SÉCURITÉ
PROTECTION
SAUVEGARDE

- *De votre matériel*
- *De vos données*
- *De votre vie privée*

Quels sont les risques encourus

Comment s’en protéger

Adapter la réponse à la menace

Le risque :

Pertes ou vol de vos données de travail ou personnelles
c.a.d. vos fichiers d'applications, photos, audio vidéo …

… mais aussi vos donnée de connexion, mots de passe divers

… mais aussi vos donnée personnelles bancaires, codes cartes

… chantage (cryptage de vos données)

… compromission de vos compte internet (reseaux sociaux)

CECI ETANT DIT (et peut être fait)

EXAMINONS QUELQUES POINTS

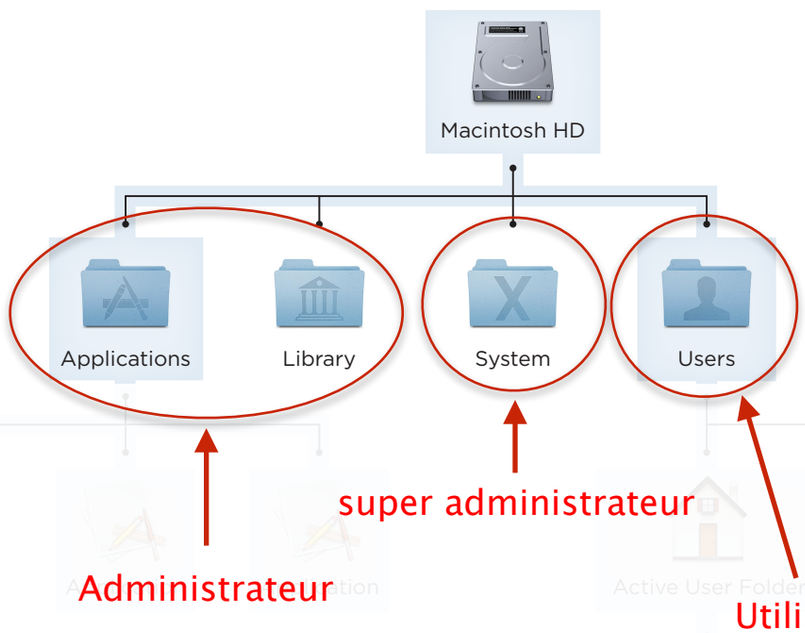
Sans être paranos, ne laissez pas n'importe qui regarder ce qu'il y a sur votre ordinateur.

Les mots de passe

- Protégez votre session - mise en veille
- MDP Facile à retenir (xpJy@n+&%Uf528##gloups!)
- Phrase de passe
- Une phrase par service
- l'écrire pour s'en rappeler
- Stockage des MDP (Onepassword)
- test : http://howsecureismypassword.net

OS X FILE STRUCTURE

Visual Guide of File and Folder Organization in OS X



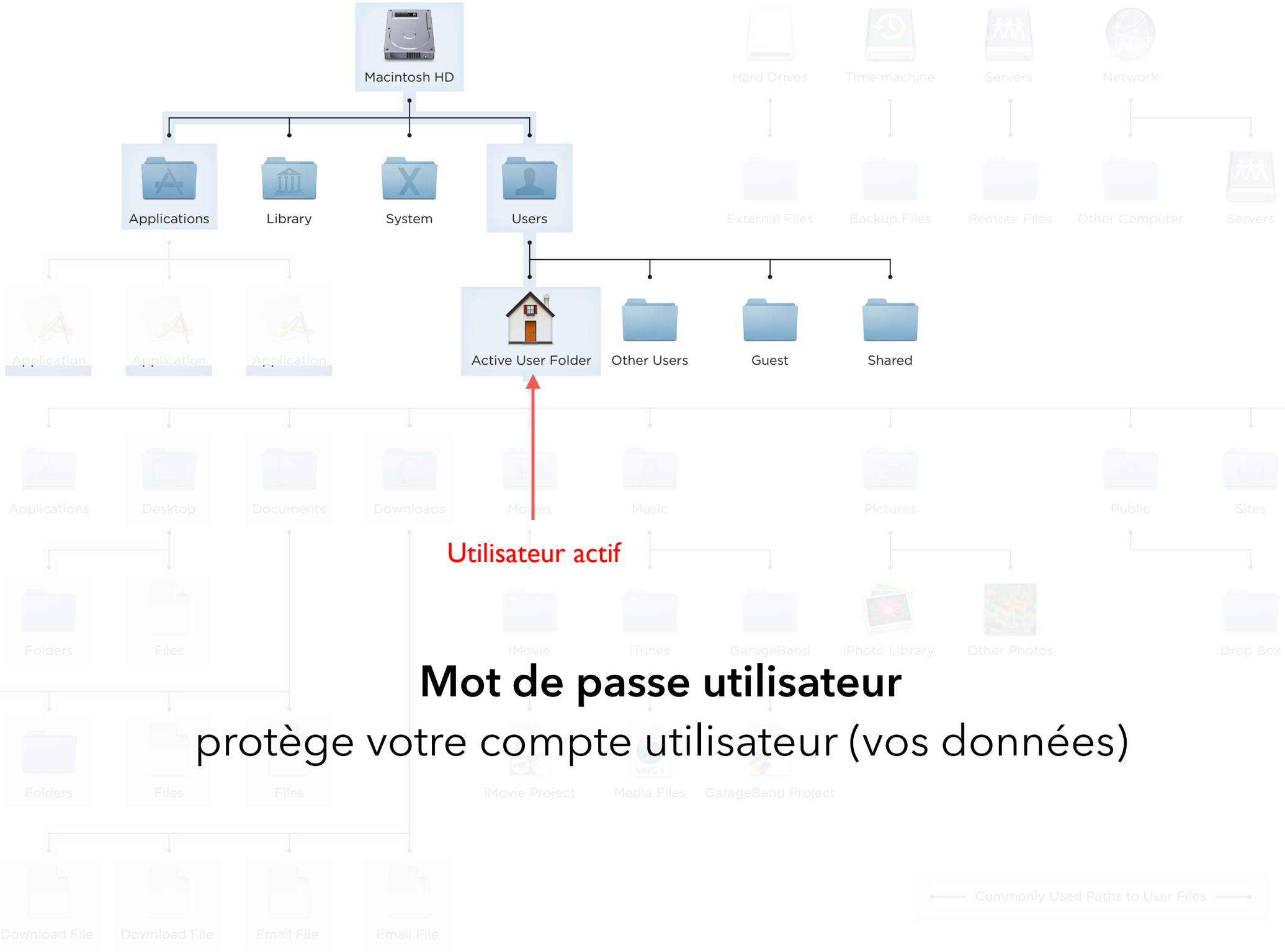
Administration

Mot Passe Administrateur

protège votre système

OS X FILE STRUCTURE

Visual Guide of File and Folder Organization in OS X



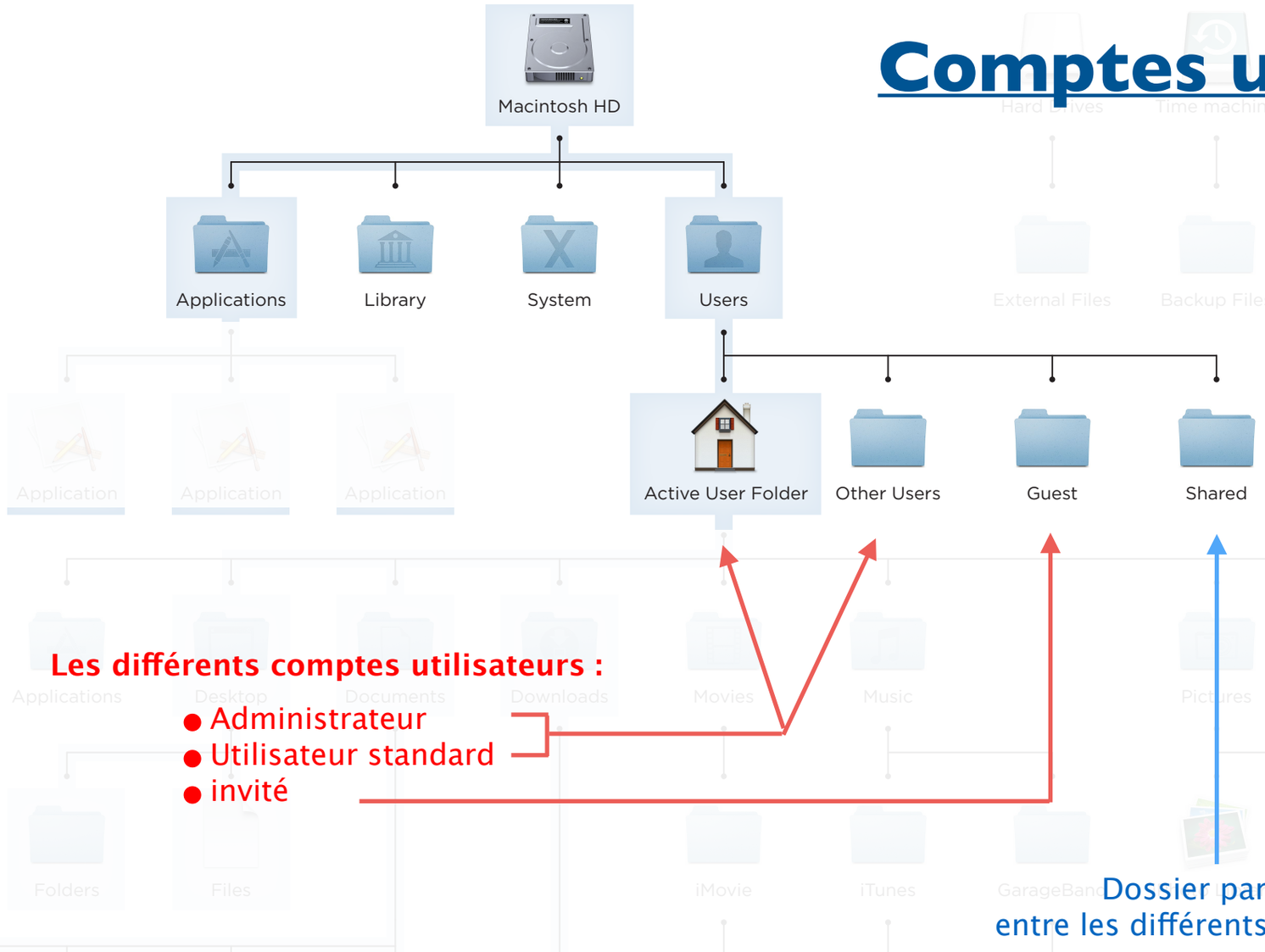
Mot de passe utilisateur

protège votre compte utilisateur (vos données)

OS X FILE STRUCTURE

Visual Guide of File and Folder Organization in OS X

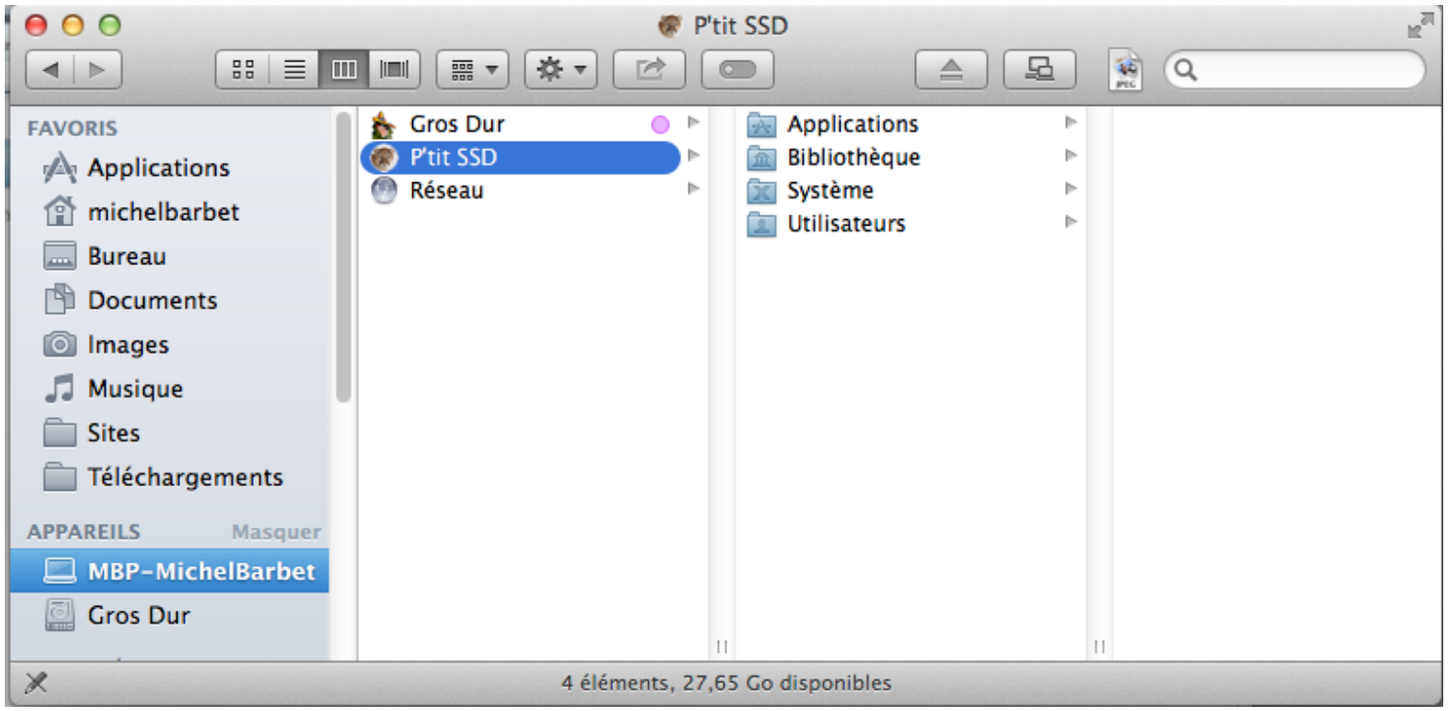
Comptes utilisateurs



Travaillez de préférence avec un compte Standard ou invité

OS X FILE STRUCTURE

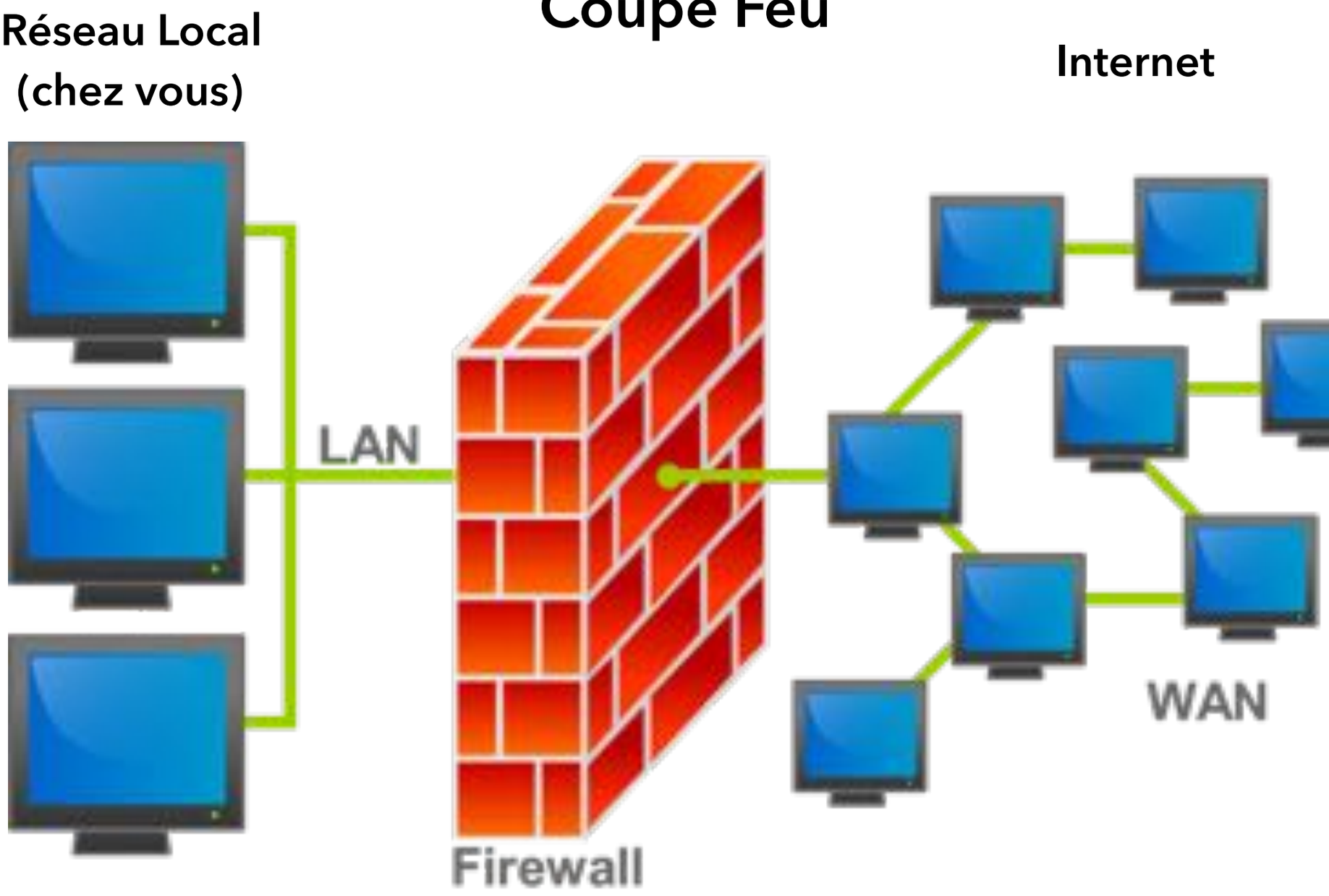
Visual Guide of File and Folder Organization in OS X

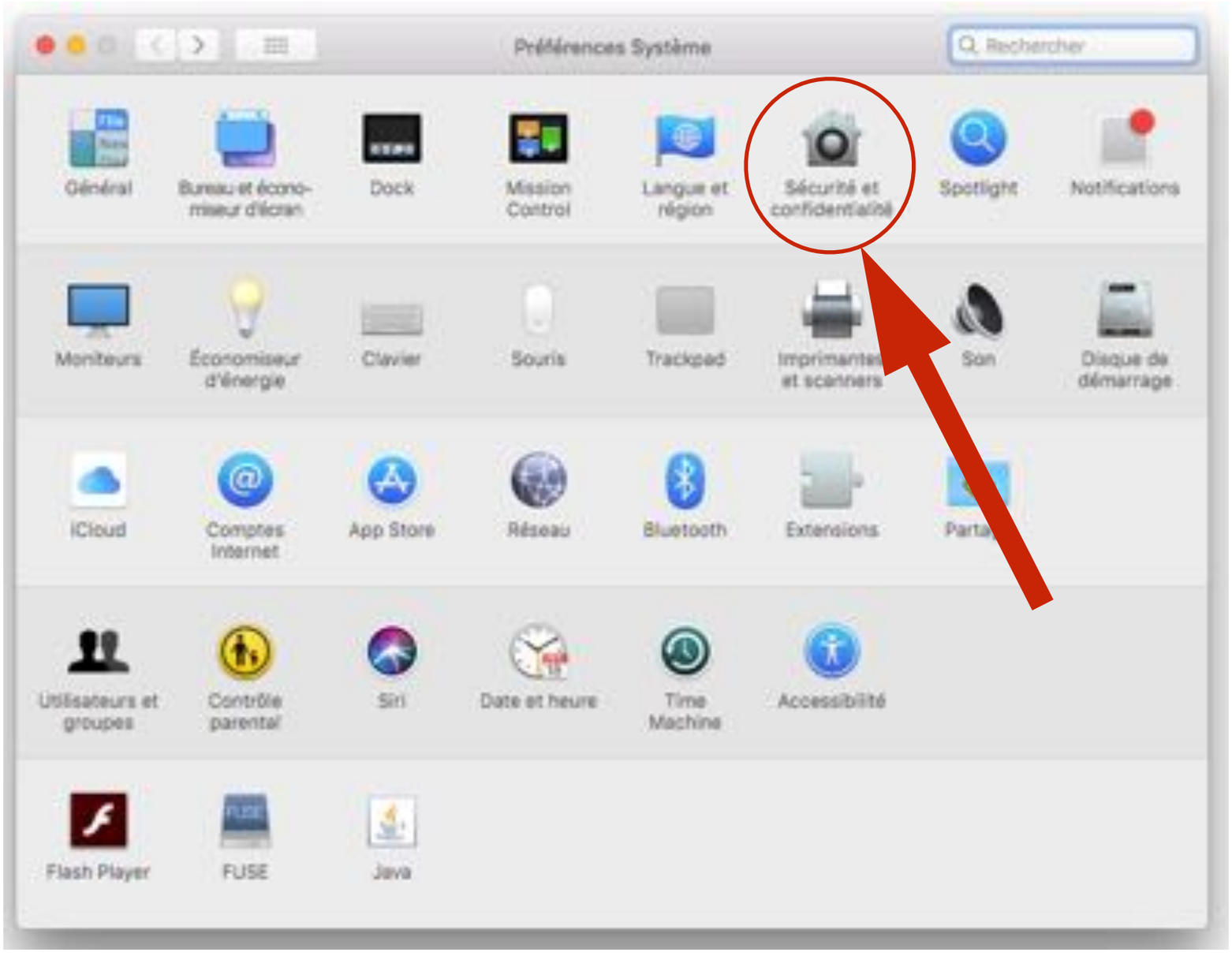


Sessions


Utilisateurs et groupes
Tout afficher
Utilisateur actuel
Michel Barbet
Admin
Autres utilisateurs
Formation
Standard
Andrebarbet
Standard
Utilisateur invité
Ouverture seulement
Options
Mot de passe
Ouverture
Modifier le mot de passe...
Nom complet :
Michel Barbet
Identifiant Apple :
Définir...
Fiche de Contacts :
Ouvrir...
Autoriser la réinitialisation du mot de passe avec l'identifiant Apple
Autoriser l'administration de cet ordinateur
Activer le contrôle parental
Ouvrir les contrôles parentaux...
Pour modifier, cliquez sur le cadenas.

Coupe Feu




Préférences Système
Rechercher
Général
Bureau et économiseur d'écran
Dock
Mission Control
Langue et région
Sécurité et confidentialité
Spotlight
Notifications
Moniteurs
Économiseur d'énergie
Clavier
Souris
Trackpad
Imprimantes et scanners
Son
Disque de démarrage
iCloud
Comptes Internet
App Store
Réseau
Bluetooth
Extensions
Partage
Utilisateurs et groupes
Contrôle parental
Siri
Date et heure
Time Machine
Accessibilité
Flash Player
FUSE
Java


Sécurité et confidentialité
Bloquer toutes les connexions entrantes
Bloque toutes les connexions entrantes sauf celles nécessaires aux services internet de base, comme DHCP, Bonjour, et IPSec.
Partage d'écran
Autoriser les connexions entrantes
Partage d'imprimante
Autoriser les connexions entrantes
Partage de fichiers (AFP, SMB)
Autoriser les connexions entrantes
1Password mini
Autoriser les connexions entrantes
aMule
Bloquer les connexions entrantes
BitTorrent
Bloquer les connexions entrantes
Autoriser automatiquement les logiciels intégrés à recevoir des connexions entrantes
Autoriser automatiquement les logiciels signés téléchargés à recevoir des connexions entrantes
Cette option permet aux logiciels signés par une autorité de certification valide de fournir des services dont l'accès s'effectue depuis le réseau.
Activer le mode furtif
Ne pas répondre à ou reconnaître des tentatives d'accès à cet ordinateur depuis le réseau par des applications de test via ICMP, tel que Ping.
Annuler
OK
Pour empêcher les modifications, cliquez sur le cadenas.
Avancé...

Utiliser internet

Naviguer sur le Web

Cookies

validation URL

logique

prudence sur les réseaux sociaux

Achats : site sécurisé (https - 🔒)

téléchargement : légal sinon Hadopi ...

Utiliser internet

Comprendre une URL

http://compteclient.orange.fr

protocole

http : **H**yper **T**ext **T**ransfert **P**rotocol
https: **H**yper **T**ext **T**ransfert **P**rotocol **S**ecure
ftp : **F**ile **T**ransfert **P**rotocol

Utiliser internet

Comprendre une URL

http://compteclient.orange.fr

Sous domaine

Utiliser internet

Comprendre une URL

http://compteclient.orange.fr

domaine

Utiliser internet

Comprendre une URL

http://compteclient.orange.fr

tld : domaine 1er niveau

.fr
.eu
.net
.org
.com
.gouv

Utiliser internet

Le courrier électronique

adresse électronique

nom d'utilisateur @ nom de domaine

titulaire du compte — *entreprise ou organisation ou fournisseur d'accès*

arobase

tours.micro.club @ numericable.fr

nom utilisateur : tours.micro.club
mot de passe : #########

Utiliser internet

http://orange.compte.fr

http://compte.orange.fr

mail@orange.compte.fr

mail@compte.orange.fr

Utiliser internet

Utiliser internet

Techniques d'attaque par messagerie

SPAM : Le spam, ce sont des emails publicitaires indésirables

- activez les filtres antispam, le filtrage du courrier indésirable
- n'achetez pas ce qui vous est proposé
- n'essayez pas de vous désinscrire
- si l'adresse du mail ne vous dit rien, n'ouvrez pas le message

HOAX : canular, souvent une chaîne de solidarité. Peux vous inciter à faire des manipulations dangereuses sur votre ordinateur.

SCAM : un dignitaire d'un pays d'Afrique vous demande de servir d'intermédiaire pour une transaction financière importante, en vous promettant un bon pourcentage. Pour amorcer la transaction, il vous faut donner de l'argent. C'est bien entendu une arnaque.

L'Hameçonnage (filoutage – fishing) :vous recevez un message imitant le format des message. d'un fournisseur, d'une banque, d'une société. Le but est de vous soutirer vos coordonnées, n° de carte… ou de l'argent.

Utiliser internet

La messagerie électronique

- Vérifiez l'adresse de l'expéditeur, il n'existe pas à priori d'expéditeur de confiance
- Méfiez vous des pièces jointes
- Ne répondez pas à une demande d'informations confidentielles
- Aucune banque/organisme ne vous demandera n° carte ou de compte par mail
- Attention aux chaines de solidarité, ce sont des canulars ou des escroqueries
- www.hoaxbuster.com
- Vérifiez les liens dans les messages, l'ortaugraffe et le vocabulaire
- paramétrez correctement votre logiciel de courrier électronique (préférences)

Virus - Malware - Adware

Quelques éléments de réflexion :

Le Mac est toujours infiniment moins visé par les attaques que Windows

Le Mac intéresse de plus en plus les cybercriminels

les utilisateurs Mac n'ont pas l'habitude de se protéger

Apple semble trop laxiste en matière de sécurité

Fonction « mise en quarantaine » basique et limité

Gatekeeper comporte des vulnérabilités

Prolifération des « Adware » sur Mac

Malware - Adware

Les malwares (contraction de « malicious » et « software »)

Ce sont des logiciels malveillants.

Leur but est d'accéder à l'appareil d'un utilisateur à son insu.

Ces types de logiciels incluent les logiciels espions, les logiciels publicitaires, les virus, les chevaux de Troie, les vers informatiques, les rootkits, les logiciels de rançon et les détourneurs de navigateur.

Malware - Adware

Mac OS X n'est pas totalement à l'abri des Malwares

Faut-il un anti-virus sur mac ?

- ✦ Jusqu'à maintenant : pas sûr
- ✦ Maintenant : posons nous la question !

http://www.securitemac.com/mac-pas-plus-sur-que-windows.html
http://www.securitemac.com/antivirus-mac

Malware - Adware

Que faut-il en déduire :

Que rien n'est définitif !

Quand ça change … ça change, même quand y'a d'la pomme !

Activez le firewall de votre Mac

Utilisez un compte standard

N'utilisez pas « Flash » ou mettez le à jour

Désactivez Java dans votre navigateur (activez le à la demande)

Téléchargez les applis de développeurs identifiés

Faites les mises à jour système et des applications

N'ouvrez pas les mails non identifiés

Ne naviguez pas vers n'importe quel site

Malware - Adware

AdWare

“Programmes” qui génèrent des fenêtres publicitaires, changent la page d’accueil de votre navigateur et modifient parfois vos préférences de moteurs de recherche.

Ils sont le plus souvent “packagés” dans les installeurs d’autres programmes

Contractés via (entre autres) :

- ➡ sites de téléchargement (Download.com, Softonic …)
- ➡ certains logiciels gratuits (ou non)
- ➡ les sites de téléchargement audio/video, type “torrent”
- ➡ les sites de piratage

Malware - Adware

Il est facile de s'en prémunir en ne téléchargeant que depuis des sources réputés sûres (sites d'éditeurs fiables .)… 😊

Sinon on peut s'en débarrasser avec un logiciel gratuit
Malwarebytes anti-malware for mac (pb c'est en anglais 😕)

Malware - Adware

Sauvegarde de vos données personnelles

- Time Machine (sauvegarde incrementielle)
  - simple à utiliser,
  - pas de prise de tête pour gérer les sauvegardes
  - permet de récupérer fichiers et dossier dans le temps
  - concerne toutes les données
- Clone de votre disque (périodicité à définir)
  - utilisable pour démarrer le Mac
  - permet de reconstituer le disque au jour du clonage
- Archiver vos documents importants (personnels)
  - Mettre en sécurité les données
  - Dégage de la place sur le disque du Mac

Faites ces sauvegardes sur des disque distincts !

Sauvegarde de vos données personnelles

Time machine

- Sur un volume Externe (pas sur le disque interne du Mac)
- Utilisez un disque (ou SSD) USB ou Time Capsule
- Taille suffisante pour être tranquille

Time capsule = borne WiFi Airport + disque dur

Sauvegarde de vos données personnelles

Cloner le disque

- Disque externe USB
- Capacité équivalente au disque à cloner
- Définir périodicité : hebdomadaire-mensuelle- trimestrielle …
- logiciels : utilitaire système ou logiciels tiers

Carbon Copy Cloner

SuperDuper

StellarDriveClone

CloneX4

Versions d’essai limitée en fonctions ou dans le temps

Sauvegarde de vos données personnelles

Archivage

- A vous de le définir
- Par ex : photos, documents personnels
- Compresser
- sécurité : image disque codée (.dmg)

Sauvegarde de vos données personnelles

RAPPEL

- Sauvegardez vos mots de passe (notez les)
- idem pour les informations de connection
- idem pour vos n°de licences (ça parait évident !)
- Eventuellement utilisez un logiciel (1password)

Comment se protéger :

CONNAITRE LE FONCTIONNEMENT DE MACOS
ET SON SYSTEME DE FICHIERS

Pour éviter les erreurs de manipulation

effacement de fichiers

erreurs d'enregistrement

Faites les mises à jour

Comment se protéger :

UTILISER DES MOTS DE PASSE DE SESSION

UTILISER UN COMPTE INVITE ou STANDARD
(pas Administrateur)

ACTIVER LE FIREWALL
(Ordinateur et Box)

SOYEZ PRUDENTS SUR LE WEB
(Sites visités - Option de sécurité navigateur)

COURRIER ELECTRONIQUE
(Spam-mails bizarres)

ATTENTION AUX UTILITAIRES EXOTIQUES …

ET SURTOUT :

FAITES DES SAUVEGARDES


Fin