Introducció

ATENCIÓ abans de començar llegiu aquests punts:

- Si feu els exercicis aquí descrits, els feu sota la vostra total responsabilitat. Cadascú ha anat configurant el seu ordinador amb aplicacions i altres particularitats i podria ser que en algun moment l'exercici no funcioni, tingueu problemes o fins i tot per una operació maldestre, tot i seguir les indicacions, esborreu dades o bloquegeu l'ordinador.
- Tot i això els següents exercicis han estat provats en 3 plataformes (Windows7, Mac OSX i Ubuntu) i alguns en iOS i Android, i han funcionat sense cap problema en el moment d'escriure'ls.
- Tingueu una bona còpia de seguretat de les vostres dades i la capacitat de tornar a instal·lar el sistema operatiu. Si no per avui, potser pel futur.
- Aquests exercicis no us faran invulnerables ni anònims ni invisibles a Internet però si us ajudaran a protegir les vostres dades i a controlar millor la vostra petjada digital.
- Aquesta documentació pot quedar obsoleta ràpidament per l'evolució de les aplicacions, els forats de seguretat que es descobreixin i l'estat de l'art de la tecnologia.

Si després d'aquests advertiments esteu preparats i disposats a continuar, comencem!

Els següents exercicis són només una introducció al tema de la privadesa i el control de la petjada digital a Internet i no tenim prou temps per a tocar altres àmbits. Si us interessa el tema ens podeu seguir al twitter a **@CryptoPartyBCN** o a **http://CryptoParty.cat** o demanar-nos un altre taller més especialitzat.

Si les aplicacions que farem servir us agraden, penseu en fer-los una petita donació o a passar a la versió Pro de pagament. Ajudant-los ens ajudem.

Temes a tractar

1. Passwords – com gestionar-los de manera segura
2. Privadesa i petjada digital – Configuració del navegador
3. Còpies de seguretat
4. Xat xifrat
5. Recuperació de dispositius robats

1 – Passwords

Consells:

- Per minimitzar èxit d'atacs de força bruta amb combinatòria de caràcters
  - Cal que siguin llargs (més de 12 o 14 caràcters)
  - Cal que tots els vostres passwords siguin diferents
- Per minimitzar l'èxit d'atacs per diccionari o llistes de paraules:
  - No useu paraules o frases conegudes (hogwards, etc) o de diccionari
  - No substituïu caràcters per nombres (i per 1, e per 3, a per 4, etc)
- Per minimitzar l'èxit d'atacs per *enginyeria social*:
  - No poseu els noms de persones, dates significatives o llocs relacionats amb vosaltres
  - No respongueu la veritat a les preguntes personals de recuperació de passwords. Per exemple si us demanen el nom de la mascota doneu un color o un dia de la setmana (i recordeu-ho!).
- No apunteu passwords en un paper o en un fitxer dins l'ordinador.
- Quan us doneu d'alta a serveis d'Internet intenteu fer servir una bústia de correu “secreta”, que pel nom no es pugui relacionar amb vosaltres i que sigui diferent que la del correu normal en l'opció per recuperar passwords oblidats. Si mai proven de recuperar el vostre password ho faran amb el vostre correu conegut.

Objectius:

- Fer que els dispositius demanin un password després d'un curt període d'inactivitat
- Usar una aplicació com KeePass per a guardar tots els passwords
- Canvieu avui els vostres passwords i deseu-los a KeePass. Empreu passwords llargs i millor si són complicats. Podeu deixar que KeePass els generi per vosaltres.

Pràctica 1: Posar un password i activar el protector de pantalla

Feu que el vostre dispositiu bloquegi la pantalla passats uns minuts d'inactivitat i que us demani un codi per a poder entrar. Trobeu com podeu forçar el bloqueig de la pantalla (Ctrl-L o altres).

Feu aquest exercici en tots els vostres dispositius. Si us el roben o el perdeu i el protector està activat compliqueu força la vida a qui el vulgui fer servir o accedir a la vostra informació. Atenció però amb les memòries micro/SD no xifrades dels telèfons i les ditades a les pantalles que puguin delatar el codi.

Windows	Tauler de Control > Presentació > Pantalla > Canvia estalvi de pantalla Tauler de Control > Comptes d'usuari i seguretat familiar > Comptes d'usuari
Mac	Preferències del Sistema > Seguretat i privadesa > General
Ubuntu	Paràmetres del sistema > Brillantor i bloqueig
Android	Configuració > Pantalla > Repòs + Estil de la pantalla de bloqueig
iOS	Configuració > General > Bloquejar/desbloquejar + Bloqueig automàtic

Pràctica 2: Què fa un password segur ?

ATENCIÓ: en el següent exercici NO escriviu cap password real vostre. No sabeu qui hi ha darrera aquesta web ni si està, o no, col·leccionant passwords reals per a fer-ne un diccionari amb el que preparar atacs.

- Aneu a la web http://howsecureismypassword.net
- Entreu el password “AAAAA” i apunteu quan pot trigar a trobar-lo:
- Entreu el password “ASDR%$” i apunteu quan pot trigar a trobar-lo:
- Entreu el password “password” i apunteu quan pot trigar a trobar-lo:
- Entreu el password “incorrect” i apunteu quan pot trigar a trobar-lo:
- Entreu el password “AAAAAAAAAAAAAAA” i apunteu quan pot trigar en trobar-lo i compareu-ho amb els anteriors:
- Conclusió: millor passwords llargs que curts i complexes, millor paraules que no estiguin en diccionaris o llistes, i encara millor si els llargs tenen nombres i caràcters especials.

Pràctica 3: On deso els meus passwords ?

Instal·larem KeePass com a gestor de passwords. KeePass crea una llista xifrada dels vostres users/passwords i us permet crear grups on classificar-los. *Per què ens fiem de KeePass?* És programari lliure, és a dir, que el codi del programa està disponible per a ser revisat i compilat, fet que augmenta la seguretat doncs més gent el pot revisar i comprovar que fa el que diu i ho fa bé.

1. Aneu a **https://keepass.info**
2. Descarregueu *KeePass* (versió 2.X o “professional”)
   - Linux: descarregueu KeePass via “Centre de programari”
   - iOS: descarregueu *MiniKeePass* via l'AppleStore
   - Android: descarregueu *KeePassDroid* via la Play Store
3. Instal·leu-vos l'aplicació
4. Apunteu-vos el password (llarg, difícil de deduir, etc) de xifrat de la base de dades. No el perdeu o no podreu accedir mai més al llistat xifrat dels vostres passwords.
5. Creeu entrades per a un o dos serveis online (email, twitter, facebook) i salveu-les
6. Podeu aprofitar el camp “Observacions” per a anotar les preguntes secretes i les respostes sense sentit que heu donat.
7. Aneu al navegador i obriu la pàgina d'un d'aquests serveis
8. Poseu el cursor sobre el camp “user”
9. Aneu a KeePass i seleccioneu l'entrada del servei escollit en el navegador
10. Feu servir KeePass per a entrar-hi (Ctrl-V)
11. Entreu als serveis (email, twitter, ...) i aprofiteu per a canviar els passwords actuals per altres més llargs.
12. Actualitzeu-ho immediatament a KeePass
13. Salveu la base de dades de passwords i feu-ne una còpia en una memòria USB.
14. Recordeu d'actualitzar la còpia del USB després de cada canvi i deseu-la bé.

- Si porteu un llapis de memòria podeu provar de descarregar i instal·lar la versió portable. O si porteu varis dispositius, exporteu-la i carregueu-la des de l'altre dispositiu.

2 – Privadesa i petjada digital

Reducció de la petjada digital i ser conscients de què i com es genera.

Vídeos curts sobre la petjada digital
http://www.internetsociety.org/your-digital-footprint

Quatre coses a fer en el navegador per a augmentar la nostra privadesa
https://www.eff.org/deeplinks/2012/04/4-simple-changes-protect-your-privacy-online

Com activar el "Do not track" en el navegador
https://www.eff.org/deeplinks/2012/06/how-turn-do-not-track-your-browser

Consells:

- Tapar la webcam amb un gomet
- Desactivar GPS, Bluetooth, WiFi, Dades quan no es vulgui fer servir (conserva bateria i talla seguiment en botigues i centres comercials o en ciutat, i evita deixar rastres (MAC address) i deixar una porta d'entrada al nostre dispositiu -bluetooth, WiFi i Dades-)
- Fer que el dispositiu **no** es connecti automàticament a WiFi obertes
- El telèfon però seguirà localitzant-nos (triangulació segons potència detectada de les torres); el podeu posar en "mode avió" per desactivar Telf, Dades, WiFi i Bluetooth
- Revisar opcions de privadesa en tauletes i mòbils.
- Metadades: tots els mòbils d'aquesta sala consten com que han estat junts durant unes hores (lloc, temps, acció, ...)
- Emprar VPN en WiFi obertes o públiques
- Gmail i altres serveis de correu gratis llegeixen el correu "per inserir publicitat"--> canvi a un domini propi i hosting?
- Opcionalment podeu fer servir un filtre polaritzant per a la pantalla del portàtil.

Objectius:

- Tapar la webcam (gomet una mica masegat per a facilitar treure'l quan calgui la càmera)
- Saber com activar i desactivar GPS, Bluetooth, WiFi i Dades de cada dispositiu
- Revisar opcions de privadesa del tauletes i mòbils
- Navegar "anònimament" --> pestanyes del navegador
- Identificació del nostre navegador **`http://ipcheck.info`**
- Esborrar *cookies* al sortir del navegador (o reset de "marcador de publicitat" al iPad)
- Instal·lació de Collusion
- Evitar *profiling* via AddBlockPlus i/o Ghostery
- Evitar moltes comunicacions web en clar via https everywhere
- Saber com habilitar i deshabilitar l'execució de codi Javasript en les planes web que carreguem
- Conèixer i usar nous cercadors: Startpage (ixquick) i Duckduckgo
- Llegir **`http://dontbubble.us`**
- Tancar sessions obertes a Google, Yahoo, LinkedIn, etc o tenir-les en navegadors diferents

Pràctica 4: Actualitzar el Sistema Operatiu i les aplicacions

És vital tenir el sistema operatiu i les aplicacions que fem servir actualitzades, en particular les que presenten regularment importants forats de seguretat (java, AdobeReader, Flash, etc) que poden permetre que s'executi codi no desitjat en el nostre dispositiu.

1. Identifiqueu en quines opcions de menú podeu forçar una cerca de les darreres actualitzacions.
2. Activeu les actualitzacions automàtiques, però no actualitzeu ara, feu-ho a casa.

Windows	Tauler de control > Sistema i seguretat > Windows update >
Mac	Preferències del sistema > Actualització de programari
Ubuntu	Icona de la roda > Actualització de programari

Atenció però amb les actualitzacions de les Apps en dispositius mòbils i tauletes. Sovint aquestes demanen més accés al dispositiu (localització, accés a fotografies i memòria SD, contactes, etc) quan en teoria, pel servei que ens han de donar, no els caldria.

Pràctica 5: Què és el profiling (Behavioral tracking)?

És la recopilació de dades amb la finalitat de fer un perfil d'una persona. Les dades es poden recollir a través de la petjada digital (*cookies*, navegador, ús d'Internet, ...) i es poden creuar, venent-les, amb altres dades recollides per altres agents (ús de la tarja de crèdit, dades de la tarja de fidelitat del supermercat o la benzinera, lectors de matrícules dels pàrquings, geolocalització, etc).

Vegeu aquest vídeo: Gary Kovacs: Tracking our online trackers (6m39s)
https://www.ted.com/talks/gary_kovacs_tracking_the_trackers

Els navegadors d'Internet deixen una empremta i el que fem amb ells també.

1- El nostre navegador pot ser identificat
Arrenqueu un navegador i aneu a **http://ipcheck.info**
D'entrada ja saben la IP des de la que ens connectem.
Seleccioneu fer el test.
Aquí teniu tota la informació que una web que visitem pot saber de nosaltres o el nostre navegador.
Amb tantes variables, poden arribar a filar molt prim i identificar quines planes mira un determinat navegador, i fer-ne un perfil.

Equivalentment podeu mirar **https://panopticlick.eff.org/**
D'entre els centenars de milions de navegadors d'Internet que hi ha al món és interessant veure com el nostre no és un de tants, és un d'entre uns pocs.

2- **La bombolla digital**
Segons el nostre historial de cerques i visites a Internet, les empreses que ens fan el seguiment van tenint un perfil nostre que usen “per a donar-nos una millor experiència i servei”, fet que comporta que veiem resultats dins la bombolla que ens van creant.

1. Arrenqueu dos navegadors i busqueu a Google (o Bing, Yahoo, etc) la mateixa paraula, per exemple “Viena” o “crisis”
2. Compareu els resultats dels dos navegadors.
3. Compareu-los amb els de la persona que tingueu al costat (cercant les mateixes paraules)
4. Captureu la pantalla per a comparar més tard (ImpPt, Ctrl+P, etc)

3- **Trencant la bombolla digital: els cercadors alternatius**

https://duckduckgo.com
https://startpage.com

i poseu-los a la barra de menús del navegador.
Busqueu la mateixa paraula de l'exercici 3 en aquests cercadors i compareu resultats.

Dediqueu 3 minuts a llegir https://donotbubble.us

4- **“Referer”: perquè hem de dir-los quina web acabem de visitar ?**
Amb el paràmetre “referer” la web que visiteu ara mateix pot saber quina altra web acabeu de visitar. Realment ho necessita saber ?

Si teniu Firefox podeu deshabilitar el paràmetre “**referer**”

1. Poseu “about:config” sense les cometes allí on normalment podeu la URL a visitar.
2. No feu cas de l'avís i segiu endavant
3. En la barra de cerca escriviu: referer
4. Veureu una variable de configuració del navegador **`network.http.sendRefererHeader`**
5. Seleccioneu-la i doneu-li valor zero
6. Ok i tanqueu la pestanya.

https://www.eff.org/deeplinks/2012/04/4-simple-changes-protect-your-privacy-online

5- **Quines dades necessita realment una App ?**
Les Apps dels mòbils i tauletes són aplicacions tancades sobre les que no tenim control. Algunes demanen accés a dades i parts del dispositiu que no semblen lògiques per a la feina que han de fer. Realment els cal la localització, accés als contactes, fitxers i fotografies, etc ? Penseu-ho dos cops abans d'instal·lar o actualitzar.

Pràctica 6: Configuració del navegador (Firefox)

Firefox: Configuració > Privadesa

- “Do not track” --> és força indiferent perquè no és obligatori pels llocs web fer-ne cas
- Esborrar totes les *cookies* al sortir del navegador
- Accepta galetes de tercers: Mai
- Mirar les galetes emmagatzemades i qui les ha posat (.ru, .my, ... ?!)
- Mida de la cache: a zero si no voleu emmagatzemar res (pot ser un problema econòmic si la connexió es fa via 3G)

No enviar res. No permetre propostes d'enllaços ni pre-càrrega de planes web.

Complements: deshabilitar Java i Flash (i saber com habilitar-los només quan realment calgui). Actualitzar però Java, Flash i AdobeReader sovint, ja que són coladors de seguretat i cal tapar els

forats amb les actualitzacions.

Pràctica 7: Extensions a afegir al navegador

Instal·leu-vos el Firefox **https://mozilla.org** (ordinadors i mòbils Android); per a iOS, proveu Opera **http://opera.com** tot i que aquest exercici no es pot fer amb Opera

Aneu a Firefox > Complements

Afegiu **Lightbeam**
Ens informa de amb quins altres servidors interactuem quan visitem una plana web. Aneu a la web d'un diari digital. Mireu què ens diu Lightbeam i compareu-ho amb els anuncis i la informació incrustada de la pàgina. (Win/Mac/Linux)

Afegiu **https everywhere**
Força, sempre que sigui possible, una connexió xifrada https entre el vostre navegador i el servidor web. El nom del domini que visiteu no es xifra però si la informació que rebeu i llegiu. Enllaç: **https://www.eff.org/https-everywhere** (Win/Mac/Linux/Android)
https és imprescindible quan feu comerç electrònic (busqueu el cadenat al costat de la URL)

Afegiu **AddBlockPlus**
Bloqueja i no mostra per pantalla anuncis de tercers. Comproveu-ho visitant la plana del Youtube o d'un diari digital. Fa doncs també més ràpida la càrrega de les planes i consumeix menys ample de banda. (Win/Mac/Linux)

Afegiu **Ghostery**
Elimina els elements de seguiment (*trackers*, *beacons* o *cookies* de tercers) i disminueix el seguiment que ens fan sense el nostre permís. (Win/Mac/Linux/Andoid; iOS és una App navegador)

Afegiu: **NoScript**
Permet bloquejar/habilitar l'execució de codi en Java i Javascript de les webs que visitem i crear una llista de les que si confiem (el nostre banc, etc). Permet evitar atacs de Cross-Scripting i similars.

Torneu ara obrir o refrescar la plana del diari digital obert quan Lightbeam i compareu els anuncis vistos abans i els d'ara. Mireu també què ens diu Lightbeam ara.

Feu aquest exercici en els vostres diferents dispositius.

Més informació a
https://www.eff.org/deeplinks/2012/04/4-simple-changes-protect-your-privacy-online

Pràctica 8: Revisar connectors del navegadors i històrial

Anar al Firefox > Complements > Connectors

- Java, Flash, QuickTime, ... > seleccionar “demanar si vull activar-lo”

- Deshabilitar i/o eliminar els connectors que no ens calguin
- El mateix per a les Extensions

Anar al Firefox > Opcions > Privadesa

- Revisar a les preferències del navegador quan i com esborrar *cookies* i historial.
- Accepta galetes de tercers: Mai
- Accepta galetes de llocs web fins: que tanqui el Firefox
- Neteja l'historial quan es tanqui el Firefox
- En particular CAL esborrar l'historial i cookies sempre que fem servir un ordinadors públic.

Pràctica 9: Canviar els DNS

El DNS cal per convertir (resoldre) un domini. És a dir, fer que si entrem al navegador la web **`meneame.net`** ens retorni l'adreça IP que identifica on rau físicament el servidor i permet que ens hi connectem.

Els ISP (Internet Service Providers) ens assignen per defecte els seus servidors DNS. Això vol dir que cada cop que carreguem una pàgina web, enviem un correu electrònic, etc, els DNS del ISP entren en funcionament per a cercar on és el servidor que es correspon al domini del servei demanat. Es a dir, el nostre ISP sap què consultem i quan ho fem. Si volem canviar això, cal canviar els DNS que es fan servir per defecte quan ens connectem al router i aquest ens assigna una IP i els DNS.

Una opció pot ser canviar els DNS del router de casa (pràctica 11). Amb aquesta solució, qualsevol que es connecti des del nostre router farà servir aquests DNS nous.

Una altra és forçar al dispositiu (ordinador, tauleta, telèfon) a fer servir uns altres DNS o fins i tot obviar el DNS per a alguns llocs.

- En sistemes **Windows** cal anar a Network Connections > Properties > TCP/IPv4 > (botó dret) Properties > Use the following DNS server addresses

  `http://mintywhite.com/windows-7/change-dns-server-windows-7`

- En sistemes **Mac** cal anar a System Preferences > Network > seleccionar la connexió sobre la que volem fer el canvi > DNS > i usar +/- per afegir o treure els DNS de resolució desitjats
- En sistemes **Unix** podeu obviar l'ús del DNS editant el fitxer `/etc/hosts` i afegint la IP i el domini al qual resol alguns serveis. Com no podreu llistar-hi totes les webs que hi ha (per això es va inventar el DNS) anem a Paràmetres del sistema > Xarxa i seguint les indicacions de la web
  `http://www.linuxandlife.com/2012/06/how-to-change-dns-in-ubuntu-linux.html`
- **iOS**: Aneu a Configuració > WiFi, seleccioneu la xarxa, premeu sobre la icona d'informació i canvieu els DNS
- **Android**: Depèn molt de la versió i de si sou *root* o no.

Una tercera manera de fer servir uns altres DNS és utilitzar una VPN, usant els DNS que aquest servei proporciona.

Pels casos u i dos, quins DNS podem fer servir? Per exemple un parell qualsevol d'aquests:

- 213.167.155.16 # DNS Island Telecom
- 89.233.43.71 # Censurfridns
- 208.67.220.220 # OpenDNS
- 89.104.194.142 # Censurfridns
- 85.214.20.141 # FoeBuD e.V.
- 77.109.138.45 # Swiss Privacy Foundation
- 77.109.139.29 # Swiss Privacy Foundation
- 87.118.85.24 # Swiss Privacy Foundation
- 208.67.222.222 # OpenDNS
- 87.118.100.175 # German Privacy Foundation e.V.
- 94.75.228.29 # German Privacy Foundation e.V.
- 62.141.58.13 # German Privacy Foundation e.V.
- 85.25.251.254 # German Privacy Foundation e.V.

Google ha popularitzat el seu DNS a través d'unes IP molt fàcils de recordar. Però què guanyem de negar la informació al ISP i donar-la a Google? Millor fer servir algunes d'aquests DNS llistats anteriorment.

Fer servir DNS alternatius i lliures és també una manera d'evitar la censura si mai us trobeu amb ISP o en llocs on l'accés a certes web hagi estat bloquejat a nivell de DNS.

DNSSEC – DNS xifrat per a evitar comunicar amb qui no toca

DNSSEC són unes extensions tècniques al sistema de DNS que xifren la comunicació de manera que ens assegura que la resposta del DNS (és a dir la adreça IP corresponent al domini que cerquem) és correcta i no ha estat alterada ni en origen ni en trànsit cap el nostre dispositiu. Emprar doncs DNS amb les extensions DNSSEC és molt més segur.

El tema és que nosaltres, com usuaris, no podem escollir entre usar-lo o no usar-lo. És una tecnologia que, tal com passa amb https o altres, l'han d'adoptar els registres i registradors de dominis. Podem però comprovar mentre naveguem si DNSSEC està o no actiu per a un domini determinat.

Aneu a **https://www.dnssec-validator.cz/** i instal·leu-vos el complement DNSSEC-VALIDATOR (cal reinicialitzar el navegador). Aquest complement indicarà si la resolució del domini s'ha fet via DNSSEC o no. A més a més, si està fent servir DNSSEC, comprovarà (tecnologia DANE) també que els certificats que fa servir el https són correctes i que no han estat manipulats, evitant així un atac actiu contra el nostre ús de https (comunicació xifrada entre el nostre ordinador i el servidor web).

Si un domini té DNSSEC pot també oferir una nova tecnologia (DANE) que signa els certificats del https, fet que posa una barrera més a un atac actiu contra la privadesa de la nostra comunicació amb aquest lloc web. Una de les icones que DNSSEC-VALIDATOR ens mostra indica precisament si DANE és ja actiu o no.

Pràctica 10: Ús d'una VPN (virtual private network)

Una VPN xifra la comunicació de sortida del nostre ordinador (web, mail, xats, ..., qualsevol) fins a un altre ordinador que serà el nostre punt de sortida a Internet, i per tant sortim a Internet amb una adreça IP (identificador del nostre ordinador a Internet) que no és l'assignada pel nostre ISP.

1. Aneu a **`http://ipcheck.info`** o **`https://whatismyip.com`** i anoteu la localització de la IP assignada pel nostre ISP
2. Aneu a **`https://vpngate.net`**
3. Seguiu les instruccions de "How to connect" per a la configuració del vostre dispositiu.
4. Sortiu per la VPN
5. Aneu a **`http://ipcheck.info`** i compareu la localització que ens ha assignat la VPN amb la assignada inicialment pel ISP

Altres serveis VPN per a provar:

- openvpn.net (software lliure de VPN si el vostre dispositiu no en porta) i el seu servei de VPN de pagament **`privatetunnel.com`**.
- **`IPredator.se`** (permet ús gratuït de prova durant 3 dies)
- **`vpntunnel.se`**

Si teniu contractat un servei de VPN el podreu també configurar fàcilment en el vostre mòbil o tauleta. Feu-ho.

L'ús de la VPN és altament recomanat (obligat!) quan feu servir WiFi públiques, obertes, o que no inspirin confiança (ex. aeroports, hotels, cafès i bars, etc). És molt fàcil que algú connectat a la mateixa WiFi pugui capturar les vostres sessions o crear un punt d'accés amb un nom atractiu o que suplanti a un punt WiFi bo i pugui capturar totes les vostres comunicacions. Amb la VPN totes les vostres comunicacions surten de l'ordinador xifrades, travessant les ones/cable, el router WiFi i la Internet fins als servidor VPN més protegides.

Pràctica 11: Tor, the onion router – navegació encara més privada

Tor https://torproject.org és un servei que funciona sobre Internet que a través del xifrat i el desviament del tràfic a través de tres capes de servidors, ajuda a fer més privada la vostra navegació. Hi ha diferents maneres de fer servir Tor, la més fàcil és amb el navegador de Tor.

1. Aneu a https://torproject.org
2. Si heu instal·lat el DNSSEC-VALIDATOR mireu els logos de DNSSEC i DANE
3. Descarregueu-vos el navegador per a la vostra plataforma
4. Mentre descarrega llegiu-vos la plana, explica què fa i què no.
5. Comproveu amb quina IP sortiu a Internet amb http://whatismyip.com
6. Navegueu

Pràctica 12: Revisar el router de casa

Exercici pels atrevits o qui sàpiga el que fa. Atenció canviar el firmware del vostre router o canviar certs paràmetres el pot inutilitzar totalment i anul·larà la garantia. Feu-ho només si teniu prou coneixement i sota la vostra total responsabilitat.

El firmware dels routers (el soft que porten dins) no s'actualitza amb massa freqüència, per a no dir mai, fet que pot deixar molts forats de seguretat oberts a mesura que es van descobrint noves vulnerabilitats.

Si sabeu com fer-ho i on trobar la darrera versió del firmware del vostre router, actualitzeu-lo

A banda d'actualitzar, o no, el firmware del router, és convenient repassar els següents punts:

- Canviar el password per defecte per administrar del router (i apunteu-lo al KeePass)
- Deshabilitar connexions d'administració remota del router
- Canviar els DNS reemplaçant els que proporciona el ISP per un parell dels llistats anteriorment

Hi ha també firmwares lliures i normalment més potents i segurs per a certs *routers*. Per exemple podeu mirar a **http://dd-wrt.com** o **https://openwrt.org/** si n'hi ha algun de recent pel vostre *router*, i si us interessa, instal·lar-lo. **Atenció**, això anul·larà la garantia del vostre *router* i si hi ho feu malament el pot deixar inservible; feu-ho només si teniu prou coneixement i sota la vostra total responsabilitat.

3 – Còpies de seguretat

L'objectiu de fer còpies de seguretat és el de poder recuperar la informació que ens interessa de manera ràpida i assegurant la validesa i consistència del contingut.

Consells:

- Feu sempre còpies de seguretat, i millor si les teniu per duplicat
- Si no les feu diàriament, feu-les setmanalment
- Estabiu una rutina o una entrada a l'agenda per a obligar-vos a forçar o comprovar que l'heu fet.
- Comencem de la manera més fàcil, la que ens proposa el propi sistema operatiu.
- No deseu totes les còpies de seguretat properes al vostre ordinador. Si us entren a robar, hi ha una inundació o no podeu tornar a l'oficina (evacuació, tall de carreteres, etc) heu de poder disposar d'una segona còpia actualitzada i vàlida.
- Si fas backups al núvol recorda que tu ja no tens les dades. Ni properes ni sota control directe.
- Atenció amb l'evolució dels estàndards d'aparells de lectura/escriptura, els connectors i dels formats dels fitxers. Qui pot obrir ara un fitxer en AmiPro, PageMaker 2, o WordStar? SCSI, RS232, HP-IB, ...? O llegir un ZIPdrive, una DAT o diskets de 3,5”?

Objectius:

- Saber com fer automàticament les còpies de seguretat bàsiques proposades pel propi sistema operatiu.
- Saber com esborrar realment els fitxers que hem enviat a la paperera

Pràctica 13: Còpia de seguretat bàsica

Hi ha moltes aplicacions per a fer còpies de seguretat però aquí ens centrarem en les que ens ofereixen directament els propis sistemes operatius Windows, Mac, Linux/Ubuntu. Són procediments que permeten fer còpies de seguretat de manera fàcil i amb poca intervenció.

Windows	Tauler de control > Sistema i seguretat > Fes una còpia de seguretat
Mac	Configurar la TimeCapsule
Ubuntu	Paràmetres del Sistema > Còpia de seguretat. A partir d'aquí configurem què, on, amb quina freqüència, etc ho volem fer

No ho farem perquè pot ser un procés molt llarg però mirem on hi ha les opcions a fi de fer-ho a casa.

Podem fer la còpia de seguretat a un disc extern USB que tingui molta més capacitat que el del nostre ordinador. Això ens permetrà guardar versions antigues de de les còpies (tal com fan els serveis al núvol).

En els **iOS, inclosos els iPad**, es pot fer a través del iTunes (i enregistrar-ho o no localment) o via iCloud; que cadascú decideixi segons la confiança que li inspiri cada mètode.

En els **Android** hi ha molta variabilitat degut a la varietat de versions d'aquest sistema operatiu que estan actives. Ofereixen també l'opció de desar-ho tot al núvol propietari de Google, és un tema de confiança. Hi ha aplicacions, com per exemple *MyBackup*, *truBackup* or *Backup your mobile* permeten fer la còpia sobre la tarja SD (o el núvol!) i faciliten la posterior còpia a un ordinador o disc extern el fitxer de backup. Molt més simple que copiar els fitxers i directoris a copiar connectant el mòbil a l'ordinador via el cable USB.

Un cop feta la còpia de seguretat en el disc USB extern podeu mirar-ne el seu contingut per a veure com són els fitxers i com xifra les dades el procediment de còpia. Aquest xifrat no us protegirà al 100% de cap especialista amb mitjans que realment vulgui accedir a les vostres dades, però si ho posarà molt difícil que accedeixin a les vostres dades en cas de robatori, pèrdua, etc.

Tenim ara una còpia però segons la importància de les dades en caldria una segona a fi d'assegurar-ne la disponibilitat. Una opció pot ser tenir dos discs externs i alternar-los a cada còpia de seguretat. Recordeu però de tenir el segon disc, i també el primer si pot ser, lluny del dispositiu, és a dir, tenir els 3 repositoris de dades en llocs diferents. Una altra opció pot ser fer servir un servei de backup al núvol per a aquesta còpia redundant. Però allò que és al núvol no és a terra i normalment està sota control d'una empresa amb la que hem de confiar.

I finalment el xifrat del propi disc dur de l'ordinador. La millor opció és xifrar el disc dur de

l'ordinador al començament del seu ús.

Pràctica 14: Esborrar fitxers de debò

Quan esborrem un fitxer, de fet no s'esborren els seus bits ni posem a zero l'espai que aquest ocupava; només s'indica al sistema de fitxers que l'espai que feia servir aquell fitxer està ara lliure i es pot fer servir. Així doncs, amb certes eines, es poden recuperar fitxers que creiem haver esborrat i eliminat de la paperera sempre que l'espai que ocupava el fitxer esborrat no l'utilitzi ara un altre fitxer. Per a més informació sobre el tema, **https://en.wikipedia.org/wiki/Data_remanence**

Esborrar bé fitxers és doncs molt important si mai regaleu o reveneu un ordinador o altre dispositiu.

Per a Linux i Windows hi ha aplicacions com **http://bleachbit.com/** o **http://eraser.heidi.ie** que reescriuen vàries vegades l'espai que ocupava el fitxer a fi de mirar de deixar-ho tan net (bleach = lleixiu) com sigui possible. CCleaner **https://www.piriform.com/mac/ccleaner** també funciona sobre Mac.

La pràctica consisteix en instal·lar una d'aquestes aplicacions i preparar una tasca de neteja d'un directori d'exemple. **Atenció** abans de jugar amb aquesta aplicació, assegureu-vos que teniu una bona còpia de seguretat. Els fitxers esborrats amb aquestes aplicacions NO es poden recuperar.

No cal fer moltes passades, amb una reescriptura del contingut ja és suficient per a la gran majoria dels casos (llegiu l'explicació a la web del Bleachbit).

4 – Xat xifrat

Les converses, igual que el correu electrònic, no viatgen xifrades per la xarxa. Amb una mica de tecnologia algú pot llegir el que diem o escrivim.

Consells:

- Els serveis amb formats propietaris (whatsapp, telegram, whisper, etc) no garanteixen la seguretat.
- Whatsup ha estat comprat per Facebook. Telegram pot dir que xifra les comunicacions, però és una empresa russa i la llei els pot obligar a donar accés a les converses.
- Skype va passar de ser un canal P2P a ser un canal que centralitza les comunicacions en els seus servidors.
- Com no sabem mai com circula la informació, res millor que assegurar-nos que som nosaltres qui la xifrem i protegim la nostra privadesa.
- TextSecure és una aplicació de codi obert per a mòbils i desenvolupada per reconeguts experts en xifrat i protecció de la privadesa. Permet l'emmagatzematge i l'enviament de SMS i MMS xifrats a altres usuaris que també facin servir TextSecure.

Objectius:

- Provar **`Crypto.cat`**, un xat sobre el navegador.
- Provar Pidgin/Audium, una aplicació que suporta diferents protocols de sistemes de xat
- Configurar Pidgin amb les extensions OTR (Off the Record) per a poder tenir converses protegides pel xifrat de la comunicació.
- Posar el Fingerprint de OTR a la signatura del correu electrònic
- Instal·lar TextSecure al mòbil

Pràctica 15: Cryptocat

És una extensió per a Firefox (i altres navegadors) que permet xat xifrat un a un o en grup.

Inicialment Cryptocat era una eina de xat xifrat però que es basava el seu funcionament en un servidor central, és a dir, amb un únic punt de fallada que podria caure sota control de tercers via atac o requeriment. Va rebre moltes crítiques per aquest fet i després dels canvis actualment cryptocat es basa en una extensió del navegador i no depèn de servidors centrals.

1. Obriu el Firefox o un altre navegador i aneu a **`https://crypto.cat`**
2. Instal·leu-vos l'extensió i reinicieu el navegador
3. Si no veieu la icona de cryotpcat, aneu a la configuració dels menús del navegador i afegiu-la.
4. Piqueu sobre la icona del cryptocat, inventeu-vos un àlies que no us identifiqui i entreu a la sala de xat preparada pels monitors d'aquest taller.
5. Proveu què tal va i mireu de fer una conversa un-a-un amb alguna altra persona present a la sala de xat. O crear la vostra pròpia sala i seguir fent proves.

Pràctica 16: Pidgin i les extentsions OTR (Off the Record)

Per a que la comunicació entre dues o més persones sigui xifrada cal que tots els participants facin servir les extensions OTR sobre el seu programa de xat i les hagin configurat i usin correctament. OTR protegeix el contingut de la conversa però no us fa anònims. Llegiu amb calma la web de l'aplicació i de OTR per saber què ofereix i què no.

Si teniu Windows o Linux prenem **Pidgin** (un programa multi-protocol de missatgeria instantània) per exemple. Per a Mac, descarregueu-vos **Audium** **`http://audiumx.com`** en lloc de Pidgin.

Aneu a **`https://pidgin.im`**
Descarregueu-vos i instal·leu l'aplicació

Aneu a la secció de la web de Pidgin on llista els ThirdParty plugIns
Cerqueu OTR (Off the Record) i aneu a la plana web que us indica (**`https://otr.cypherpunks.ca`**)
Descarregueu-vos les extensions de Pidgin-OTR

Instal·leu les extensions de Pidgin-OTR

Arrenqueu Pidgin i aneu al menú Eines > Connectors per a comprovar que OTR està habilitat.

Ara cal afegir usuaris al xat. Si ja teniu un compte de correu a Yahoo, Gmail o altres, podeu fer servir aquests comptes. Si per exemple us doneu d'alta a AIM veureu, un cop acabat el procés de registre que us diuen:

> *The new AIM logs and stores your conversation history (starting now) whenever you chat with other people using the new AIM. By clicking this button, you agree to the new AIM terms of service.*

És una bona raó per a no fer servir segons quins serveis. Alternativament a **https://jabber.de/register/** podeu obtenir un compte de xat XMPP molt més seriós.

Tornem a anar al menú Eines > Connectors i seleccionem OTR. S'obre una finestra de diàleg en la que escollirem el nostre perfil de xat i en generarem les claus de xifrat de la comunicació. Activem les opcions OTR per defecte “Automatically initiate private messaging” i “Do not log OTR conversations”.

Provem de fer un xat xifrat amb l'usuari **cryptopartybcn**

1. Afegiu-lo com amic
2. Espereu a que us accepti
3. Comenceu una conversa
4. Piqueu sobre le botó on diu “Not private”
5. Intercanvieu pregunta i resposta per a autentificar-vos (ex. Per l'exercici podem escollir “Shared secret” acordar preguntar-nos quin dia de la setmana és a avui. No és una bona pràctica però ens permet fer una bona simulació)
6. Un cop fet veureu que la conversa passa a “Private”.

En aquest punt tenim una conversa xifrada. Això no us fa anònims ni invulnerables però si protegeix el contingut de la conversa. Llegiu amb atenció l'ajuda de Pidgin i OTR.
https://otr.cypherpunks.ca/

Afegiu el vostre compte al Pidgin/Audium i genereu les claus de xifrat. Deseu còpia de users/pwds i claus al KeePass!

5- Trobar dispositius robats

Si perdem o ens roben l'ordinador, tauleta o telèfon, no n'hi ha prou amb tenir un còpia de seguretat, password que bloquegi l'entrada o xifrades les dades. Volem poder recuperar el dispositiu.

Consells:

- La prevenció és el primer pas. Atenció on o a qui deixeu els dispositius
- Cal protegir el dispositiu amb un password de bloqueig
- Cal xifrar el contingut del disc o tarja SD
- Cal tenir còpies de seguretat recents, distrubuïdes i millor si xifrades
- Cal activar l'auto-esborrat (iPad) després de 10 o més errors en el PIN de desbloqueig

Objectius:

- Instal·lar i provar *Preyproject*.
- Saber com posar un password a la BIOS de l'ordinador

Pràctica 17: Prey project

És un servei de seguiment i localització fet en codi obert. Si bé ofereix un serveis *premium* de pagament ofereix gratuïtament la possibilitat de controlar fins a tres dispositius per usuari.

Prey es centra en la recuperació de dispositius robats o "perduts" i trobats per tercers. El programa i el codi de Prey és 100% obert i es pot consultar, fet que permet que qui vulgui comprovi que fa la seva feina bé i sense passar dades a tercers no autoritzats. Si no us fieu de Prey project, podeu descarregar el programari i instal·lar-lo en un servidor vostre.

Prey no envia dades al servidor si no és que des de la web de Preyproject no el declarem com a perdut. En aquest cas, Prey, que fins aquest moment ha estat dormint en el nostre dispositiu, es desperta i mira d'enviar la informació que des del nostre compte a la web de Preyproject, demanem que ens enviï.

1. Aneu a **https://preyproject.com/** descarregueu l'aplicació pel vostre dispositiu i instal·leu-la
2. Doneu les dades del compte que obrireu a Prey
    - Recordeu el que hem practicat abans amb els passwords i KeePass!
3. Acabada la instal·lació, aneu a la plana de Preyproject
4. Entreu i configureu el tipus de report que voleu rebre i salveu els canvis
5. Declareu el dispositiu com "Missing" i salveu el nou estat
6. Espereu una estona i comproveu a l'apartat de "Informes"
7. Vist l'informe, declareu el dispositiu com "Ok" i salveu el nou estat.

Tenir protegit l'accés a l'ordinador amb un password pot no activar Prey, i ells recomanen tenir un compte "Convidat" sense privilegis d'Administrador de l'ordinador i si pot ser amb limitacions de les accions que pot fer.

- FI -