



Sécurité sur internet

Partie 2

Liens & emails



Sécuriser la navigation web

- ▶ La meilleure invention d'internet ? ➔ Les liens !
- ▶ Mais leur simplicité peut être dangereuse
- ▶ Suivre un lien à partir d'un site :
 - ▶ Si le lien est sur une page d'un site « connu » **NON-participatif** (c'est à dire le contenu est écrit par la société et non le monde entier) il est probablement sans danger
 - ▶ Se méfier des liens dans les endroits « publics » comme des forums, des réseaux sociaux (en particulier twitter) ou pire des sites de « streaming » vidéos ➔ danger
- ▶ Comment vérifier un lien ?
 - ▶ Vérifier l'adresse qui se trouve derrière un lien avant de cliquer dessus. Pour cela passer la souris sur le lien sans cliquer ce qui affichera l'adresse du site internet et non l'alias qui vous est présenté. Ceci est particulièrement utile pour les liens reçus dans des e-mails. Le nom de domaine de cette adresse doit toujours être exactement identique à celle attendue et connue de vous.
- ▶ Penser à vous déconnecter d'un site une fois l'utilisation terminée.

Sécurité sur les emails

- ▶ La meilleure invention d'internet ? ➔ Les mails !
- ▶ Mais la simplicité pour envoyer/recevoir un email peut être dangereuse
- ▶ 3 type d'attaques dans les emails



SPAM est ennuyeux mais peu dangereux



Phishing pour voler de l'argent ou des données
Le Phishing (Hammeçonnage) va être totalement générique en envoyant le même mail à des millions de gens.
Le Spear-phishing (Pêche à la lance) est en plus ciblé directement sur vous car la personne veut vous attaquer et a trouvé des portions de données personnelles sur le net permettant de vous cibler.

Sécurité sur les emails

- ▶ Vous **connaissez** l'expéditeur
 - ▶ Vérifiez quand même son adresse email
 - ▶ Vérifiez le « Reply To » ou « Réponse à » qui peut être différent
 - ▶ Avant de cliquer sur un lien vérifier l'adresse sous-jacente en laissant votre souris au-dessus
 - ▶ Avant de cliquer sur une pièce jointe, vérifiez l'extension de la pièce jointe : **ne pas** cliquer sur un .exe, .vbs, .bat, .com et ne cliquez que sur des extensions de documents connus (.jpg, .doc, .docx, .xls, .xlsx, .png, .mp4, .mov, .avi etc...)
- ▶ Vous **ne** connaissez **pas** l'expéditeur
 - ▶ Si l'email semble URGENT ou semble grave : c'est **très probablement** une arnaque
 - ▶ Vérifiez son adresse email
 - ▶ Avant de cliquer sur un lien vérifier l'adresse sous-jacente en laissant votre souris au-dessus comme sur une page web, si vous ne pensez pas que cela soit utile, éviter de cliquer dessus
 - ▶ N'ouvrez **aucune** pièce jointe
 - ▶ « ... » et Afficher l'original peut vous donner des infos plus précises (mais **très** techniques)

