Les mots de passe

Généralités

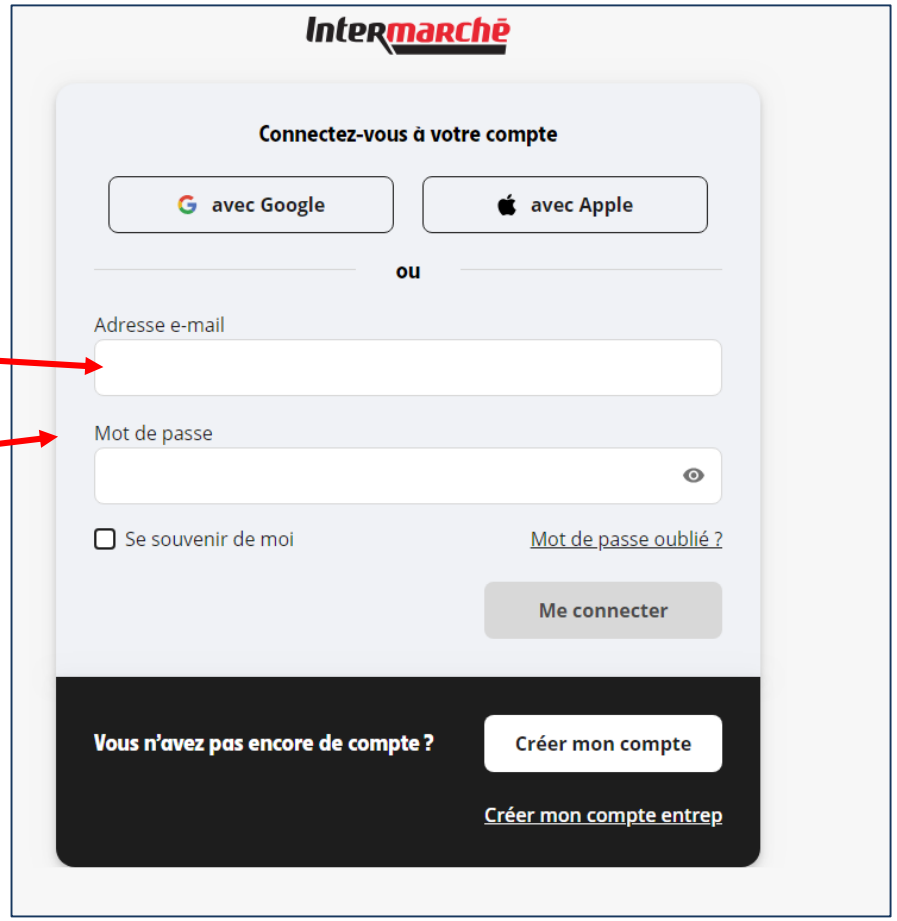
- La sécurité de l'accès à tous les services du web repose sur les mots de passe,
- La tentation est forte d'avoir une gestion simple,
- Cette pratique augmente les risques qui compromettent la sécurité de vos comptes
- 3 méthodes possibles pour gérer les MP
  - Votre gestion personnelle,
  - L'utilisation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

Les différentes façons de se connecter à un compte

- Selon les sites, la méthode pour accéder à votre compte peut différer :
- Méthode de base :
  - « authentification simple »

1 identifiant

1 mot de passe

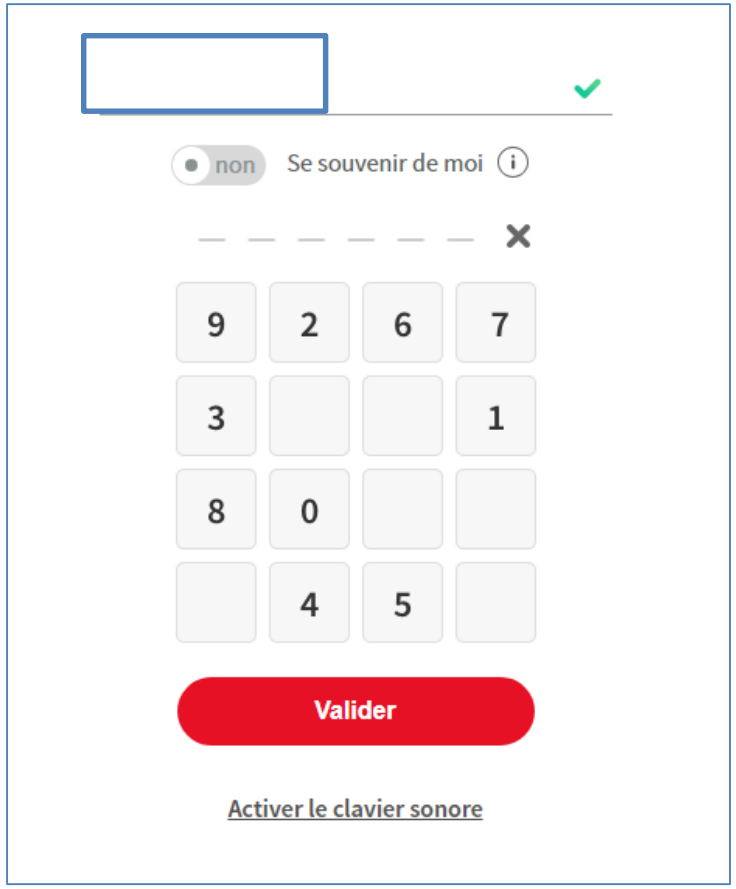


Les différentes façons de se connecter à un compte

L'identification chiffrée, la grille change à chaque fois

- impossible pour les logiciels espions (keylogger) de détecter le chiffre que vous tapez
- impossible d'utiliser un gestionnaire de mot de passe

- selon les sites il faut saisir l'identifiant et le mot de Passe ou seulement le Mot de passe sous forme chiffré



Les différentes façons de se connecter à un compte

- L’authentification à 2 étapes :
  1. L’identifiant, Le mot de passe
  2. Puis un code que vous recevez sur un équipement extérieur (téléphone) sous forme d’un texto ou d’un mail

  – Impossible pour les robots de se connecter à votre compte

  – Impossible pour vous d’utiliser un gestionnaire de mot de passe

  La double authentification est proposée sur certains sites comme Google, Facebook, les sites du services publics …

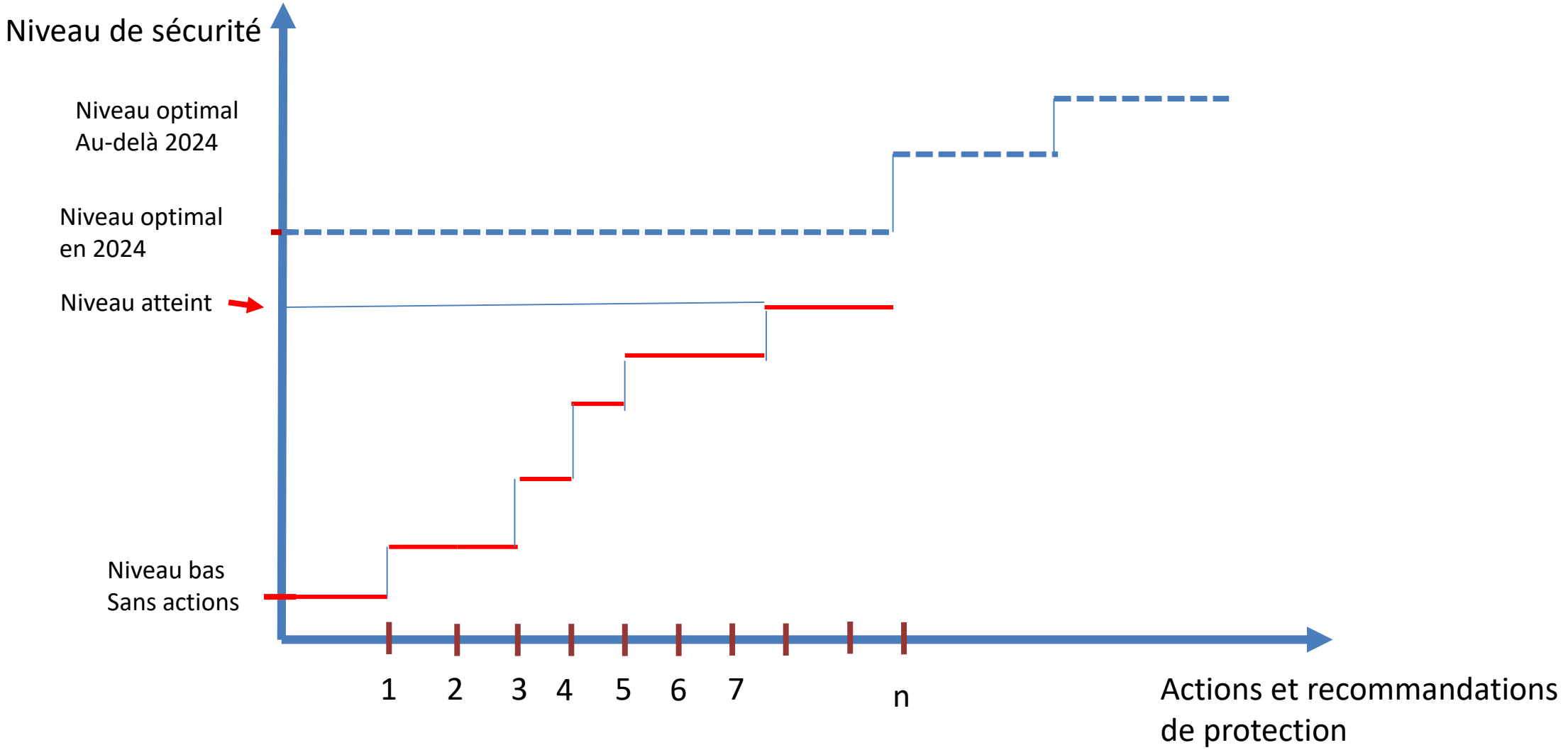
Les banques ont mis en place une « identification renforcée » basée sur « 3D-secure » voir à la fin du cours

Temps nécessaire pour « cracker » un 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

Infographie FRANCENUM.GOUV.FR Source : Hive Systems

Niveau de protection de vos comptes



Les 10 bonnes pratiques à adopter

- Utilisez un mot de passe différent pour chaque compte
- Utilisez un mot de passe fort (suffisamment long et complexe)
- Utilisez un mot de passe impossible à deviner
- Utilisez un gestionnaire de mot de passe
- Changez de mot de passe au moindre soupçon sur votre compte
- Ne communiquez jamais vos mots de passe à un tiers
- N’utilisez pas vos mots de passe sur un ordinateur partagé
- Activez la double authentification quand c’est possible
- Changez le mot de passe par défaut des services nouveaux auxquels vous accédez
- Choisissez un mot de passe particulièrement fort pour votre messagerie

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/t
- 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 mots de passe sur Google, ou l'extension Genpass pour chrome)
- Tous les conseils:
- https://genpassword.net/secure-password

Générateur de mot de passe en ligne

- Si vous n’arrivez pas à créer des mots de passe « forts », vous pouvez utiliser un générateur de mots de passe.
- Par exemple :
- https://www.motdepasse.xyz/

Exercice

- Ouvrir Chrome,
- Utilisez un générateur de mot de passe et créez quelques mots de passe « forts »
- Copier un mot de passe dans le « bloc notes » ou dans « Word »

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 mots 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.
- Plus de conseils sur ce site : (clic droit, traduire si le texte est en anglais)
  - https://genpassword.net/secure-password/

Les 10 pires mots de passe !
(info AVAST)

- 123456
- motdepasse
- 12345678
- Azerty
- 12345
- 123456789
- Entrer
- 1234567
- Football
- jetaime

Comment mémoriser les mots de passe et les retrouver facilement

Mémoriser les mots de passe
(les différentes méthodes)

- La méthode des posts it :

  elle ne marche pas…. À bannir

- 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 »
  - *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*

Stocker les mots de passe dans un carnet

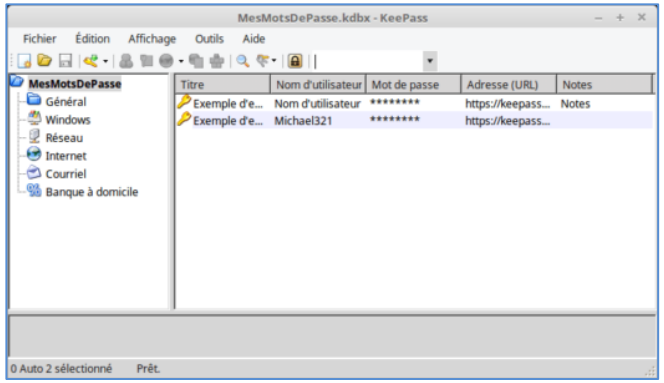
C’est une assez bonne solution à condition :
- de ne pas perdre le carnet ou l’oublier quelque part…
- de ne pas le laisser à côté de l’ordi à la maison,
- de le tenir à jour si vous changer un mot de passe,
- de ne pas se tromper en copiant les mots de passe dedans

Astuce pour ne pas se tromper en copiant le mot de passe :
- utiliser un générateur de mot de passe,
- copier le mot de passe une fois généré,
- le coller dans votre notepad ou word, puis l’imprimer
- découper le mot de passe et coller le dans votre carnet

Confusions classiques :
5 et S; O et 0; majuscules/minuscules

Mettre les mots de passe dans un fichier

- L'outil idéal pour cela est d'utiliser un « tableur » :
  - Excel si vous avez « Office » de Microsoft,
  - Mais aussi, le tableur de « libre office » (gratuit)
  - Google sheet (outil de Google, accessible dans le Drive)



- Ce fichier contenant vos mots de passe doit être stocké de façon « discrète »
  - Choisir un nom discret (et non pas « mot de passe »!)
  - Le stocker sur l'ordi, sur un cloud, ou sur le serveur de votre FAI
  - pour plus de sécurité lui mettre un mot de passe à l'ouverture

Exemple de tableau

date de mise à jour	15/01/2024				
Nom du site	adresse du site	identifiant	Mots de passe	date	commentaire
carrefour	carrefour.com	toto@gmail.com	sjnqND	15/01/2024	
engie	engie.fr	toto@gmail.com	mlnfq,5454C	02/02/2024	
facebook	fb.fr	kiki.bing@orange.fr	khsdjdhv:d;,	12/12/2023	
intermarché	inter.fr	toto@gmail.com	QJC	21/06/2018	
nogenternet	nogenternet.fr	toto@gmail.com	sdkhqlvqlk	06/05/2019	
sncf	sncf.com	toto@gmail.com	QSCK?	06/10/2020	
société générale	sg.com	toto@gmail.com	KJFQjnc	05/08/2008	

Exercice

- création d’un tableau Excel pour les mots de passe

- Mettre un mot de passe pour protéger votre fichier excel

Mémoriser les mots de passe

(les différentes méthodes n'ont pas toutes le même niveau de sécurité)

- 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, Google 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 », certains sites l'impose.
  - *A vous de choisir dans les paramètres du compte*
  - Après avoir entré votre identifiant et votre mot de passe, vous recevez un code (valable quelques minutes)sur votre messagerie (e-mail ou téléphone (SMS).
  - 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

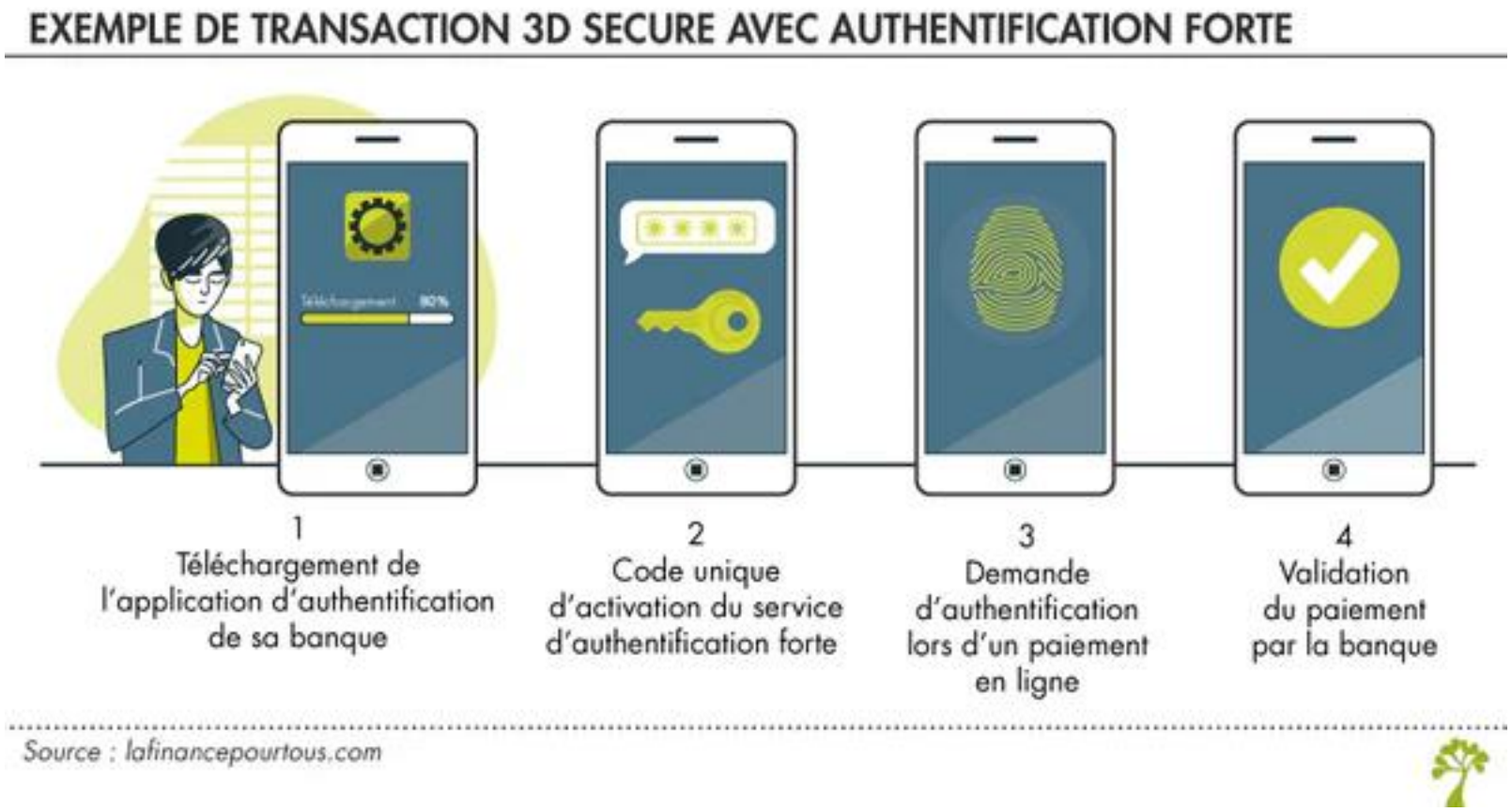
La double authentification « renforcée »
« 3D secure »

- But principal : renforcer la sécurité des transactions (achats) et réduire les fraudes.
- Principe :
  - Vous effectuez un achat en ligne (avec votre carte bleue)
  - La banque vérifie votre identité(via l'application bancaire installée sur **votre téléphone**)(1).
  - Vous autorisez la transaction sur votre téléphone (avec un code ou pas, selon les banques)
  - La transaction est autorisée ou refusée par la banque.

(1) Nécessite d'avoir installée l'application sur votre téléphone auparavant, et d'autoriser dans les paramètres d'avoir « le pass sécurité », ou « certicode plus » (ou autre terme) (clé installée sur votre téléphone)

Utilisez la double authentification

(sécurisation du compte)



Ce que je peux faire avec le Pass Sécurité

- **L'ajout d'un nouveau compte bénéficiaire** depuis L'Appli SG
- **Le Paiement 3D-Secure**, pour sécuriser vos transactions en ligne
- **La signature électronique**, le moyen le plus sûr de sécuriser vos documents officiels
- **La modification du plafond de carte**[3], pour augmenter exceptionnellement vos plafonds bancaires.
- **La consultation du Code Secret** de votre carte bancaire en ligne
- **Le service Paylib**[2], pour utiliser votre mobile comme une carte bancaire (en ligne, en magasin ou pour payer vos amis)
- **Le virement international**, pour effectuer des virements dans le monde entier et dans plus de 30 devises[4].
- **Le virement instantané**

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
  - N'oubliez pas de mettre à jour votre fichier et/ou votre carnet

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, dashlane 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
- Franceconnect pour les services publics

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

- Rappel du cours (01/2024) 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 (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
- Utile quand on multiplie le nombre de comptes, mais peu sécurisé
  - 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 »

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 (site passwords.google.com),
  - 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 google
- La liste des mots de passe enregistrée apparait et vous pouvez alors pour chaque compte :
  - Afficher en clair le MP,
  - Le supprimer

Les gestionnaires de mots de passe

- Par exemple Keepass (recommandé par cybermalveillance.gouv.fr) ou Dashlane (25 mots de passe en version gratuite)
- Il faut les installer sur l'ordinateur (extension du navigateur), le téléphone (appli)
- Ils incluent un générateur de mot de passe
- Il faut définir un mot de passe « maître » pour accéder à vos mots de passe (mot de passe fort d'au moins 12 caractères)

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
- Le piratage d'un serveur d'une société dans lequel se trouve la base de données contenant votre compte

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
- Attention aux faux QR codes qui vous envoient sur de mauvais sites web