# Se protéger d'internet

www.nathalievanassche.be

# Feuille de route

1. Votre mot de passe est-il suffisamment fort ?
2. Apprenez à reconnaître les e-mails frauduleux
3. Sécurisez votre compte Google
4. Achetez en ligne en sécurité

# Créez un mot de passe fort

- comprend au moins 13 caractères ;
- ne contient ni votre nom d'utilisateur, ni votre vrai nom, ni le nom de votre société, ni un mot tiré de la musique (titre de chanson, nom de groupe ou de chanteur, …), etc. ;
- ne contient pas de mot entier ;
- est complètement différent des mots de passe que vous avez utilisés précédemment ou que vous utilisez pour d'autres services ;
- doit contenir des lettres (majuscules et minuscule), des chiffres et des caractères spéciaux (@ , < > ? ! $ etc.).

# Créez un mot de passe fort

- Exemple d'un mot de passe fort : 1tvTmQ2tl'Ap
- Optez pour des moyens mnémotechniques pour fabriquer et retenir des mots de passe forts

# Ne communiquez pas vos mots de passe

- Un mot de passe sûr, une fois volé, ne protège pas votre compte
- Les pirates informatiques ont plusieurs options pour voler votre mot de passe :
- Ils volent votre mot de passe par le biais du phishing ou de faux messages. Vous tombez dans le panneau et leur communiquez inconsciemment votre mot de passe

Exemple :
« Bonjour, je suis le responsable informatique de l'entreprise SuperAntiVirus, j'ai besoin de votre mot de passe pour mettre votre système à jour et vérifier vos coordonnées client, celui-ci ne sera pas partagé et vous pourrez le changer ensuite. »

- Une fuite de données au niveau du service en ligne d'une entreprise peut diffuser votre mot de passe sur la toile.

# Et en plus :

- Pensez à changer votre mot de passe pour un compte donné régulièrement ! Changez-le au moins tous les 3 mois.
- N'utilisez pas les mêmes mots de passe sur plusieurs sites différents
- Ne conservez pas vos mots de passe dans un endroit visible

# Mon compte est piraté !

- Lancez votre antivirus pour vérifier si un virus a infecté votre appareil
- Changez immédiatement tous vos mots de passe à partir d'un ordinateur différent de celui sur lequel vos données ont été volées. Ne réutilisez pas le même mot de passe pour plusieurs comptes ; les mots de passe doivent être forts et uniques. (Voir chapitre 02 de ce cours).
- Si vos coordonnées bancaires ou les coordonnées de votre carte de crédit ont été volées, avertissez votre banque et surveillez vos comptes. Contactez Card Stop au 070 344 344.
- Si des données professionnelles ont été volées, avertissez au plus vite votre employeur.
- Prenez contact avec le site ou le service piraté et demandez-leur quelles mesures peuvent être prises.
- Déclarez le piratage auprès de la Commission de la Protection de la Vie Privée.
  https://www.privacycommission.be/

# 2. Apprenez à reconnaître les e-mails frauduleux

- Le phishing est une escroquerie en ligne à l'aide de faux e-mails, sites Internet ou messages. Comment reconnaître ces faux e-mails et faire la distinction entre les faux et les vrais messages ? Des cybercriminels habiles arriveront à vous faire douter !

- Faux e-mails : ne vous laissez plus piéger !
  (Vérifiez les cinq signes d'authenticité d'un e-mail)
  https://www.cybersimple.be/fr/sujets/faux-e-mails-ne-vous-laissez-plus-pi%C3%A9ger
- Test : Identifiez-vous à temps les messages suspects ?
  https://www.safeonweb.be/fr/participation/add/55

# Se protéger du pishing

- Vous devez protéger vous-même vos propres données personnelles (en ne les partageant pas de façon publique sur Internet) et sécuriser suffisamment vos mots de passe.
- Se méfier de ce qui paraît « trop beau pour être vrai » – ne pas être trop émotif/ve face à des situations du type argent facile, amour facile, guérison facile…etc. Comprendre également qu'une publicité reste une publicité.  Faire attention aux services gratuits
- Ne pas se connecter à des réseaux Wi-fi publics ou sur un ordinateur public pour effectuer des transactions importantes (bancaires) et sécuriser son accès wi-fi domestique, afin d'empêcher les connexions intrusives.
- Ne pas minimiser la menace (« ils font juste cela aux grandes entreprises », « je ne vais pas sur des sites bizarres donc je suis à l'abri » sont des exemples de fausses affirmations qui mettent l'internaute en danger car ces pensées font relâcher l'attention).
- Prendre le temps de rechercher sur Internet lorsque vous n'êtes pas sûr(e) : une simple recherche Google permet parfois d'éviter une attaque inopinément !

# 3. Sécurisez votre compte Google

- Ne jamais laisser son compte ouvert sur un pc public
- En cas d'oubli, comment se déconnecter à distance ?
- Définissez un nouveau mot de passe introuvable
- Ajouter un téléphone et / ou mail de secours
- Activez la vérification en deux étapes
- Google Authenticator (Nouveauté 2019)
- Etablir un Check-up de sécurité

# 4. Achetez en ligne en sécurité

- Avez-vous les bons réflexes pour bien protéger vos transactions en ligne ? https://www.cybersimple.be/fr/sujets/comment-savoir-si-je-peux-faire-confiance-%C3%A0-un-site-web

# Conseils pour acheter en sécurité sur internet

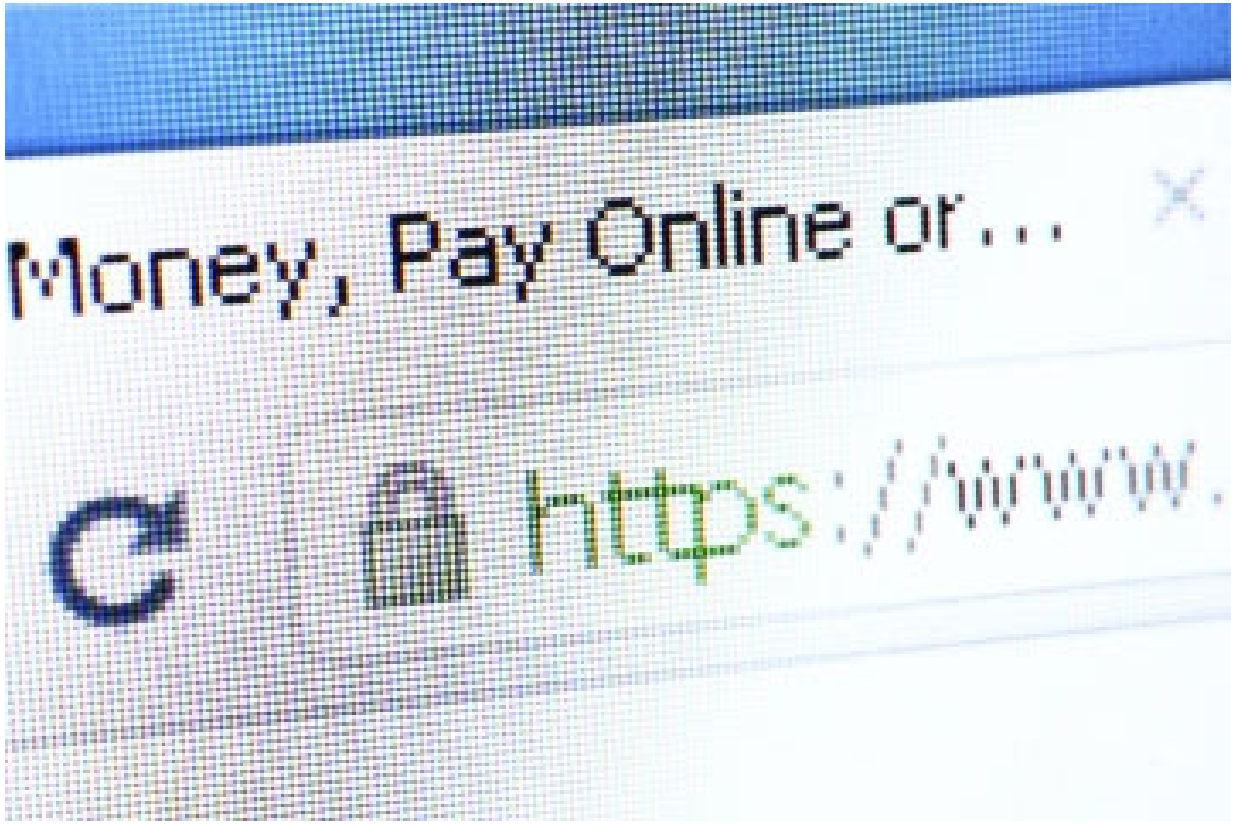
- Sécurisez votre navigation sur internet
  Effectuez toujours vos achats sur internet à partir d'une connexion WIFI protégée (de préférence chez vous). En d'autres termes, évitez de réaliser des transactions financières sur un réseau WIFI gratuit ouvert à tous.
- Préférez les sites connus
- Une boutique internet en règle (voir ci-après)

# Une boutique internet en règle

- S'il s'agit de votre premier achat sur ce site, vérifiez les points suivants :
  - Les informations sur l'entreprise doivent être claires et complètes (nom, adresse, service clients).
  - On doit pouvoir les contacter par téléphone ou courrier électronique.
  - Les garanties de livraison et de retour doivent être indiquées.
  - Vous devez pouvoir accéder à vos données personnelles et demander leur correction ou suppression.
  - Les Conditions Générales de Vente du site marchand doivent décrire précisément les modalités de paiement applicables sur le site : carte débitée à la commande ou à l'expédition ou encore après réception et vérification du bien acheté, etc.

# Conseils pour acheter en sécurité sur internet

- Une zone de paiement est bien sécurisée
  Dans une zone de paiement sécurisé, l'adresse du site commence par « https :// ». Les informations que vous donnez sont alors cryptées et traitées par les serveurs de sociétés spécialisées qui assurent la fiabilité des transactions. Dès que vous pénétrez sur un site sécurisé, une boîte de dialogue vous informe que les informations fournies seront protégées. Quand la sécurisation de votre paiement est assurée, un cadenas fermé ou une clé s'affiche devant l'adresse internet du site.


Money, Pay Online or...
https://www.

# Conseils pour acheter en sécurité sur internet

- Avez-vous reçu un accusé de réception ?
  Lorsque vous passez commande sur un site internet, le commerçant en ligne a l'obligation de vous faire parvenir, sans délai, un accusé de réception reprenant le récapitulatif de votre commande. Il est recommandé de soigneusement vérifier ce récapitulatif afin de rapidement réagir si une erreur s'est glissée dans la commande.
- Surveillez vos extraits de compte
  Vérifiez au moins une fois par semaine vos extraits de compte afin de déceler des opérations frauduleuses.

# Flairer l'arnaque

- C'est trop beau pour être vrai ? Méfiez-vous !
- Méfiez-vous des offres exceptionnelles à saisir immédiatement. Elles peuvent se révéler peu intéressantes par après, voire plus chères que dans le commerce normal. Ne vous laissez surtout pas mettre sous pression.
- Si on vous demande de payer une somme d'argent pour des raisons peu claires ou illogiques, ne le faites pas. Evitez de payer via un service de transfert de paiement tel que Western Union.
- Vérifiez sur Internet, sur Facebook si d'autres internautes n'ont pas posté d'avis négatifs (le nom du site + « avis » ou « arnaque »). Découvrir les expériences malheureuses vécues par d'autres consommateurs permet d'éviter de que l'on ne tombe soi-même dans le piège.
- Si vous avez des doutes sur le vendeur, la société qu'il représente ou les produits qu'il vend, mieux vaut ne rien acheter.

# Réagir en cas d'arnaque

- Si vous pensez avoir été victime d'une arnaque à la consommation ou si vous soupçonnez une arnaque, signalez la fraude et l'escroqueries via pointdecontact.belgique.be (https://meldpunt.belgie.be/meldpunt/fr/bienvenue). Plateforme en ligne où les consommateurs et les entreprises peuvent signaler les tromperies, fraudes, arnaques ou escroqueries. Sur la base de questions concrètes, ils reçoivent immédiatement une réponse reprenant un avis et/ou un renvoi à l'instance compétente pouvant les aider.
  Vous contribuerez ainsi à éviter que d'autres personnes tombent dans le piège !
- Si la fraude consiste à une récupération de vos données bancaires vous devez rapidement bloquer votre compte bancaire via Card Stop au 070 344 344 et contacter votre banque pour qu'elle suspende votre abonnement de banque par internet.
- Vous avez payé avec votre carte de crédit ? Contestez le paiement auprès de l'émetteur de votre carte de crédit.

# Protégez les données de votre carte bancaire

- Ne donnez jamais le code confidentiel de votre carte bancaire, à qui que ce soit.
- N'enregistrez jamais les informations de votre carte (numéro, date, cryptogramme) en tant qu'identifiant commercial sur un site marchand.
- Evitez de donner les informations de votre carte par courrier (électronique ou papier), par sms ou téléphone si vous pouvez faire autrement (paiement par internet…). Ne donnez les informations et données de votre carte qu'à un commerçant dont vous êtes sûr.

# Pour un achat en ligne ou pour une réservation, on peut vous demander

- le n° de votre carte bancaire : 16 chiffres répartis en 4 blocs de 4 chiffres (au recto),
- la date d'expiration (au recto),
- le cryptogramme : 3 derniers chiffres imprimés (au verso de la carte à côté de la zone de signature),
- le nom et éventuellement le prénom (au recto)
- un code supplémentaire de type 3DSecure sur certains sites marchands *. Envoyé par sms, courrier électronique, téléphone (le SMS étant le plus souvent utilisé), ce code permet de vérifier que la personne en train d'effectuer le paiement est bien le propriétaire de la carte.
- *Tous les paiements par carte sur internet ne sont pas concernés par ce système ; certains sites commerçants, y compris de grands acteurs, n'ont pas ce dispositif de protection pour le client.

# Attention aux arnaques sur internet ! (Complément)

- Emission on n'est pas des pigeons :
- https://www.rtbf.be/info/societe/onpdp/detail_attention-aux-arnaques-sur-internet?id=9191060