat directament a l’equip per algun delinqüent informàtic que tingui accés físic al mateix.

**ALTRES**

**Accés a la BIOS**

Si analitzem el procés d’engegada de l’ordinador, recordem la importància de la BIOS; és l’encarregada de localitzar i carregar el sistema operatiu o gestor d’arranc.

L’ús de **contrasenyes per** accedir **a la BIOS** **evitarà** que **personal no autoritzat** realitzi modificacions indesitjades en la configuració d’aquesta, així com canvis en la seqüència d’arranc, el que permetrà la posada en marxa de l’equip des de discs extraïbles i l’accés a les dades emmagatzemades en el mateix, vulnerant la confidencialitat d’aquests.

