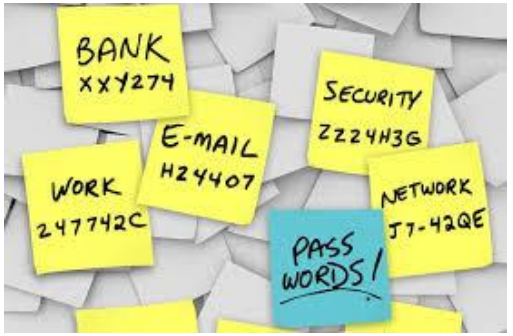
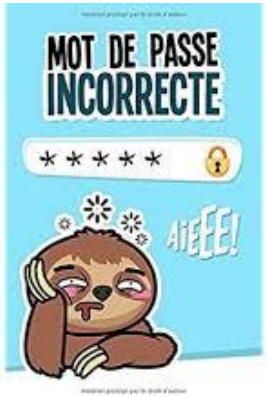
Les mots de passe



Cours N°2-A



Généralités

- La sécurité de l'accès à tous les services du web repose sur les mots de passe,
- La tentation est forte d'avoir une gestion simple,
- Cette pratique augmente les risques qui compromettent la sécurité de vos comptes
- 3 méthodes possibles pour gérer les MP
  - Votre gestion personnelle,
  - L'utilisation de votre Navigateur,
  - L'utilisation d'un outil (logiciel) spécialisé

Créer des mots de passe forts (conseils microsoft)

- Comprendre au moins 12 caractères (ou mieux, 14 ou plus)
- Comprendre des lettres majuscules, minuscules, des chiffres et des symboles
- Ne pas être un mot qui se trouve dans le dictionnaire
- Ne pas être le nom d'une célébrité ou de quelque chose de célèbre (comme un personnage connu, un produit ou une organisation)
- Être radicalement différent des précédents mots de passe (en cas de vol, seul le compte concerné sera vulnérable)

Méthodes pour créer des mots de passe forts

- Être facile à mémoriser, mais difficile à deviner par d'autres personnes
- Envisagez d'utiliser une expression:

Ex : Jadorelescours2020deNogent/ernet

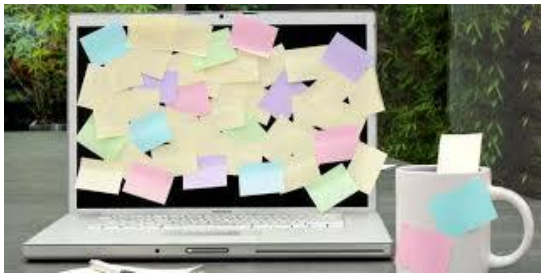
- Evitez les combinaisons trop simples
- Utilisez la méthode des premières lettres :
  - Jalc2020dN
- Utilisez la méthode phonétique:
  - ght3DVD%$
- Avec Chrome, à condition d'être synchronisé, faire un clic droit dans le champ « mot de passe » et sélectionner « suggérer un mot de passe »
- Utilisez un générateur de mots de passe (tapez générateur de mot de passe sur Google)

Sécuriser vos mots de passe (microsoft)

- Ne partagez votre mot de passe avec personne. *Même s'il s'agit d'un ami ou d'un membre de votre famille.*
- N'envoyez jamais de mot de passe par courrier électronique, message instantané ou tout autre moyen de communication non fiable.
- Utilisez un mot de passe unique pour chaque compte.

  Si une personne vole un mot de passe que vous utilisez pour plusieurs comptes, toutes les informations protégées par ce mot de passe sont menacées sur l'ensemble des comptes.

Mémoriser les mots de passe
(les différentes méthodes)



- La méthode des posts it :

  elle ne marche pas….

- Le cahier ou le carnet :

  c'est mieux, mais il ne faut pas le perdre…. Et en voyage on le met dans la valise, ou dans la voiture…..

- Le fichier (excel), c'est encore mieux (à condition de le mettre à jour, lui donner un nom « discret », et le « cacher » mais n'est disponible que sur le PC
  - *Il est possible de protéger le fichier avec un mot de passe :*
  - *Ouvrir le fichier, sélectionner fichier/informations/Protéger la présentations (ou le classeur)/chiffrer avec mot de passe >>> saisir un mot de passe*
  - *A chaque fois que vous ouvrirez ce fichier il faudra saisir ce mot de passe*

Mémoriser les mots de passe
(les différentes méthodes suite)

- Envoyer le fichier sur votre messagerie et le classer dans un répertoire de votre boite mail; stocké sur le serveur de votre FAI; il sera accessible de partout.
- Mettre le fichier dans un « cloud » (dropbox, drive…),
- Mettre le fichier dans une clé USB, et la garder sur vous
- Utiliser la mémorisation proposée par Chrome
- Utiliser un gestionnaire de mot de passe

Sécuriser vos mots de passe (microsoft)

- Si vous ne souhaitez pas mémoriser plusieurs mots de passe, songez à utiliser un gestionnaire de mots de passe. Les meilleurs gestionnaires de mots de passe mettent automatiquement à jour les mots de passe stockés, les cryptent et nécessitent une authentification multifacteur pour y avoir accès.
- Ne stockez pas le mot de passe sur l'appareil qu'il protège.
- Vous pouvez noter vos mots de passe sur papier, tant que vous les maintenez en sécurité. Ne les mettez pas sur des pense-bêtes ou des papiers que vous gardez près de l'appareil à protéger .

Utilisez la double authentification
(sécurisation du compte)

- Pour renforcer la sécurité, certains sites permettent la « double authentification »
  - *A vous de choisir dans les paramètres du compte*
  - Après avoir entré votre identifiant et votre mot de passe, vous recevez un code sur votre messagerie.
  - Il suffit alors d'entrer le code pour accéder à votre compte
- Quelques sites qui utilisent la DA :
  - Outlook, Gmail, Facebook, Instagram,
  - Skype, Whatsapp,
  - Amazon, Paypal, eBay,
  - Les clouds : Dropbox, Onedrive, Google Drive
  - ….
- Même si votre MP est découvert, il n'est pas possible d'accéder à votre compte

Utilisation des mots de passe

- Modifiez immédiatement les mots de passe des comptes dont vous soupçonnez la sécurité compromise,
- Évitez d'entrer votre mot de passe sur un appareil si vous n'êtes pas certain de sa sécurité.

Les appareils partagés ou destinés à un usage public peuvent avoir installé un logiciel d'enregistrement qui peut garder votre mot de passe lors de sa saisie.

- Eviter d'enregistrer votre mot de passe sur un ordinateur public ou partagé.
- Activer l'authentification multifacteur lorsqu'elle est disponible.

La fonction « mot de passe oublié »

- Si vous avez oublié ou perdu vote MP, cliquez sur « mot de passe oublié » lors de la connexion à votre compte.
- Le processus peut être différent d'un compte à l'autre:
  - Vous devez saisir votre e-mail, un lien vous est alors transmis dans votre boite mail pour réinitialiser votre MP, parfois c'est un MP provisoire qui est envoyé (il faut le changer dès la connexion sur votre compte)

Comment modifier un mot de passe

- Le processus peut être légèrement différent d'un compte à l'autre mais le principe est le suivant :
  - Connectez vous à votre compte,
  - Allez sur votre « profil » (paramètres/profil)
  - Allez sur la rubrique ou le menu « mot de passe »
  - Cliquez sur « modifier »
  - Saisissez votre nouveau mot de passe et validez
  - A la prochaine connexion vous devrez saisir le nouveau mot de passe

La gestion des mots de passe

- Tous les navigateurs proposent d'enregistrer identifiants et mots de passe lorsque vous ouvrez un compte:
  - Cela permet de les utiliser ultérieurement sans les ressaisir
  - Ils sont très peu protégés
- Il existe des « gestionnaires de mots de passe » tels que keepass, lastpass, dashline etc…
  - Ils permettent de stocker vos identifiants et MP dans un coffre fort
  - Vos mots de passe stockés sont « chiffrés », mais le mot de passe d'accès n'est pas sauvegardé (à ne pas perdre!)
  - Gratuits/payants
  - Peuvent s'installer sous forme d'extension dans votre navigateur
- Google Chrome dispose d'un gestionnaire de mots de passe (les autres navigateurs aussi)
- Mais quels sont les risques ?
  - Le piratage de comptes sur les serveurs (orange, amazon etc…)
  - L'accès à vos MP enregistrés sur votre PC,
  - La perte du mot de passe d'accès

L’accès aux services publics avec un seul mot de passe

- Rappel du cours (01/2020) sur les services publics:
  - Système d’authentification unique qui permet d’accéder aux principaux sites du services publics avec un seul identifiant et mot de passe.
  - utilisation de « France connect »
  - Cela concerne les sites :
    - Service-public.fr; ameli; impots.gouv.fr, ANTS.gouv.fr, lassuranceretraite.fr

Le gestionnaire de mot de passe de Chrome

- Chrome peut vous proposez d'enregistrer vos mot de passe :
  - Ouvrez Chrome
  - Cliquez sur votre profil en haut à droite
  - Cliquez sur la clé : mot de passe
  - Activez (ou désactivez) l'option « Proposer d'enregistrer les mots de passe »

Les mots de passes sont alors enregistrés sur votre ordinateur et peuvent être « consultés » par un malware

Le gestionnaire de mot de passe de Chrome (comment consulter les mots de passe enregistrés)

- Ouvrir Chrome,
  - Accéder aux paramètres (3 points verticaux/paramètres)
  - Saisie automatique/mots de passe
  - La liste de vos compte avec les mots de passe apparaît
  - Vous pouvez supprimer la mémorisation d'un mot de passe en cliquant à droite sur les 3 points verticaux puis « supprimer » ou sur l'œil pour voir en clair le MP

Le gestionnaire de mot de passe de Chrome (synchronisation activée)

- Il peut vous proposez un mot de passe (clic droit la fenêtre mot de passe puis « suggérer un mot de passe »)
- Il permet d'enregistrer vos mots de passe, lorsque vous ouvrez un nouveau compte
- Très utile quand on multiplie le nombre de comptes,
- **Mais, les mots de passe sont enregistrés sur le disque dur de votre PC, ils sont donc à la merci d'un malware.**
- **Ils sont très faciles d'accès si vous prêtez votre PC (sans avoir créé un compte visiteur) ou sans mot de passe sur le compte administrateur Windows**

Le gestionnaire de mot de passe de Chrome (suite)

- Si votre profil Google chrome est synchronisé (*) avec votre compte Google :
  - Vos mots de passe sont stockés en ligne (dans le cloud Google),
  - Ils sont partagés avec vos différents appareils (de même que votre historique de navigation et vos favoris)
  - Si vous changez d'ordinateur et activez votre compte Google Chrome, vous retrouvez vos mots de passe
  - Permet à Google de vous pister…..

(*) revoir le cours synchronisation de Nogenternet

Le gestionnaire de mot de passe de Chrome
Consulter les mots de passe enregistrés sur votre compte Google

- Ouvrez Chrome,
- Accéder au site passwords.google.com
- Connectez vous à votre compte
- La liste des mots de passe enregistrées apparait et vous pouvez alors pour chaque compte :
  - Afficher en clair le MP,
  - Le supprimer

Le vol de mot de passe
(les principales techniques)

- Lire le fichier contenant les mots de passe de votre navigateur web,
- Intercepter les connexions réseau dans la phase d'identification avec le site web,
- Voler les mots de passe lorsque vous les saisissez au clavier(keylogger)
- Capturer l'écran quand vous utilisez un clavier virtuel (tablette, téléphone)
- Certains cookies

Evitez les duperies

- Sachez détecter les actions qui pourraient vous conduire à fournir votre mot de passe

  (Ex :e-mail d'une boutique en ligne, de votre banque etc….)
- En règle générale, méfiez-vous des personnes qui vous demandent des informations sensibles, même si vous connaissez la personne ou l'entreprise et qu'elle est digne de confiance.

  Par exemple, un escroc a peut-être piraté le compte d'un ami et envoyé un courrier électronique à tous les membres du carnet d'adresses de cet ami.
- Traitez toutes les demandes d'informations sensibles non sollicitées avec précaution.

Evitez les duperies

- Ne partagez jamais votre mot de passe suite à une demande par message ou par téléphone (par exemple, pour vérifier votre identité), même si celle-ci semble provenir d'une entreprise ou d'une personne de confiance.
- Accédez toujours aux sites Web à l'aide de liens approuvés. Des escrocs peuvent copier l'apparence du site Web d'une entreprise pour vous tromper et vous faire cliquer sur un faux lien ou une fausse pièce jointe.
- Faites attention aux liens qui apparaissent dans les messages électroniques, les messages instantanés ou les SMS non sollicités. En cas de doute, accédez directement au site Web officiel de la banque ou du service