Cyber Sécurité

lifebeats

lyondellbasell

Quelle Sécurité pour Vos Données Personnelles en Ligne?

- Certains logiciels et solutions indiqués sur cette présentation sont donnés uniquement **à titre d'information** et ne peuvent être installés que sur **votre ordinateur personnel** (ne pas utiliser sur les supports informatiques LyondellBasell**) à vos propres risques**. LyondellBasell ou l'une de ses entités ne peuvent pas être tenus responsables en cas de dommages physiques ou portant sur les logiciels causés à votre équipement ou sur des données.

- Votre identité en ligne est votre passeport pour interagir avec des millions de services disponibles en ligne, allant de l'e-mail à des applications d'entreprise, des magasins web et même des téléphones cellulaires.

- Avez-vous déjà pensé aux risques de perdre des informations personnelles ou d'exposer votre identité en ligne?

Risques liés aux E-mails

- **Un compte de courriel unique pour tout ce que vous Faites**
  - Difficile de naviguer entre ce qui est légitime et «d'autres types d'informations» que vous recevez
  - Un point d'échec - Si vous perdez ce compte de messagerie, il n'y a généralement pas de "plan B"
  - Des mécanismes efficaces pour prévenir les e-mails basés sur le phishing

Tout ce que vous devez faire est de donner votre e-mail de suite!

Que signifie Phishing?
Phishing est l'envoi d' e-mails courants basés sur de la manipulation et la fraude sociale. C'est une technique avec laquelle les cyber- délinquants tentent de vous tromper en vous demandant d'effectuer une action ou de divulguer une information.

Comment Ne Pas Utiliser d’e-mails de façon risquée

- Une règle d’Or - Plus votre e-mail devient public, plus vous recevrez de SPAM et d’e-mails frauduleux-phishing .

- Avoir plusieurs comptes de messagerie pour traiter des domaines différents.
  - Communication personnelle
  - listes de communication et de distribution
  - Promotions
  - Loisirs
  - Achats en ligne

- S’ inscrire uniquement sur des sites qui paraissent vraiment pertinents. Éviter les offres de dernières minutes pour "donner votre carte de visite".

- Lors d‘une inscription à un service par e-mail, NE JAMAIS RÉUTILISER le meme MOT DE PASSE.

Mots de Passe – Risques Associés

- Mots de Passe (✝ RIP)
  - Ne jamais le réutiliser!
  - Les criminels sont capables de vérifier les noms d'utilisateurs et mots de passe sur plusieurs sites Web.
  - Même si vous acceptez les risques, quelles conséquences pour vous si vos fournisseurs étaient piratés ?
  - Avez-vous déjà utilisé un ordinateur dans un cyber café, hôtel ou tout autre ordinateur partagé? Il y a de grands risques que vos informations d'identification soient déjà dans des mains criminelles.

Proteger Les Mots de Passe

- **Ne jamais**, en aucune circonstance, réutiliser ses mots de passe.

- Lors de la souscription de services en ligne, toujours chercher **un deuxiéme moyen d'authentification** (mot de passe unique, appels, SMS ou même des e-mails envoyés sur un compte secondaire).

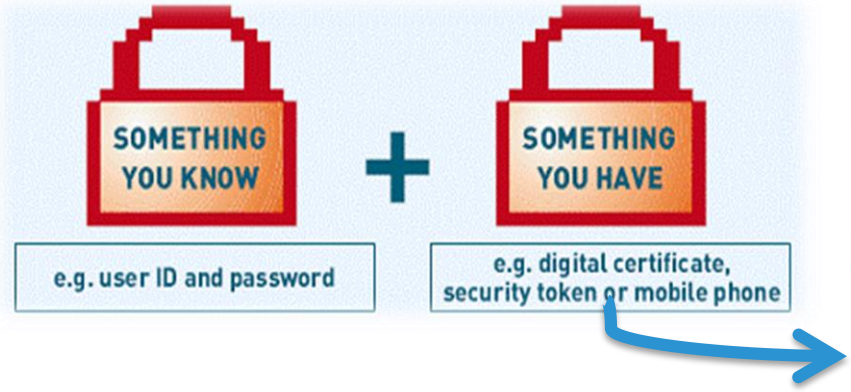
- L'utilisation du mot de passe général « gardien » peut être utile quand il utilise un cryptage avancé et ne permet pas des aller-retour sur une navigation Internet.

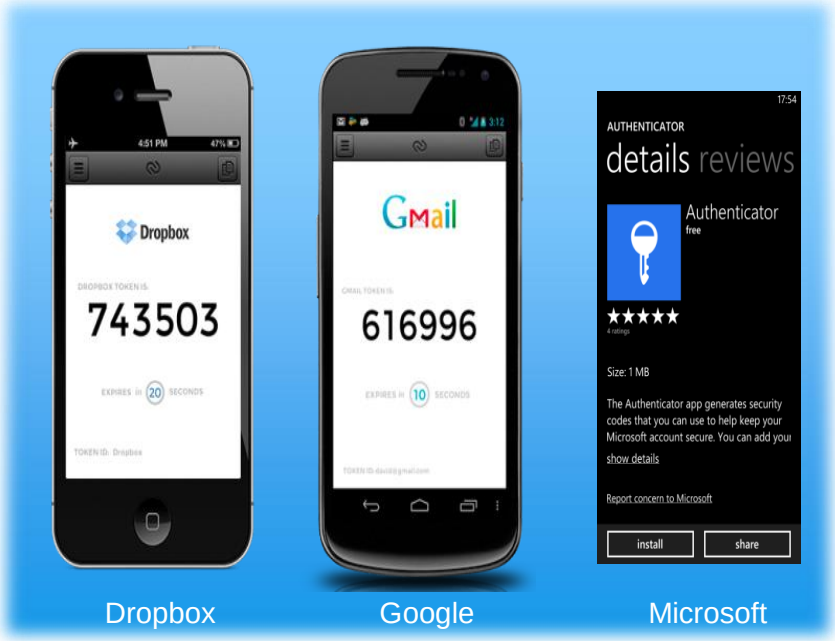
- Éviter de laisser des supports « intelligents » sans etre protegés par un mot de passe.

Renforcer la Sécurité des E-mails – Associer deux Moyens d‘Authentification

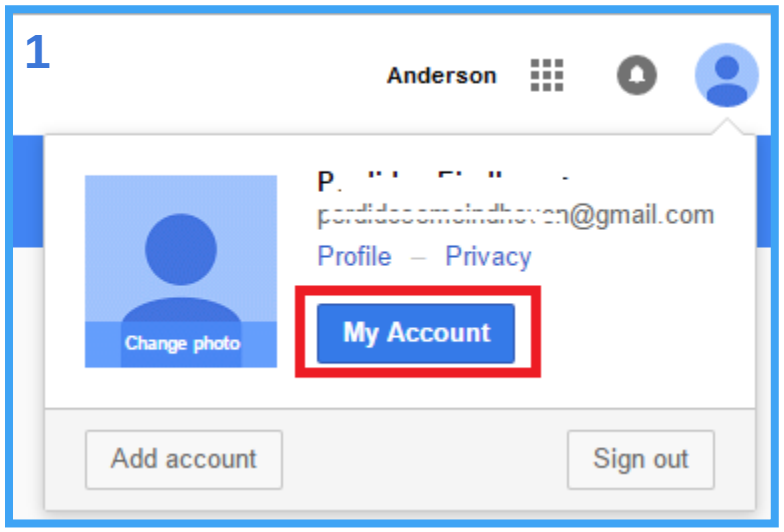
- Pour se connecter à un fournisseur par e-mail, on est généralement tenu de fournir **un seul facteur d'authentification**, **pratique** habituellement **utilisée**, comme un mot de passe par exemple.

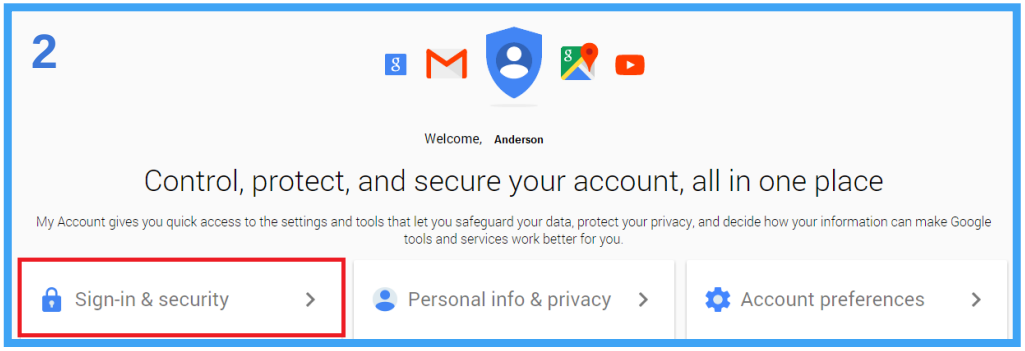
- Il est évident que si un pirate obtient l'accès à votre mot de passe, il est presque certain qu'il sera en mesure d'accéder à votre e-mail, à moins que ...

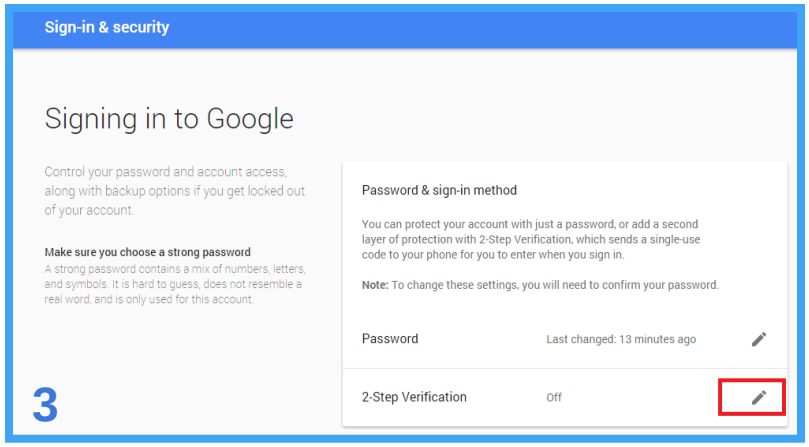


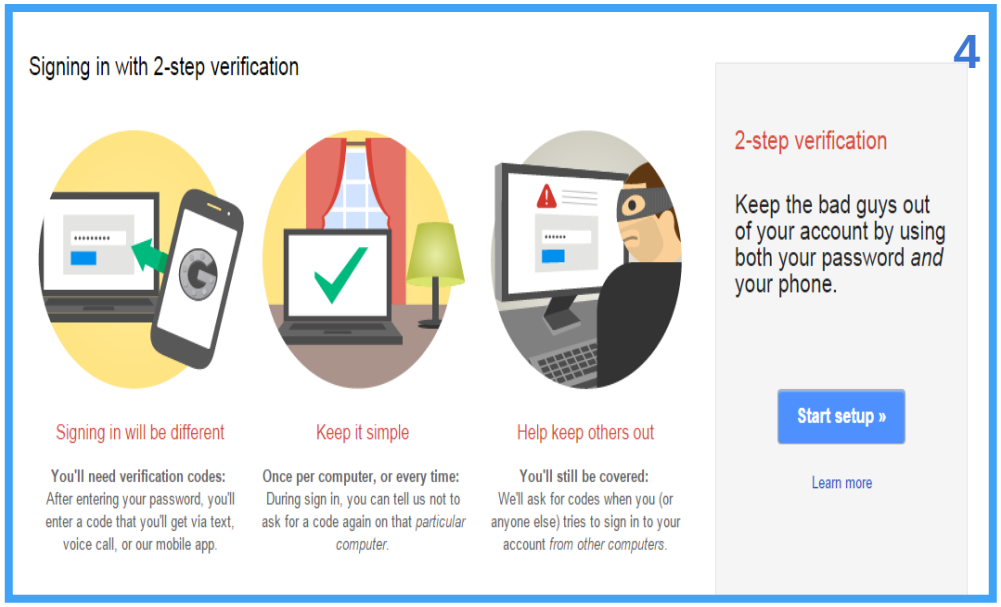


Activation sur Google de 2 Moyens d' Authentification en 2 Etapes

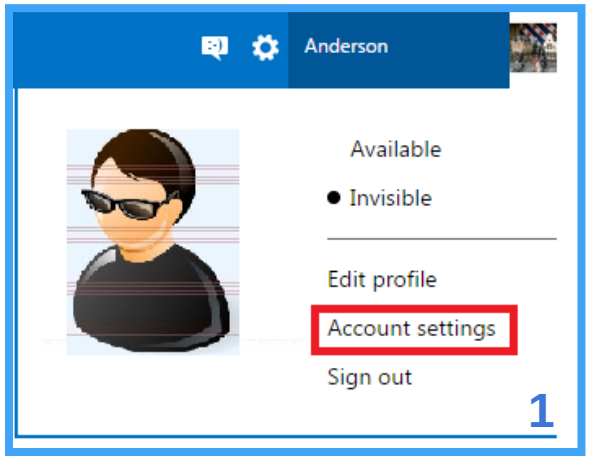


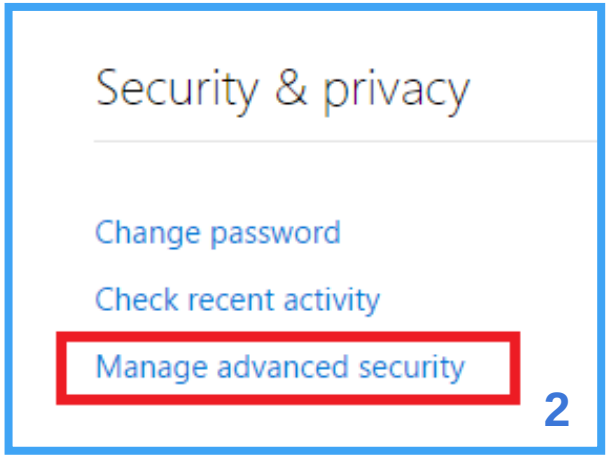


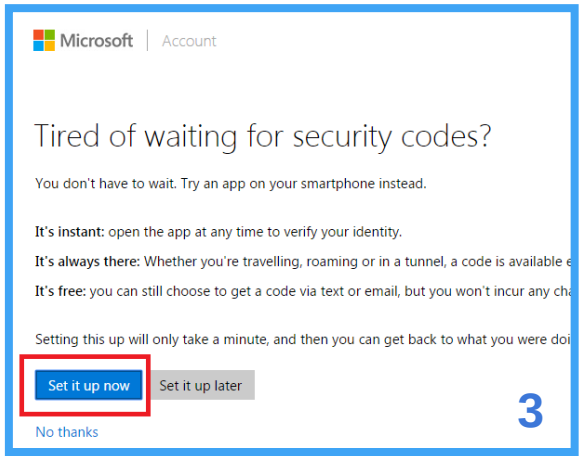


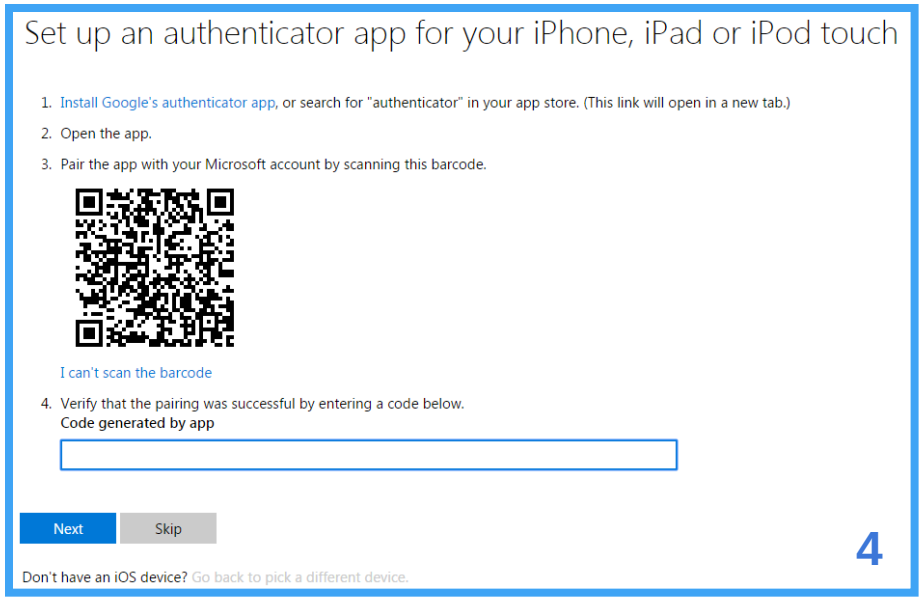


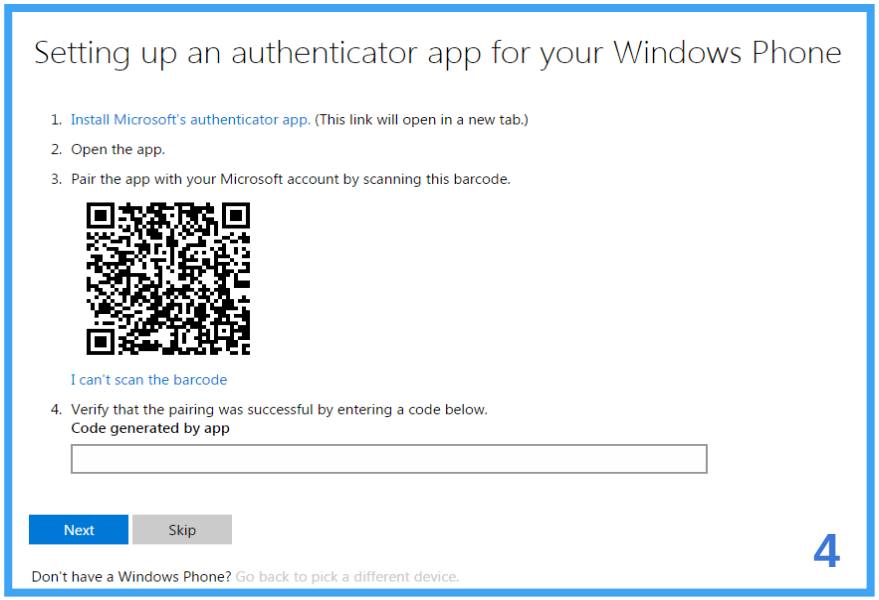
Activation sur Microsoft de 2 Moyens d' Authentification en 2 Etapes











Ordinateurs au Domicile - Pratiques à Risques

- Un seul ordinateur et plusieurs utilisateurs:
  - Différents types d'accès exigent différents niveaux de sécurité;
  - Il est prouvé (le piratage, les jeux et la pornographie) sont fréquemment utilisés par les criminels pour ’planter ’ les logiciels à partir de virus malveillants.
  - Avez-vous confiance en l'ordinateur de votre ami? Prend-il soin de son ordinateur de la même manière que vous le faites?
- Faire attention à la connexion de périphériques de stockage ou de DVD à partir d'autres périphériques. Des contaminations par des virus à partir de clés USB sont encore des techniques très fréquentes.

Multi-Fonctions Mais ... Avec des Limites

≠

Comment Ne Pas Utiliser l'Ordinateur de façon risquée

- Séparer les Affaires et les Divertissements; Il n'est pas possible de gérer les deux domaines sur un même système informatique sans s'exposer à des risques sérieux. Le même principe est à appliquer avec l'utilisation des appareils mobiles.
- .Ne Pas Partager les Ordinateurs! Une erreur ou plutot un problème est – l'utilisation des ordinateurs de conférence et des ordinateurs des Hôtels et Cyber Cafés.
- Acheter Un Système de Sécurité Complet (Firewall, Antivirus, AntiSpam) et activer OS (Windows, Android, Mac OSX, Linux ou XYZ) avec des mises à jour automatiques.
- Eviter le téléchargement ou l'acquisition d'un logiciel à partir de Sources Inconnues ou partagées avec des amis.
- Toujours Garder son matériel Informatique avec des systèmes mis à jour en installant les correctifs nécessaires et les mises à jour régulières des antivirus.

Cyber Sécurité

Elle est entre Vos Mains!

Commencez Dès Aujourd'hui.

Rédigé par: Anderson Domingues (LBR) & Suzanne Jurczik (LBR)