

M1

Sécurité des systèmes d'informations

2023-2024

SESSION

3
Partie
2



Aujourd’hui : Session 3 : Hygiène numérique

- Correction TP 2
- Connaître le Système d’Information
- Maîtriser le réseau
- Sécuriser les terminaux
- Gérer les utilisateurs
- Sécuriser physiquement
- Contrôler la sécurité du S.I.
- Nomade





- Connaître le Système d'Information
- Maîtriser le réseau
- Sécuriser les terminaux
- Gérer les utilisateurs
- Sécuriser physiquement
- Contrôler la sécurité du S.I.
- Nomade

Attribution de privilèges : Grands principes (1/2)

- Moindre privilège :
 - n'attribuer aux utilisateurs que les droits
 - dont ils ont besoin pour effectuer leurs tâches ;
 - ne pas donner les privilèges importants à tous les utilisateurs, seulement à ceux qui en ont besoin ;
 - Exemple : le privilège « Administrateur »
 - pour un visiteur qui a juste besoin d'accéder à Internet :
 - ne pas lui donner un accès aux disques ou aux applications sensibles.

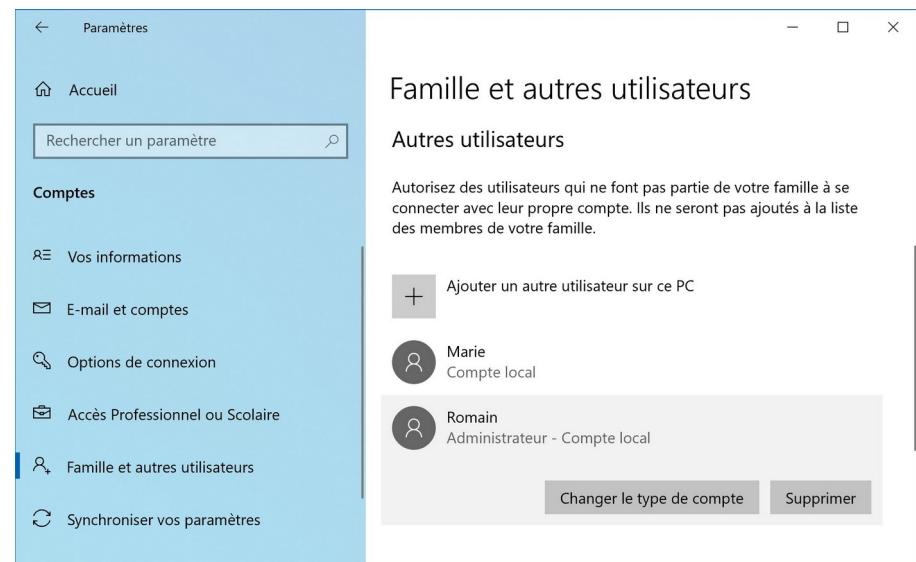
Attribution de privilèges : Grands principes (2/2)

- Besoin d'en connaître :
 - Donner les accès et les privilèges appropriés aux utilisateurs :
 - donner accès seulement aux données nécessaires aux utilisateurs
 - restreindre l'accès aux répertoires contenant les données sensibles

DROIT	UTILISATEUR ANONYME	UTILISATEUR AUTHENTIFIÉ	ADMINISTRATOR
Backup and Migrate			
Accéder à Backup and Migrate	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Accéder à la section d'administration de Backup and Migrate.			
Effectuer une sauvegarde	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Sauvegarde n'importe quelle base de donnée disponible.			
Accéder aux fichiers de sauvegarde	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Accéder et télécharger les fichiers de sauvegardes créés précédemment.			
Supprimer des fichiers de sauvegardes	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Supprimer les fichiers de sauvegardes créés précédemment.			
Restaurer le site	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Restaurer la base de donnée du site depuis un fichier de sauvegarde.			
Administre Backup and Migrate	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Modifier les profils, les plannings et les destinations de Backup and Migrate.			
Block			
Administrer les blocs	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Contextual links			
Utiliser les liens contextuels	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Utilisez les liens contextuels pour réaliser des tâches liées à des composants d'une page.			
Custom breadcrumbs			

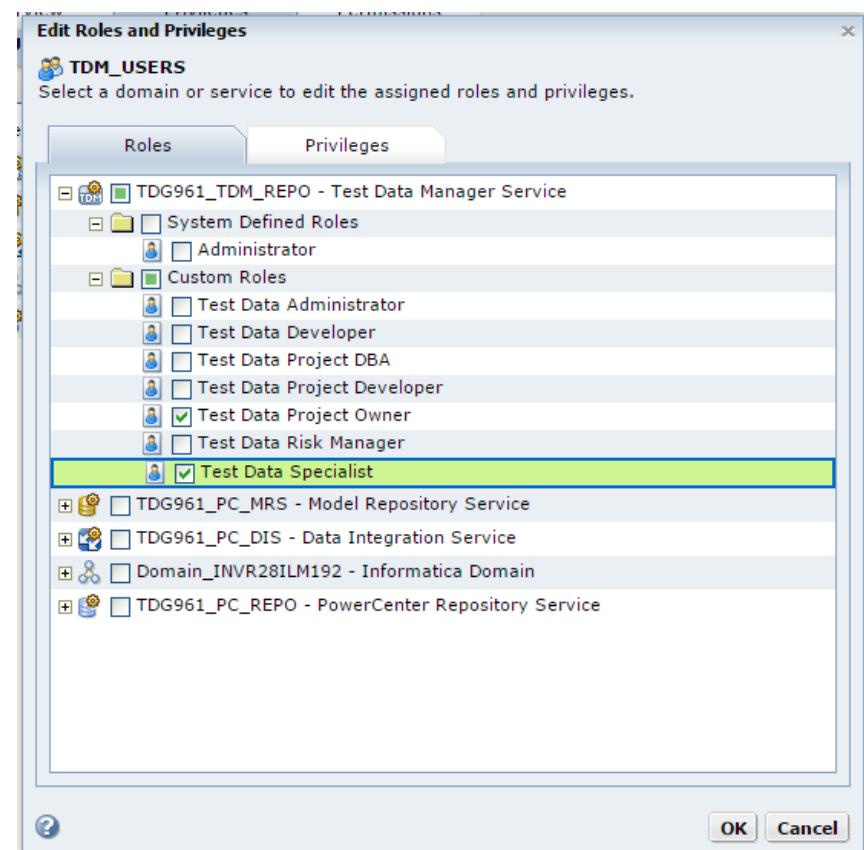
Attribution de privilèges : recommandations (1/2)

- Attribuer les comptes aux utilisateurs de manière nominative ;
 - Un utilisateur = un compte ;
 - Tracer les actions effectuées par chaque utilisateur ;
 - Éviter les comptes partagés entre plusieurs utilisateurs.



Attribution de privilèges : recommandations (2/2)

- Faire signer une charte d'utilisation du SI, informant sur :
 - La conduite à tenir lors de l'usage du SI ;
 - Actions encouragées :
 - Utiliser son poste pour des recherches, pour le travail qui est confié ;
 - protéger ses moyens d'accès : badge, identifiant, etc.
 - Actions interdites :
 - installer des logiciels malveillants / arrêter les outils de détection de codes malveillants ;
 - porter atteinte à un autre utilisateur du SI.
 - Les conditions et les règles d'utilisation des ressources du S.I. ;
 - Les responsabilités de l'utilisateur et ceux de l'entreprise/université ;
 - Les sanctions internes, pénales, civiles encourues ;

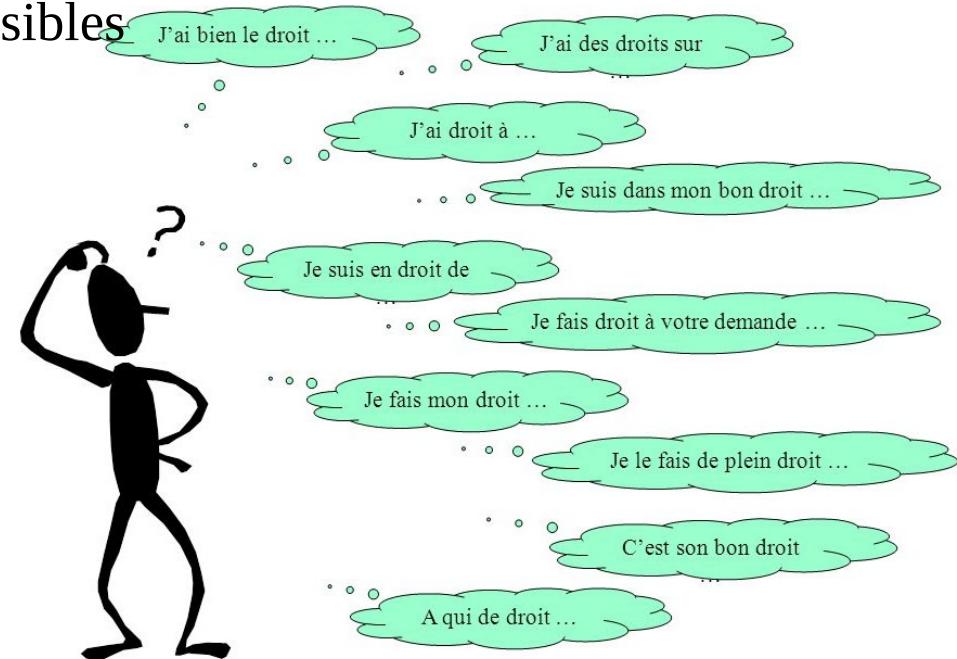


Attribution de privilèges :

- procédures d'attribution / retrait de privilèges
- Définir une procédure d'attribution/retrait de privilèges.
 - Tenir à jour une liste des droits attribués à chaque utilisateur ;
 - Chaque nouveau compte utilisateur doit être créé en respectant les principes d'attribution de privilège ;
 - Au besoin, chaque utilisateur doit avoir son répertoire personnel et sa boite aux lettres ;
 - Lorsque qu'un utilisateur n'a plus besoin d'accéder au système (démission, changement de poste...), la procédure de retrait de droit doit :
 - Décrire la désactivation de son compte et la suppression de son compte ;
 - Décrire la procédure de retrait des accès aux locaux (badge, clés).

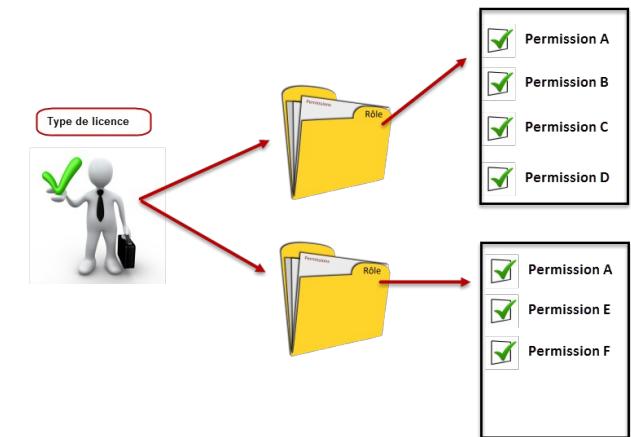
Attribuer les bons droits

- Les ressources sensibles du SI
 - Ressources précieuse pour un pirate
 - Répertoire contenant les données sensibles
 - Bases de données
 - Boîtes aux lettres électroniques
 - Etc.
- Bonnes pratiques
 - Définir la population → Accès
 - De contrôler strictement son accès
 - Personne ciblée
 - S'assurer les utilisateurs sont bien authentifiés
 - Eviter :
 - Duplication des codes
 - Contrôle d'accès moins strict



Rôles Utilisateur (1/2)

- Administrateur
 - Ayant les privilèges les plus élevés sur le système.
 - Il peut être de plusieurs types :
 - Administrateur système : en charge de l'administration des systèmes, de la gestion des disques
 - Administrateur réseau : en charge des équipements réseaux, des règles de filtrage
 - Administrateur sécurité : en charge de la journalisation, de la supervision
- Utilisateur
 - Ayant le droit d'utiliser le système
 - Accéder à des répertoires sensibles
- Invité
 - Ayant peu de droits
 - Pas d'accès aux répertoires contenant les informations sensibles



Rôles Utilisateur (2/2)

	Administrateur	Éditeur	Auteur	Contributeur	Abonné
Gérer les réglages : thèmes, extensions...	✓	✗	✗	✗	✗
Gérer les pages	✓	✓	✗	✗	✗
Gérer <u>tous</u> les articles	✓	✓	✗	✗	✗
Gérer <u>tous</u> les commentaires	✓	✓	✗	✗	✗
Gérer les commentaires de <u>ses</u> articles	✓	✓	✓	✗	✗
Publier <u>ses</u> articles	✓	✓	✓	✗	✗
Importer des médias	✓	✓	✓	✗	✗
Rédiger des articles	✓	✓	✓	✓	✗

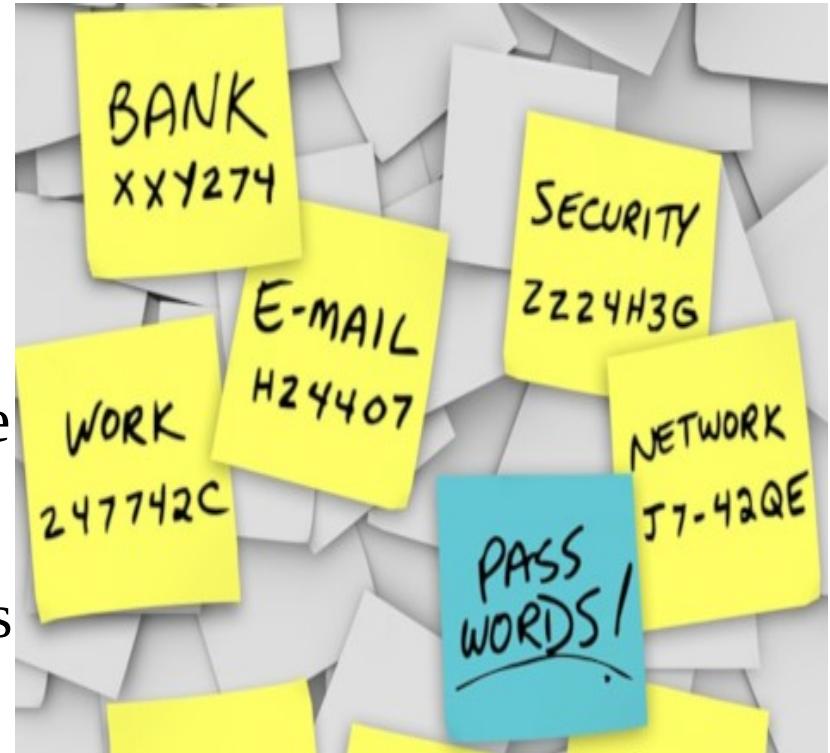
Mots de passe : politique de mots de passe

- Définir une politique de mot de passe qui oblige à
 - Créer un mot de passe complexe :
 - différent d'un mot sorti du dictionnaire
 - différent d'une date de naissance (celle de votre conjoint, enfant...)
 - différent d'une partie du nom d'utilisateur, du nom, ou du prénom, etc.
 - Changer régulièrement les mots de passe (tous les 6 mois) ;
 - la fréquence des changements dépend de la sensibilité des systèmes accédés, par exemple le code pour accéder en ligne à son compte bancaire sera changé plus régulièrement.
 - Utiliser un mot de passe pour déverrouiller l'écran de veille.
- Consulter les recommandations élaborées par l'ANSSI.

<https://www.ssi.gouv.fr/guide/recommandations-relatives-a-la-authentification-multifacteur-et-aux-mots-de-passe>

Directive du mot de passe

- Mot de passe d'une longueur minimale de
 - 8 caractères (utilisateurs)
 - 14 (administrateurs)
- Composés de différentes combinaisons
 - Majuscule, Minuscule, Chiffres, Caractères spéciaux
- N'utilisez pas les six derniers mots de passe
- Changez régulièrement
 - (au moins une fois en 90 jours) = 3 mois
- Plusieurs tentatives erronées
 - compte bloqué



!\\ Les configurations et les développements
→ les mots de passe doivent respecter au minimum ces règles

Mots de passe : mémorisation

- Ne pas choisir le même mot de passe pour différents comptes.
 - Même si ce principe devient difficile à respecter au vu du nombre de mots de passe que les utilisateurs doivent se rappeler ;
 - A minima, ne jamais réutiliser son mot de passe de messagerie. Le compte email devient en effet le pivot numérique de chacun.
 - En cas de perte de mot de passe, c'est souvent grâce à la boite email que l'on est en mesure d'en régénérer un nouveau ;
 - L'email sert aux sites marchands pour nous identifier lors de l'ouverture d'un compte ;
 - Si le compte email se fait pirater, c'est une partie significative de la vie numérique de l'utilisateur qui est affectée (usurpation d'identité, suppression malveillante de documents, changement forcé de mots de passe et impossibilité de les régénérer...).

Résistance d'un mot de passe

- Longueur : 8 à 28 caractères
 - 8 caractères
I63c0SLe!
3 semaines
- Composé :
 - Majuscules :
 - ABCDEFGHIJKLMNOPQRSTUVWXYZ
 - Chiffres :
 - 0123456789
 - Caractères spéciaux :
 - !@#\$%^&*(){};:<,.?/\+-_=^[]~"
 - Minuscules :
 - abcdefghijklmnopqrstuvwxyz

Vérifier le votre : <https://www.security.org/how-secure-is-my-password/>

Mots de passe : stockage des mots de passe

- Toujours stocker les mots de passe sous forme chiffrés
- Mauvais exemple : Sony, répertoire nommé « Password » et contenant les mots de passe « en clair » ;
- Utiliser des « porte-feuilles » de mots de passe :
 - Dashlane – KeyPass XC – 1Password
- ou créer votre « porte-feuille », chiffré et protégé par un mot de passe fort.
- Ne pas enregistrer les mots de passe sur les navigateurs Web



Face aux limites des mots de passe et à leur difficulté d'utilisation, de nouveaux moyens d'authentification sont proposés.

COMBIEN DE TEMPS FAUT-IL À UN PIRATE POUR TROUVER VOTRE MOT DE PASSE EN 2023 ?

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
5	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
6	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
7	Immédiat	Immédiat	1 seconde	2 secondes	4 secondes
8	Immédiat	Immédiat	28 secondes	2 minutes	5 minutes
9	Immédiat	3 secondes	24 minutes	2 heures	6 heures
10	Immédiat	1 minute	21 heures	5 jours	2 semaines
11	Immédiat	32 minutes	1 mois	10 mois	3 ans
12	1 seconde	14 heures	6 ans	53 ans	226 ans
13	5 secondes	2 semaines	332 années	3 000 années	15 000 ans
14	52 secondes	1 an	17 000 ans	202 000 ans	1 million d'années
15	9 minutes	27 ans	898 000 ans	12 millions d'années	77 millions d'années
16	1 heure	713 ans	46 millions d'années	779 millions d'années	5 milliards d'années
17	14 heures	18 000 ans	2 milliards d'années	48 milliards d'années	380 milliards d'années
18	6 jours	481 000 ans	126 milliards d'années	1 trillion d'années	26 trillions d'années

<https://www.francenum.gouv.fr/magazine-du-numerique/combien-de-temps-un-pirate-met-il-pour-trouver-votre-mot-de-passe-comment>

Autres méthodes d'authentification

- Biométrie ;
 - permet l'authentification par la lecture des attributs physiques peu changeant d'une personne : empreinte digitale, voix, rétine, etc. ;
- Carte à puce + code pin ;
- SSO : Single Sign-On ;
 - L'utilisation du SSO permet d'éviter que les utilisateurs aient à ressaisir leurs mots de passe
 - Utilisation d'un seul formulaire d'authentification pour accéder à différents services
- Double Authentication
 - Ex :Google Authenticator - Authenticator...
- OTP(One Time Password).
 - Généré à chaque demande et utilisable une seule fois. Sa durée de validité très courte :
 - Un OTP peut être un code de validation de paiement en ligne reçu par sms ;
 - ou généré par un générateur matériel de jetons sécurisés.



Token Safenet



Sensibilisation des utilisateurs (1/3)

- Se tenir informé de l'actualité liée à la sécurité :
 - des vulnérabilités publiées
 - fuite d'information : Sony
 - « scam » appelé 419 ou arnaques sur Internet :
 - arnaque à la nigériane, etc.
- Faire attention aux pièces jointes
 - Même pour les expéditeurs connus
 - Télécharger d'abord
 - Faire un scan avec l'antivirus,
 - Avant d'ouvrir la pièce jointe.

Sensibilisation des utilisateurs (2/3)

- Désactiver l'exécution
 - Des liens hypertextes
 - Affichage des images dans les mails ;
- Préférable de copier et coller le lien hypertexte dans le navigateur.
 - Technique du phishing consiste à faire afficher un lien qui paraît légitime à la lecture,
 - mais qui pointe en fait vers une site malveillant.
 - Cette technique ne fonctionne que si on clique sur le lien.
- Faire attention aux ralentissements/lenteurs de son poste ;
- Applications web
 - penser à cliquer sur le bouton déconnecter
 - lorsqu'on a finit de surfer sur le site afin de désactiver le cookie ;
- Déconnecter son poste lors qu'il n'est pas utilisé.

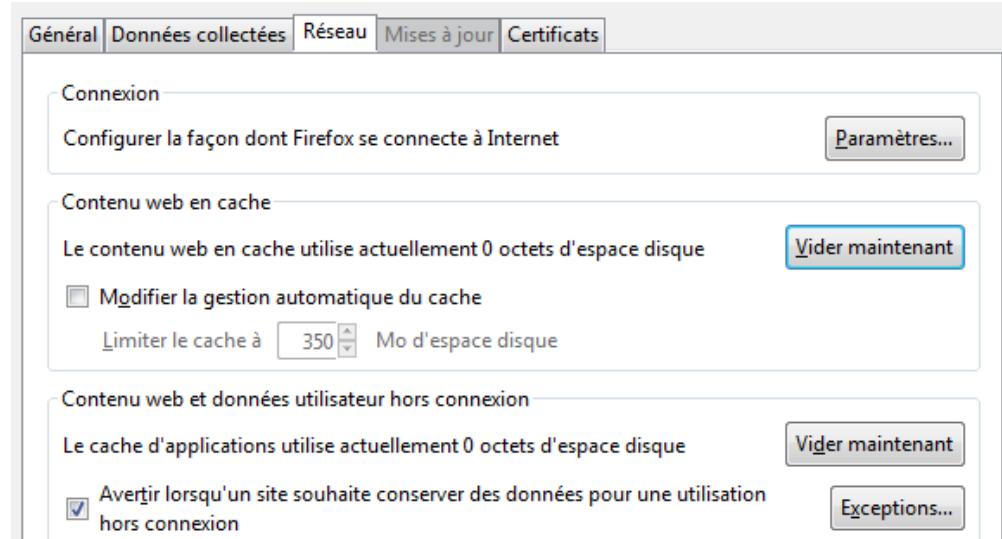


Sensibilisation des utilisateurs (3/3)

- Éviter les sites dont les certificats proposés ne sont pas reconnus :

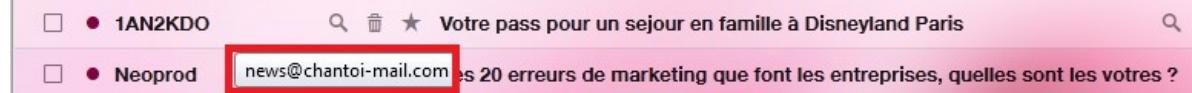


- Dans la mesure du possible
 - naviguer toujours en « https »
- Cela est d'autant plus important
 - sur les hotspots publics !
- Effacer régulièrement l'historique de navigation :
 - les fichiers temporaires,
 - les cookies votre navigateur Web.



Spam

- Traiter le spam
 - protéger son adresse mail
 - au besoin, créer une adresse poubelle : xxx@yopmail.com
 - marquer les mails indésirables
 - comme tel afin d'affiner la politique de détection des spams
 - ne pas ouvrir les spams, et ne pas cliquer sur les liens contenus
- Faire attention aux mails envoyés dont l'émetteur est inconnu
- Faire attention aux contenus des mails



P. St, You are receiving this message because you opted-in your email address
@yahoo.com to receive emails from diploe.antsy.bgxxbx.com.

If you would like to be removed from our mailing list, please [click here](#).

To ensure ongoing optimal receipt of these communications, please add
customerservice@tabard.bgxxbx.com to your address book.

If, for any reason, this promotion is not capable of running as planned, sponsor reserves the right to
cancel, terminate, modify or suspend the promotion. This includes, but is not limited to, infection by
computer virus, bugs, tampering, unauthorized intervention, fraud, technical failures or any other causes
beyond the control of the sponsor. Why did the Onion Price Go Up So Suddenly?.. BecauseRajnikanth
Ordered An Onion Dosa. ! :)

Phishing / Spear phishing / Social engineering (1/2)

- Ne pas donner suite au mail, coup de fil vous demandant de :
 - Rappeler rapidement votre conseiller bancaire alors que vous ne l'avez pas contacté ;
 - Donner des informations personnelles parce que vous avez gagné un voyage, un prix, etc.
 - D'envoyer votre mot de passe/code bancaire/code pin par mail sous le prétexte urgent :
 - d'éviter la fermeture de votre adresse mail (car vérification en cours) ;
 - de valider l'existence de votre carte bancaire désactivée, etc.
 - De faire un transfert d'argent à un de vos contacts dans le besoin à l'étranger.

En cas de doute, renseignez-vous mais ne répondez pas au mail.

Phishing / Spear phishing / Social engineering (2/2)

- Limiter les informations que vous partagez

- par les réseaux sociaux ou mail

- Date de départ en voyage

- <http://pleaserobme.com> : sur la base de tweet (position) indique les maisons vides.

- Informations personnelles

- Données (photos/vidéos) potentiellement compromettantes ;

- Chantage menant à des suicides d'adolescents « chantage à webcam »

- Quelques liens utiles :

- <http://www.arnaque-chantage-webcam.com/>
 - <http://www.laveudunet.com/>
 - <http://blog.mavieprivee.fr/post/34628211803/chantage-a-la-webcam>

Le jeune homme, prénommé Gauthier, a mis fin à ses jours le 10 octobre après avoir été victime d'un chantage sur Facebook de la part d'une jeune fille avec qui, il venait de faire virtuellement connaissance

En janvier, Cédric, 17 ans, s'est pendu dans sa chambre à Marseille, 3 mois après avoir été piégé au cours d'un "plan webcam"

Réagir en tant que victime

- Ne jamais payer de rançons ;
- En cas de chantage / usurpation d'identité / atteinte à la réputation :
 - Ne communiquez plus avec l'escroc ;
 - bloquer ses messages / son contact.
 - Signalez et recevez de l'aide ;
 - Faire bloquer ce contact sur le site du chat, ou sur Facebook ou Skype ;
 - exercer le droit à l'oubli sur Google :
https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=fr
 - signaler : <https://www.internet-signalement.gouv.fr/>
 - pour les mineurs : <http://www.netecoute.fr/>
- En cas de ransomware (rançongiciel) :
 - En entreprise ou à l'université : signalez aux responsables informatiques ;
 - A la maison : rechercher de l'aide sur des sites et forums spécialisés :
 - <http://stopransomware.fr/nettoyer-son-ordinateur/>
 - Les sites d'éditeurs de solutions antivirales : Symantec, etc.
- Porter plainte à la police ou à la gendarmerie.



A retenir

- Ne pas faire confiance
 - aux collaborateurs / utilisateurs
- Chacun peut devenir un maillon faible



EXERCICE

<https://school.hello-design.fr>

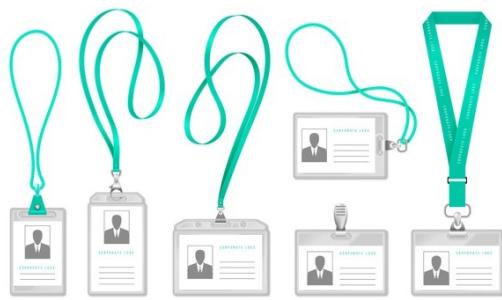
3C



- Connaître le Système d'Information
- Maitriser le réseau
- Sécuriser les terminaux
- Gérer les utilisateurs
- Sécuriser physiquement
- Contrôler la sécurité du S.I.
- Nomade

Protection physique des locaux (1/3)

- Protéger physiquement les locaux contenant les biens sensibles :
 - Contrôler l'accès aux locaux :
 - usage de badges par exemple ;
 - Utiliser des alarmes pour identifier les intrusions ;
 - Protéger les clés ou badges dans des coffres par exemple.



Protection physique des locaux (2/3)

- Les prises d'accès réseau doivent être protégées de manière à être inaccessibles
 - aux visiteurs/personnes mal intentionnées
 - Si les prises d'accès réseau sont exposées
 - ne pas les connecter au réseau.
 - Plutôt le faire au besoin et désactiver ensuite.



Protection physique des locaux (3/3)

- Protéger contre les incidents environnementaux
 - Incendie : extincteur, détecteur de fumée, etc.
 - Inondation : s'installer en zone non inondable, surélever les éléments, etc.
 - Panne électrique : utiliser des onduleurs, etc.



Imprimantes / Photocopieuses

- Faire attention lors des photocopies
 - à ne pas oublier les originaux
- Aller rapidement retirer les documents imprimés pour éviter que des informations sensibles soient révélées
- Ne pas oublier que les imprimantes disposent :
 - De disques durs
 - D'historique des impressions
 - dont les titres de documents pourraient être révélateurs
 - De configuration IP pouvant être usurpée
- Les documents papiers sensibles doivent être détruits à la déchiqueteuse
- Les imprimantes ne doivent pas être accessibles depuis Internet.



Sécuriser les équipements (1/2)



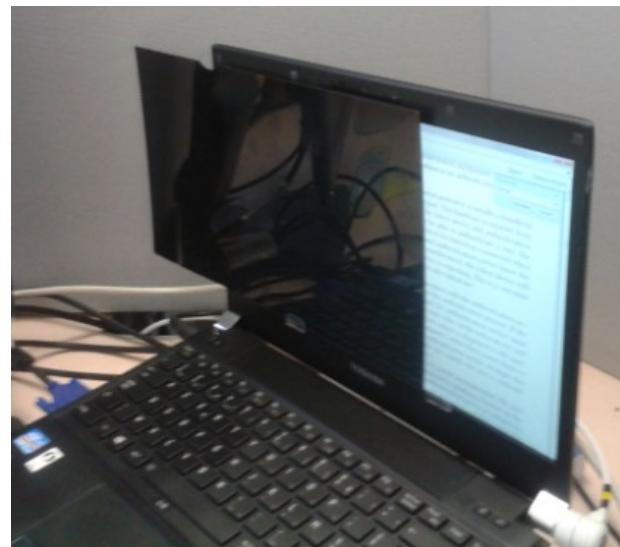
- Attacher avec un câble de sécurité les équipements le permettant
- Protéger l'accès aux équipements :
 - Avoir un code/mot de passe pour restreindre l'accès à son équipement :
 - lecteur d'empreinte ou signe sur téléphone
 - code PIN ou mot de passe
 - Demander un code/mot de passe pour sortir de la veille



Sécuriser les équipements (2/2)



- Faire attention aux médias USB
 - Des clés USB piégées sont parfois offertes ou abandonnées
 - Toujours scanner (anti-virus) une clé USB avant de l'utiliser
- Utiliser les filtres de confidentialité d'écran
 - Écran d'ordinateur (fixe, portable)
 - Écran de téléphone



Petit Jeu

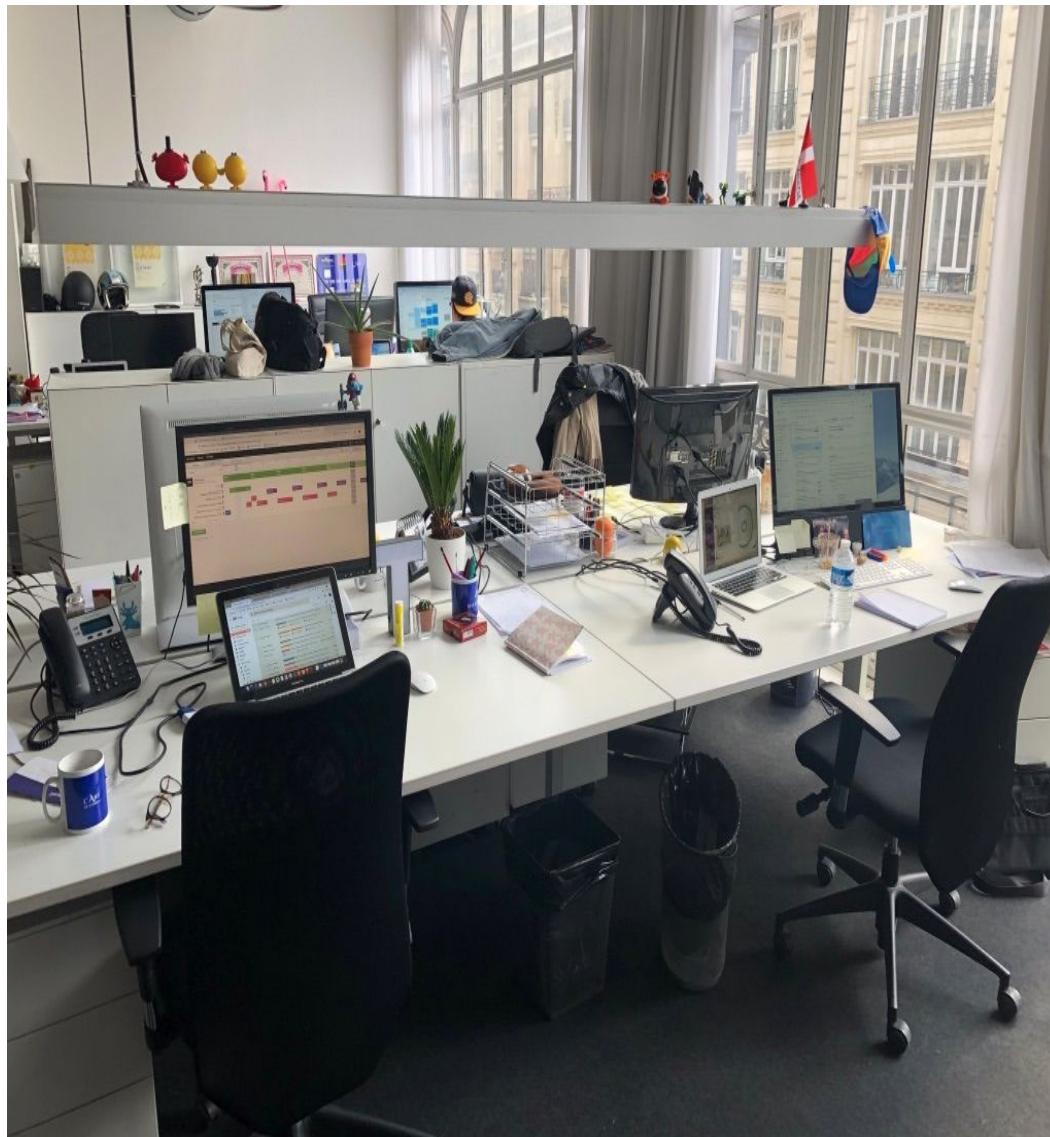
- Trouver les risques et failles de sécurité



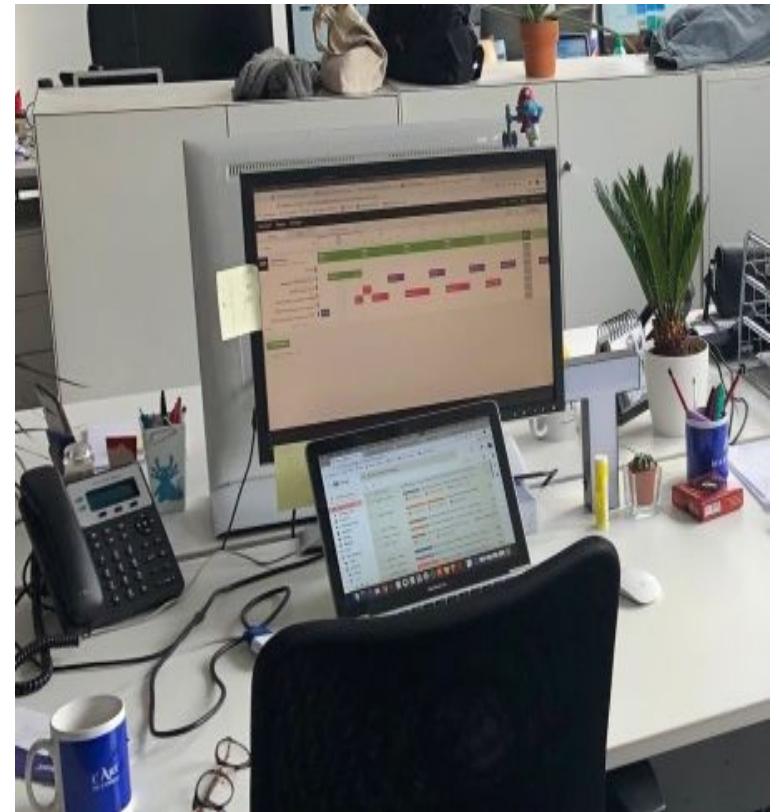


Mot de passe WIFI écrit en clair



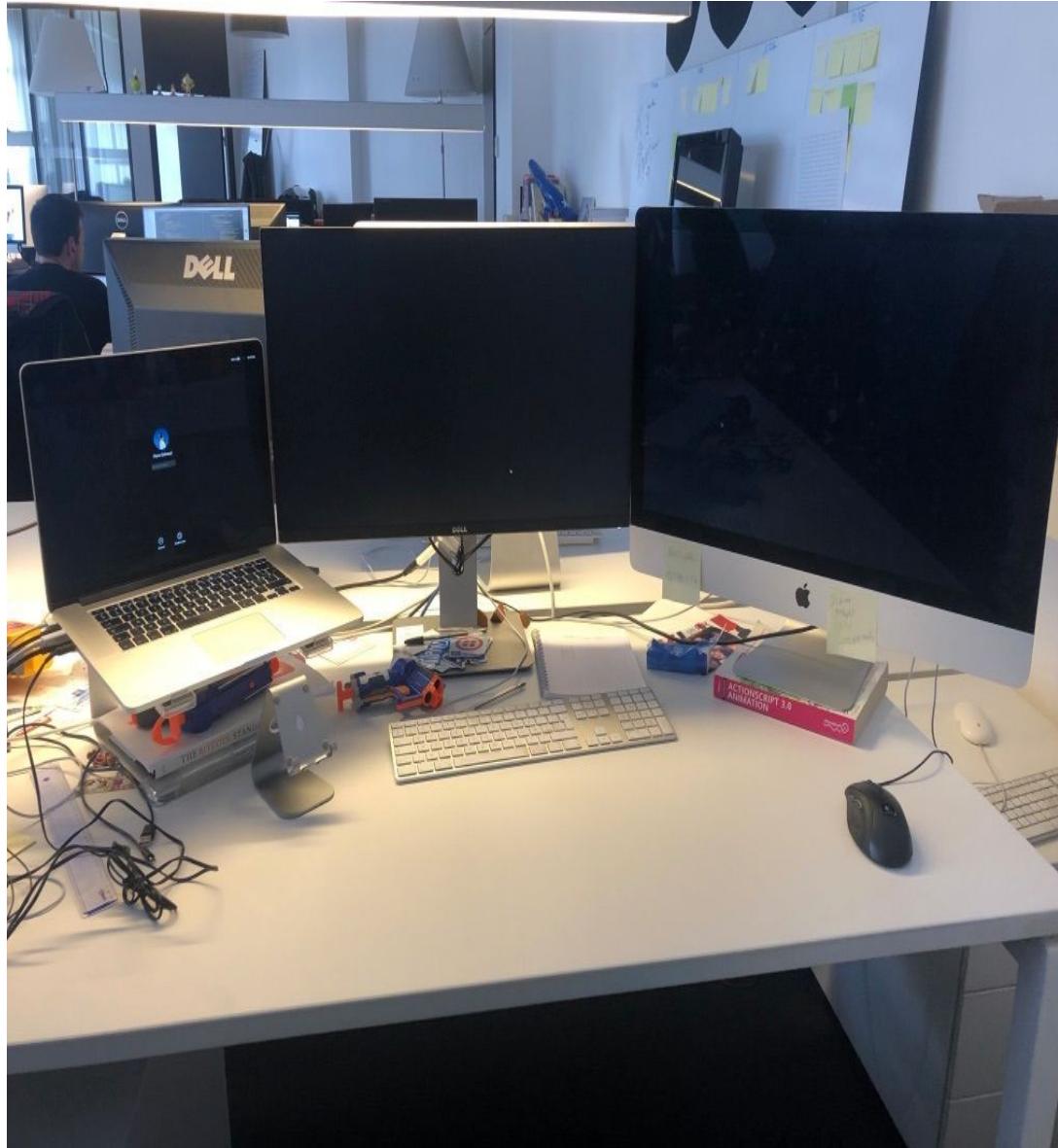


Ordinateur non verrouillé pendant la pause déjeuner



Le bureau d'un(e) collègue - 15:50

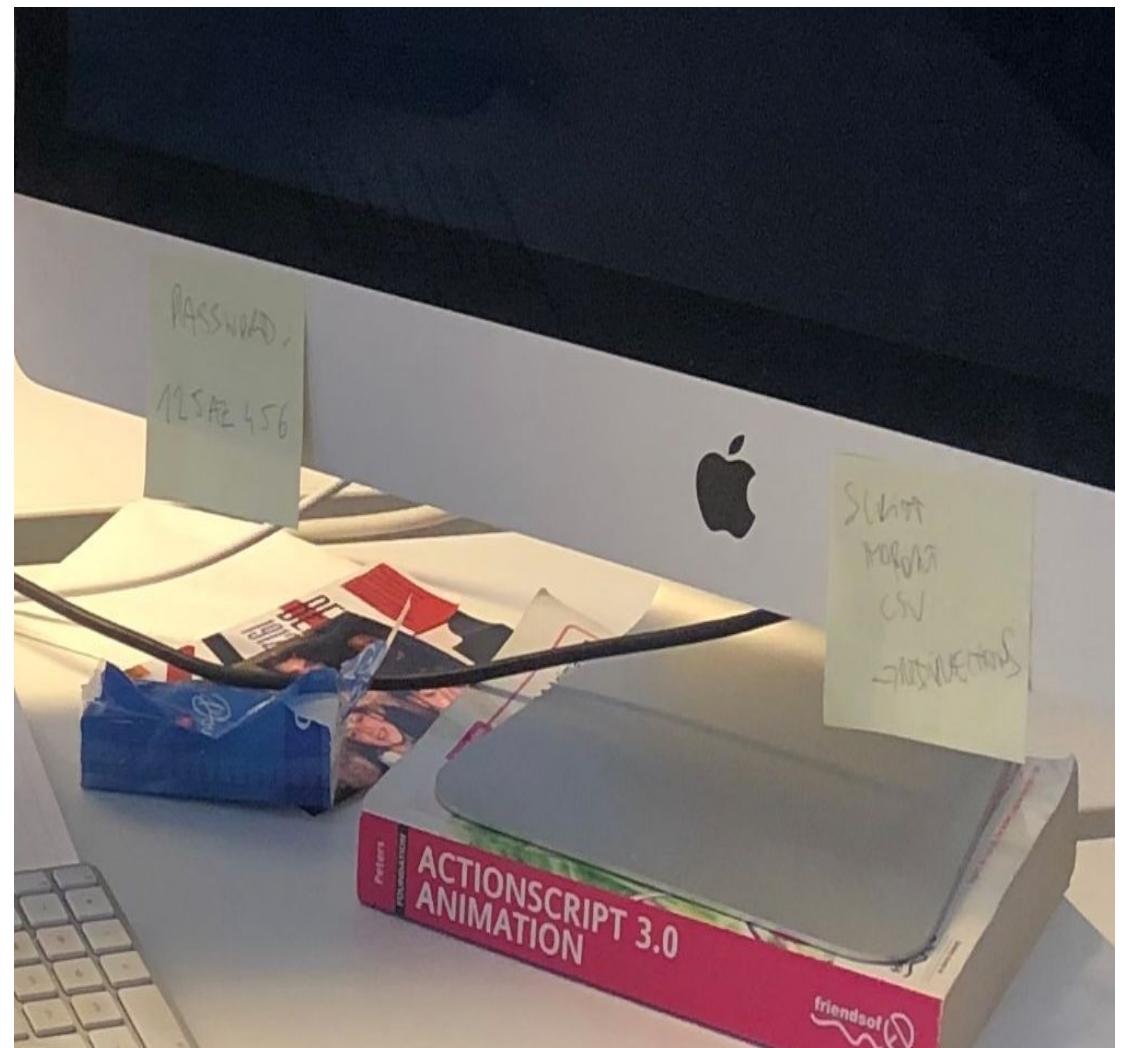
Q



Le bureau d'un(e) collègue - 15:50

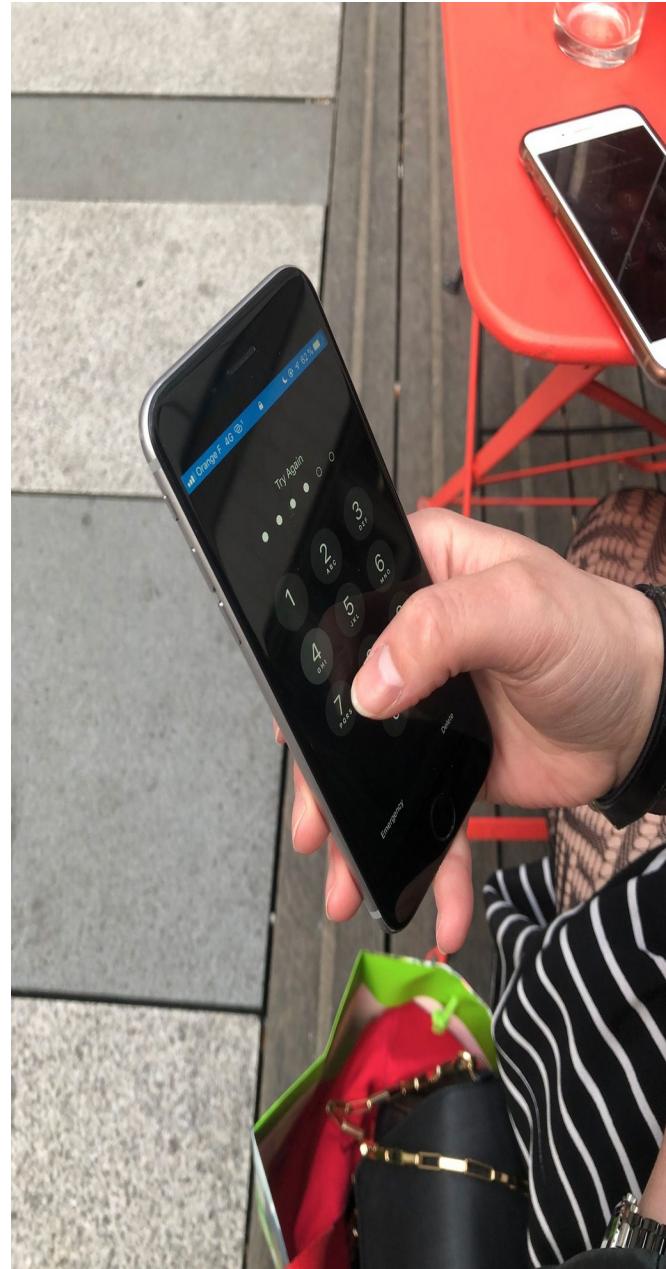
R

Mot de passe de l'ordinateur
sur un post-it

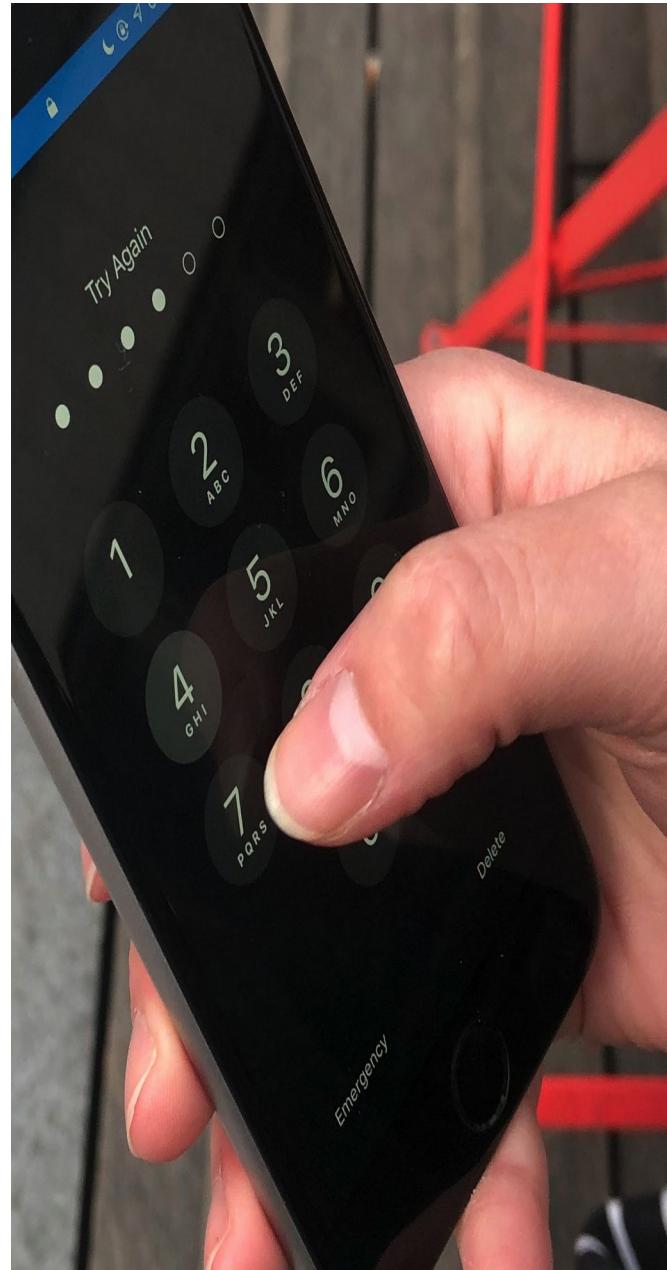


Coworking - 19:45

Q

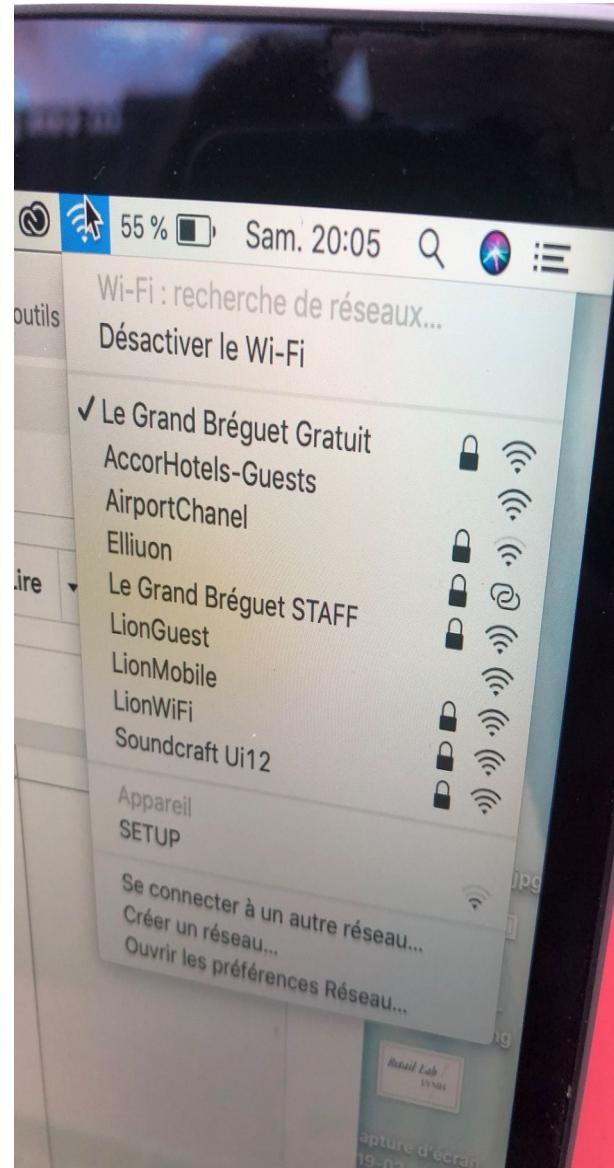


Déverrouiller son téléphone en public

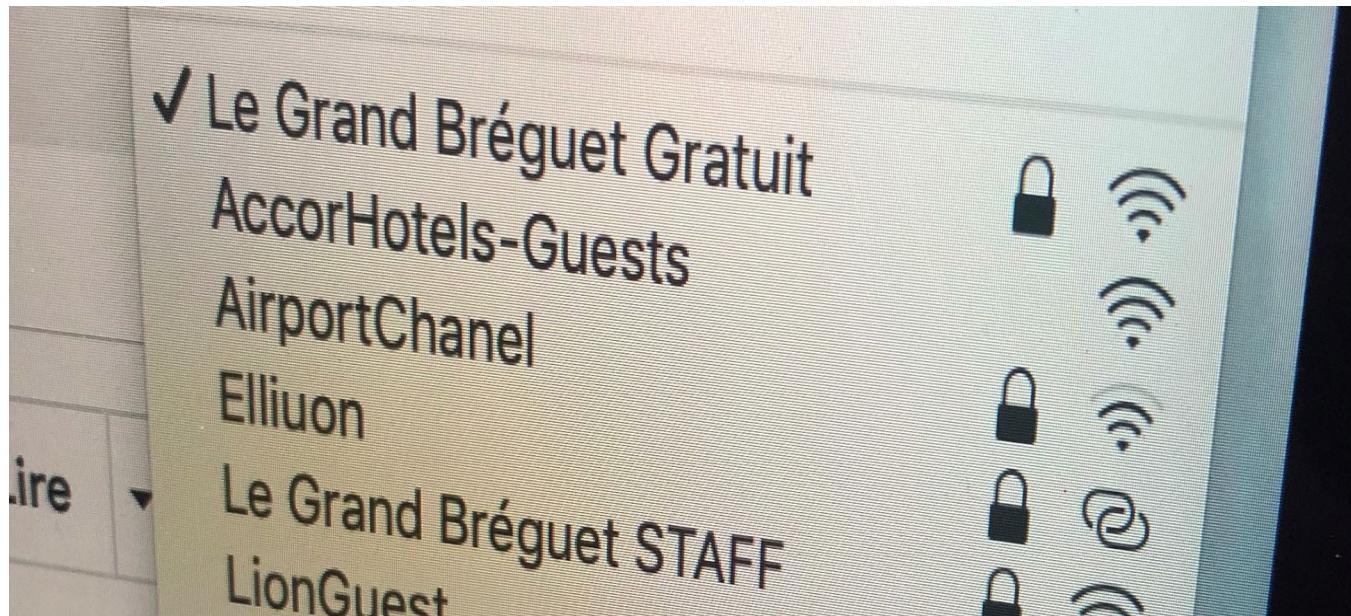


Coworking - 20:05

Q

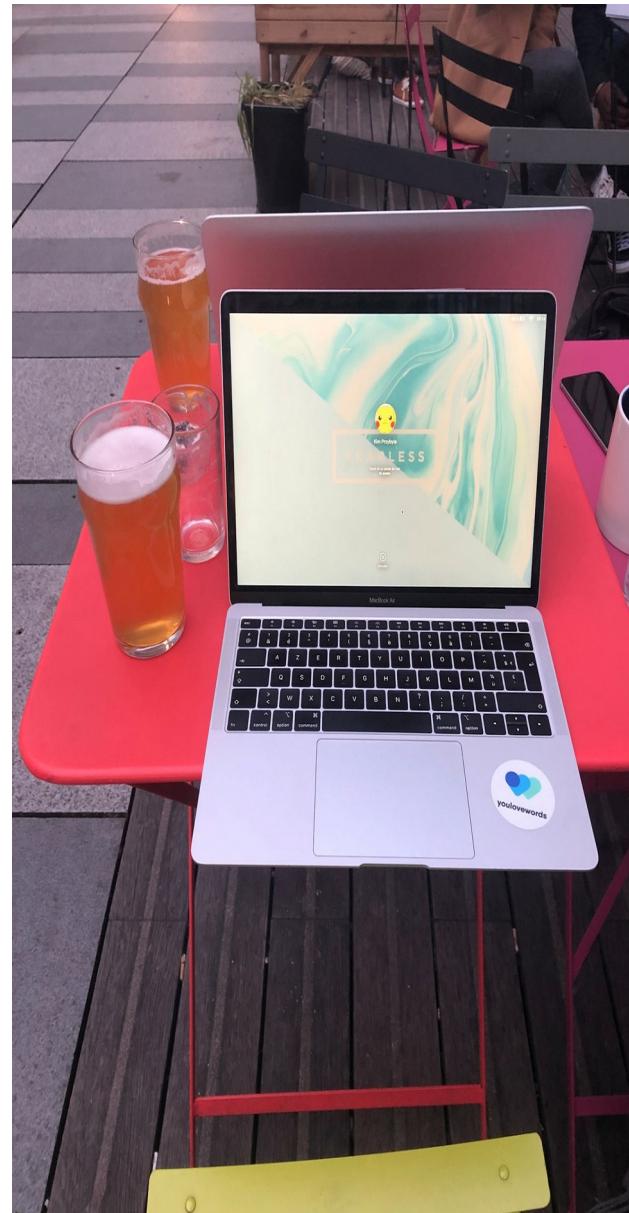


Se connecter à un wifi gratuit. Rien n'est gratuit = parano ?



Coworking - 20:15

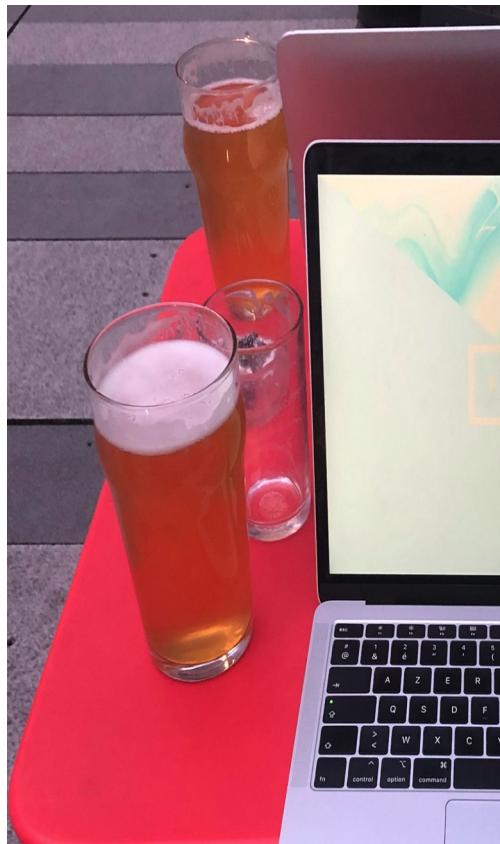
Q



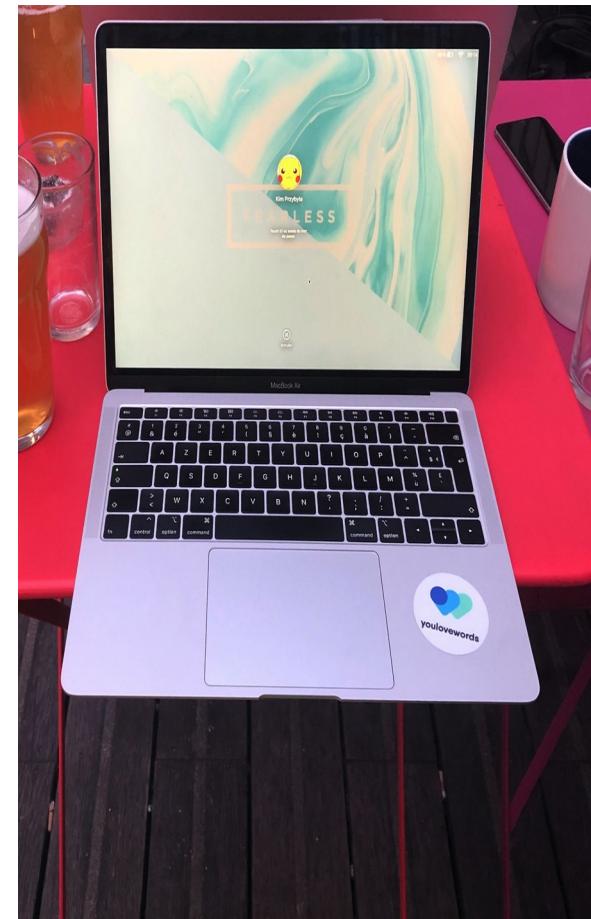
Coworking - 20:15 (double faille)

R

Liquide près d'un objet informatique

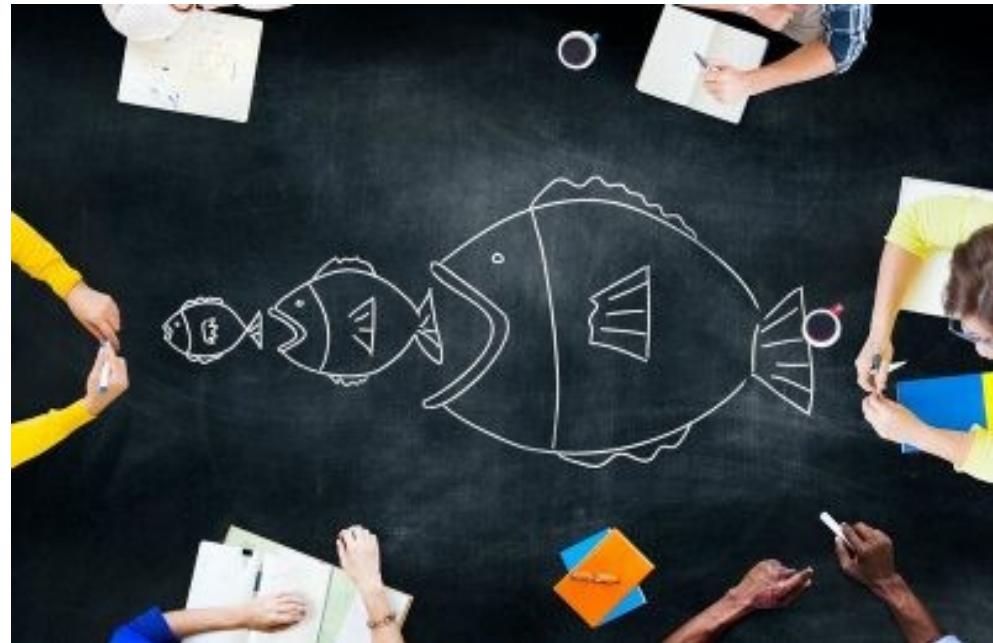


mauvais positionnement d'un ordinateur



A retenir

- N'importe où vous vous trouvez
 - Peu comporté un risque envers la sécurité



- Correction TP 2
- Connaître le Système d'Information
- Maîtriser le réseau
- Sécuriser les terminaux
- Gérer les utilisateurs
- Sécuriser physiquement
- Contrôler la sécurité du S.I.
- Nomade

Composants importants

- Avoir des journaux pertinents
 - Déetecter d'éventuels dysfonctionnements
 - Tentatives d'accès illicites
- Définir les composants critiques du SI
 - Agir équipements réseau et sécurité, serveurs critiques, postes de travaux..
- Analyser la configuration des éléments journalisés

Contrat/Maintenance/Professional Services (1/2)

- Lors de l'achat de :
 - matériel :
 - souscrire à des contrats de maintenance
 - Une assurance pour vous garantir une assistance en cas de difficulté
 - application : souscrire à des contrats de support et d'assistance.
 - niveau 1 : description et enregistrement du problème rencontré.
Conseil/information basique
 - niveau 2 : intervention de technicien
 - niveau 3 : intervention d'expert.
- SLA (Service Level Agreement)
 - Indique le niveau de service garanti par le prestataire pour une prestation de service donnée.
 - Exemple : couverture 3G ou 4G.



Contrat/Maintenance/Professional Services (2/2)

- Cyber-assurance, c'est :
 - Assurance visant à indemniser
 - Assister les victimes de cyber-attaque
 - Fuite de données, attaque à la e-réputation...
 - Exemple : AXA propose pour les particuliers
 - Protection Familiale Intégrale

Noter que la souscription d'une assurance est considérée comme une mesure de sécurité permettant de réduire les risques portant sur l'entreprise

Au même titre :

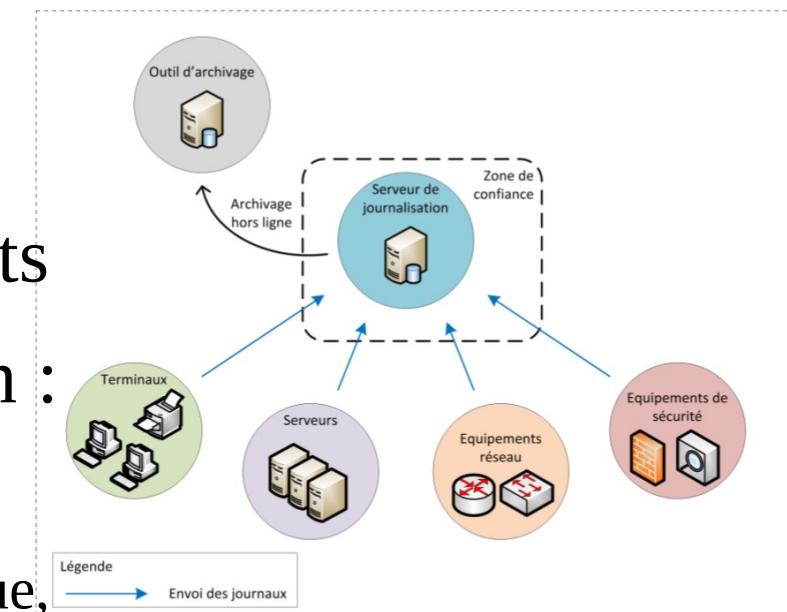
- Une assurance habitation n'empêchera pas un incendie
Mais compensera/limitera les pertes financières de la victime



Souscrire à des services d'assurance/support/maintenance pour les composants sensibles.

Surveiller / Superviser

- Activer la journalisation d'évènements
 - Enregistrer les tentatives d'accès réussies ou pas
 - Enregistrer les tentatives de modifications d'informations sensibles
 - ...
- Consulter les journaux d'évènements
- Définir une politique de supervision :
 - définir les seuils :
 - au-delà de tel taux d'occupation du disque, recevoir une alerte
 - Définir le type d'alerte souhaité : SMS, mail...



Incidents de sécurité : catégories d'incidents

- Divulgation d'information personnelle ;
 - carte de crédit, vol d'identité, numéro de sécurité sociale, etc.
- Déni de service
 - entrant ou sortant
- Activité causée par un code malveillant
 - Vers, virus, keylogger, Rootkit
- Enquête et activité criminelle
 - Vol de terminal, fraude, pornographie infantile
- Non respect de la politique de sécurité
 - partage de mot de passe
- Défacement Web
 - Redirection de site, déacement d'un site internet
- Vulnérabilité non corrigée
 - système/application vulnérable, non application d'un correctif important



Incidents de sécurité : gestion des incidents de sécurité

- Un processus de gestion des incidents de sécurité permet de :
 - Réagir rapidement et de réduire l'impact en cas d'incident ;
 - Améliorer la prévention et la sensibilisation ;
 - Déetecter et d'identifier les incidents ;
 - Améliorer le niveau de sécurité.
- Exemple de réaction en cas d'une infection virale :
 - déconnecter le poste du réseau ou d'Internet, sans l'éteindre
 - S'assurer que l'antivirus/antimalware est à jour avec les dernières signatures
 - Exécuter le scan complet (en « mode sans échec » par exemple) avec un antivirus
 - Contacter un spécialiste au besoin ;
 - Chercher à identifier la cause.

La norme ISO 27035 décrit le processus de gestion des incidents.

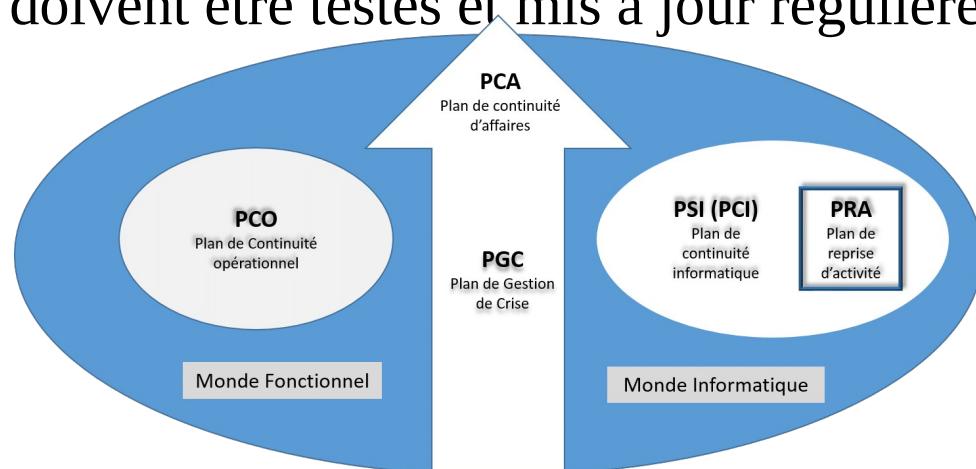
Plan de secours (1/2)

- Avoir un plan de secours
 - En cas de dysfonctionnement important (électrique, télécom...)
 - Double alimentation
 - pour un téléphone : batterie de secours
 - ordinateur/serveur : onduleur, batterie de secours, groupe électrogène
 - Accès Internet
 - utiliser son téléphone comme modem en cas de dysfonctionnement de sa Box
 - En entreprise, souscription à une offre Internet comme ligne de secours fournie par un opérateur différent
 - Avoir une sauvegarde de ses données en cas de panne de son disque dur



Plan de secours (2/2)

- En entreprise, il y a des
 - PRA : Plan de Reprise d'Activité
 - Permet de « reprendre » après une interruption inattendue comme la perte d'un site de travail
 - Exemple : utilisateur d'un site de secours « B » et déplacement du personnel en cas d'incendie dans le site principal « A »
 - PCA : Plan de Continuité d'Activité qui permet de s'assurer que l'activité ne s'arrêtera pas
 - Exemple : usage d'une architecture réseau redondée en haute disponibilité
 - Routeur en actif/actif
 - Les PCA et les PRA doivent être testés et mis à jour régulièrement



Audit : informations générales

- Un audit
 - Peut porter sur tout ou partie du S.I., une application,...
- Le but de l'audit est généralement :
 - d'évaluer le niveau de sécurité par rapport à un référentiel (interne ou à une norme) ;
 - obtenir un agrément ou une certification :
 - ASIP Santé, PCI-DSS, 27001, etc.
 - trouver des faiblesses et les corriger :
 - site Web ;
 - application développée « in-house »
- L'audit peut être réalisé par :
 - des experts appelés « auditeur sécurité », « pen-testeur »
 - des sociétés spécialisées.
- Un cadre légal et contractuel est requis pour les audits :
 - Pour les audits de site Web, il faut l'accord du propriétaire du site (par exemple l'association étudiante), de l'hébergeur du site (OVH ou l'université) et parfois celui de l'opérateur ;
 - L'auditeur doit indiquer à partir de quelles adresses IP publiques son audit sera effectué ;
 - L'auditeur doit s'engager à ne pas provoquer d'incident de sécurité (dénie de service par exemple) au cours de son audit.



Audit : types d'audit (1/2)

- Audit de conformité pour déterminer les écarts par rapport à un référentiel
 - Politique de sécurité interne ou exigences de sécurité d'un cahier de charge
 - Norme internationale : exemple 27001, PCI-DSS, ASIP Santé
- Audit en vue de l'obtention d'un(e) certification/agrément
 - Audit physique des datacenters pour obtention d'un agrément SAS 70
 - Audit 27001 en vue de démontrer la bonne application des principes de la norme



Audit : types d'audit (2/2)

- Audit Technique

- « Boite noire » ou « Pentest »

- sans aucun accès, on évalue le système (site web par exemple) du point de vue d'un attaquant quelconque

- « Boite grise » ou « test du stagiaire »

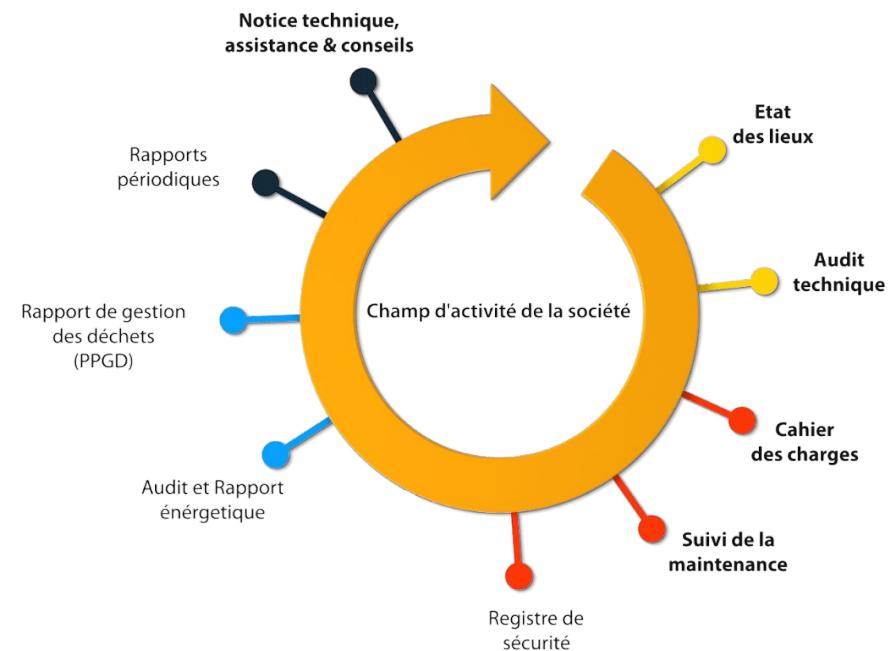
- on dispose de quelques informations et on essaye d'élèver ses privilèges

- « Boite blanche » pour faire des « audits de configuration » par exemple.

- On dispose d'accès, y compris administrateur et on évalue le système par rapport à un référentiel

- « Forensic » ou « Post-mortem »

- effectuer sur un système après une attaque.



A retenir

- Les incidents de sécurité peuvent être éviter
 - Il faut le préparer en amont



EXERCICE

<https://school.hello-design.fr>

3F



- Connaître le Système d'Information
- Maîtriser le réseau
- Sécuriser les terminaux
- Gérer les utilisateurs
- Sécuriser physiquement
- Contrôler la sécurité du S.I.
- Nomade

Nomades numériques ?

- Combiner harmonieusement travail et voyages
 - Offre une liberté et des possibilités de découverte inégalées
- Présence de difficultés
 - Risques liés au Wi-Fi public
 - Diversité des appareils
 - Paysages de cybersécurité en fonction de la géographie

Les trajets : Domicile ↔ Bureau / Ecole

- Utiliser avec précaution (sans surveillance)
 - Transport : Ratp, Ferrorière, Aérien...
 - Lieux publics
- Le matériel mobile
 - Ordinateurs portables
 - Appareils portatifs
 - Tablettes
 - Smartphones



Protéger les informations contre tout accès ou lecture non autorisé

A distance

- Télétravail
- Séparé espace Pro / Privée
- Les mêmes règles
 - Bureau propre
 - Espace confidentiel
 - Règles à prendre en compte



Zone de travail

- Les zones de travail
 - sont des zones réglementées et identifiées.
- Les personnes habilitées reçoivent :
 - Des autorisations
 - Les informations pour y accéder
 - Zones / Lieux pour travailler en toute sécurité.



Salle blanche

- Zone réservée à certaines personnes
- Objets interdits
 - Téléphone mobile
 - caméra
 - sacs / sacoches
 - Baladeur / playeur de musique (MP3-MP4-Ipod...)
 - CD ROM / DVD
 - Montre connecté de type :
smart watches



Accès par un contrôle de sécurité

Personnes

- Seuls les utilisateurs notifiés et autorisés peuvent accéder
- Possédez un justificatif
- Le matériel transporté doit être approuvé

Employés / Visiteurs / Partenaires

- Etre accompagnés
 - par une personne autorisée
- Signer le registre des visiteurs
 - Besoins professionnels à l'accueil
 - Etre escortés par un employé autorisé.
- Mouvements des utilisateurs
 - Possibilité d'être surveillés
 - Vidéosurveillance (+informations)

Accès limités ?

Zones de traitement

- Stockage
 - Informations critiques
 - Confidentielles
- Zones sécurisées.

Zones sécurisées

- Accès par le personnel autorisé
 - Serveur/Réseau/ISP/ Télécommunication Rooms (Centre de données)
- C'est votre zone de travail
 - Salle des archives financières
 - Salle des archives des RH
 - Espaces de travail spécifiques aux clients

Bonnes pratiques pour la sécurité des réseaux sans fil

- Activer la double authentification (2FA)
- Utiliser un mot de passe fort
- Chiffrer les données
- Désactiver SSID Broadcast
- Utiliser le filtrage d'adresses MAC
- Activer la sécurité WPA3
- Utiliser un VPN
- Désactiver l'administration à distance
- Changer le mot de passe par défaut
- Utiliser un pare-feu
- Désactiver UPnP (Universal Plug and Play)
- Désactiver les services inutiles

A retenir

- Attribuer les droits d'accès aux informations confidentielles :
 - Uniquement aux personnes en ayant la nécessité
 - Dont le profil les y autorise
- S'assurer du retrait des droits d'un intervenant
 - lorsque celui-ci n'a plus à avoir accès à ces données
- Les endroits/lieux sensibles
- Contrôle des accès physiques et logiques
 - identification et authentification

- Générer un mot de passe en LEET



Aujourd'hui je vais à l'aéroport

leet



TP 3

TP 3 :

- Deadline
 - Le 7 mars 2023 23:59
- Énumération structurée (avec détails)
 - Tous les formats acceptés
 - ODT, Docx, PDF, Markdown...
- Sujet :
 - Décrivez les types d'attaques 'ciblée' et 'non ciblée' ?

Rendez-vous au prochain cours

- Merci de votre attention

