



Contenu de la séance

- **Un peu de vocabulaire pour bien se comprendre**
 - Qu'est-ce que l'informatique et le traitement de l'information?
 - Qu'est-ce qu'un champ de saisie?
 - Qu'est-ce que l'hameçonnage?
 - Qu'est-ce qu'une extension?
- **Les autres fonctions de base de Chrome**
 - La protection contre l'hameçonnage
 - La suppression de la publicité et les extensions
 - Les téléchargements
 - La recherche d'un mot dans une page Web
 - L'impression d'une partie d'une page Web et d'une image d'une page Web
 - La saisie semi-automatique
 - Les témoins (cookies en anglais)
- **L'annonce de la prochaine séance Facile**
 - Je serai disponible 30 minutes avant le début de la prochaine séance Facile pour répondre à vos questions
 - Comment se retrouver sur son ordinateur présenté par Francine Couture

Note: Les exercices et les notes des exercices ont été développés avec l'environnement suivant:

- Windows 10 version 1803
- Chrome version 69



Chrome - 2ième Partie

Un peu de vocabulaire pour
bien se comprendre



Qu'est-ce que l'informatique?

- Créé en 1957, par un ingénieur allemand (Karl Steinbuch), le terme « Informatik » fait déjà référence au traitement **automatique** de l'**information**.
- Ce n'est qu'en 1966, que l'Académie française consacre l'usage officiel du mot **Informatique** pour désigner la « **science du traitement de l'information** » (TI).
- Donc l'informatique est un **domaine d'activité scientifique, technique et industriel** concernant le **traitement automatique de l'information** par l'**exécution de programmes informatiques** par des **machines** telles que : **ordinateurs, robots, appareils intelligents connectés**, etc.
- Le **traitement de l'information en informatique** est orienté vers **l'obtention de résultats planifiés** via la **transformation des données** (information formatée) fournies aux **applications**.
- Simplement dit, il s'agit pour l'application de :
 - **lire (lecture)** les données nécessaires à la production des résultats,
 - **mémoriser** ces données afin de les utiliser,
 - **traiter** les données reçues pour les transformer en résultats,
 - **écrire/afficher/émettre les résultats** recherchés sur le média de sortie choisi (mémoire interne, écran, disque dur ou virtuel, clé USB, CD, DVD, haut-parleurs, etc.).



Qu'est-ce qu'un champ de saisie?

- Un **champ de saisie** est une **zone** d'un **formulaire**, d'une **page Web** ou d'un **écran d'application** qui ressemble à un **rectangle de taille variable** à l'intérieur duquel **l'utilisateur écrit une donnée ciblée** (ex. : nom, adresse, âge, date de naissance, etc.) pour qu'elle soit ensuite **utilisée par une application** ou **envoyée à un site Web** dans le cas d'un formulaire de page Web.
- Lorsqu'on passe le pointeur de sa souris au-dessus d'un champ de saisie, le pointeur se transforme en icône de sélection de texte (I) pour indiquer à l'utilisateur que cette zone peut être sélectionnée, par un clic, afin d'y écrire via le clavier un texte ou une donnée. Lors du clic sur un champ de saisie, le curseur se met à clignoter pour indiquer l'endroit où le texte entré sera éventuellement inséré.
- Les champs de saisie sont normalement vides mais parfois ils contiennent une valeur par défaut correspondant soit à la valeur la plus fréquemment utilisée ou soit à un mot décrivant la fonction du champ (ex. : Recherche).
- En général, il est possible d'effectuer des opérations de copier-coller dans les champs de saisie.
- Un exemple connu de champ de saisie se retrouve sur la page **google.ca**
- [Voir le formulaire questions aux ateliers du CIMBCC](#)



Chrome - 2ième Partie

L' Hameçonnage



Qu'est-ce que l'hameçonnage?

- Créer et envoyer massivement des courriels pour tromper le destinataire afin de lui soutirer des renseignements personnels ou financiers de nature confidentielle.
- Tenter d'obtenir du destinataire:
 - des renseignements bancaires
 - numéros de carte de crédit,
 - numéros d'assurance sociale
 - identifiants et mots de passe de comptes courriels ou autres services payants en ligne
- Afin de frauder directement ou d'usurper l'identité de la victime, ou vendre ces informations à un autre individu dans le même but.
- Parfois difficile d'identifier une tentative d'hameçonnage car:
 - le message a un format similaire avec le logo de la société, son nom,
 - le message est rédigé en des termes rappelant ceux utilisés par l'organisation usurpée
 - le message incite le destinataire à réagir immédiatement afin d'éviter une perte financière, faire un gain ou éviter que son compte en ligne soit fermé
 - le message contient un lien qui dirigera la victime potentielle vers un site Internet ressemblant au site légitime et d'où les renseignements personnels du destinataire seront enregistrés.

Note : L'information précédente est extraite de la page sur la Cybercriminalité de la Sûreté du Québec.



Comment Google nous aide à éviter les pièges de l'hameçonnage?

- **Google** a conçu la fonction « **Navigation sécurisée** » pour identifier les sites Web suspects et en informer les internautes
 - Cette fonction analyse des milliards de site Internet chaque jour, à la recherche de sites Web suspects
 - Des milliers de nouveaux sites douteux sont découverts tous les jours, parmi lesquels de nombreux sites Web légitimes ayant été piratés
 - Analyse et gestion de dénonciations de sites Web par les internautes.
- Ces sites suspects sont signalés aux utilisateurs, afin qu'ils évitent ces pièges, par des avertissements dans les recherches Google, les navigateurs Web et les courriels Gmail pour ceux qui y sont inscrits.
- Il est important de noter **qu'il y a toujours un certain délai entre la diffusion d'une attaque d'hameçonnage sur le Web et sa détection** par les autorités concernées telles que Google.
- **La protection offerte par Google auprès de ses utilisateurs de Chrome et Gmail n'est donc pas absolue et il faut donc rester très vigilant à tout moment pour ne pas devenir les premières victimes d'une nouvelle attaque.**
- **Les paramètres de protection offerts par Google Chrome sont activés, par défaut, lors de l'installation.** Vous n'avez donc rien à faire pour obtenir cette protection mais restez toujours vigilant quand même.

Note : L'information précédente est extraite du site de Google Chrome.



Avertissements concernant les sites dangereux ou trompeurs dans Chrome

Si vous voyez l'un de ces messages, fermez l'onglet du site et ne tentez plus d'y accéder.

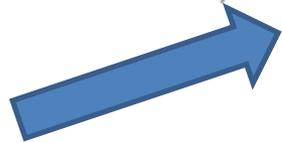
- **Le site que vous allez ouvrir contient des logiciels malveillants** : le site que vous essayez de consulter risque d'installer un logiciel malveillant sur votre ordinateur.
- **Le site Web que vous allez ouvrir est trompeur** : il se peut que le site que vous essayez de consulter pratique l'hameçonnage.
- **Le site Web que vous allez ouvrir contient des programmes dangereux** : le site que vous essayez de consulter risque de vous inciter à installer des programmes nuisibles à votre expérience de navigation.
- **Cette page tente de charger des scripts à partir de sources non authentifiées** : le site que vous consultez n'est pas sûr.

Soyez prudent lorsque vous téléchargez des fichiers : certains sites tentent de vous inciter à télécharger des logiciels nuisibles **en disant avoir détecté un virus sur votre ordinateur.**



Vérifier la sécurité de la connexion d'un site dans Chrome

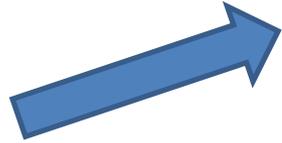
Pour vérifier la sécurité d'un site, consultez l'état de sécurité à gauche de l'adresse Web :



 **Sécurisé**

Les informations que vous envoyez ou recevez via ce site sont privées.

Même si cette icône est visible, restez vigilant lorsque vous communiquez des informations privées. Regardez la barre d'adresse pour vous assurer que vous êtes bien sur le site que vous souhaitez consulter.



 **Informations ou Non sécurisé**

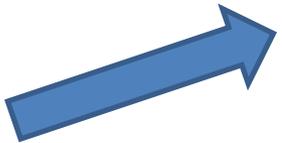
La connexion au site n'est pas privée. Un tiers pourrait voir ou modifier les informations que vous envoyez ou recevez via ce site.

Les messages "Connexion non sécurisée" ou "Paiement non sécurisé" peuvent s'afficher. Nous vous déconseillons de saisir des informations sensibles comme un mot de passe ou le numéro d'une carte de paiement.

Sur certains sites, vous pouvez accéder à une version plus sécurisée de la page que vous consultez. Pour ce faire, procédez comme suit :

1. Sélectionnez la barre d'adresse.
2. Supprimez `http://`, puis saisissez `https://` à la place.

Si cela ne fonctionne pas, contactez le propriétaire pour lui demander de sécuriser son site et vos données avec le protocole HTTPS.



 **Non sécurisé ou Dangereux**

Nous vous déconseillons de saisir des informations privées ou personnelles sur cette page. Si possible, n'utilisez pas le site.

Non sécurisé : prenez toutes les précautions nécessaires. La connexion à ce site présente un grave problème sur le plan de la confidentialité. Un tiers pourrait voir les informations que vous envoyez ou recevez via ce site

Les messages "Connexion non sécurisée" ou "Paiement non sécurisé" peuvent s'afficher.

Dangereux : évitez ce site. Si une fenêtre d'avertissement rouge s'affiche sur toute la page, cela signifie que le site a été signalé comme étant à risque par la fonctionnalité de [navigation sécurisée](#) . Il est probable que la consultation de ce site représente un risque pour vos informations privées.



Comment signaler à Google une page Web d'hameçonnage?

The screenshot shows a web browser window with the URL https://safebrowsing.google.com/safebrowsing/report_phish/?hl=fr. The page title is "Signaler une page de phishing". The main text reads: "Merci de nous aider à éradiquer les sites de phishing présents sur le Web. Si vous pensez avoir découvert une page qui se fait passer pour une autre dans le but de s'appropriier des renseignements personnels sur les internautes, veuillez remplir le formulaire ci-dessous pour signaler la page à l'équipe de navigation sécurisée Google. Les informations contenues dans le rapport seront traitées conformément aux [règles de confidentialité](#) de Google." The form includes a text input field for "URL :", a reCAPTCHA widget with the text "Je ne suis pas un robot" and "reCAPTCHA Confidentialité - Conditions", a text input field for "Commentaires : (facultatif)", and a button labeled "Envoyer le rapport". The Google logo is visible in the bottom right corner of the form area.

Copier l'adresse suivante dans la barre d'adresses de Chrome pour atteindre le formulaire de Google pour signaler un site d'hameçonnage:

https://safebrowsing.google.com/safebrowsing/report_phish/?hl=fr



Protection contre l'hameçonnage - Exemple 1

Message de Gmail lors du clic sur le lien

The screenshot shows a web browser window with the URL <https://support.google.com/mail/answer/1074268?hl=fr>. The page title is "Aide Gmail". The main content area has a red header with "Aide Gmail" on the left and "GMAIL", "FORUM D'AIDE", and "AIDE TWITTER" on the right. The main text reads: "Avertissement : 'Ce message peut cacher une tentative d'escroquerie.'" Below this, a paragraph explains: "Chaque fois que vous recevez un e-mail susceptible de cacher une tentative d'escroquerie, mais dont l'expéditeur est dans votre liste de contacts Gmail, un avertissement s'affiche." A section titled "Que faire lorsque ce message s'affiche ?" contains two dropdown menus: "Vous pensez que l'e-mail en question est une tentative d'escroquerie" and "Vous ne pensez pas que l'e-mail en question est une tentative d'escroquerie". At the bottom, there are social sharing icons for Google+, Twitter, and Facebook, and a feedback section asking "Cet article vous a-t-il été utile ?" with "OUI" and "NON" buttons. The footer includes copyright information: "©2017 Google - Règles de confidentialité - Conditions d'utilisation - Règlement du programme" and a language selector set to "français".



Protection contre l'hameçonnage – Exemple 1

Message de Chrome lors du clic sur le lien

W Catégorie:Sigle de 3 cara x Messengerie - michel_gag x Erreur liée à la sécurité x

Dangereux | 84.38.130.62/applications/

Applications Vins CIMBCC ~ Agora cPanel Wiki C... test1 ~ ~ + Pocket LP La Presse Météo OLF TSX IMDB W an W fr W ATH Autres favoris



Le site Web que vous allez ouvrir est trompeur

Les individus malveillants à l'œuvre sur le site **84.38.130.62** pourraient tenter de vous inciter à effectuer des opérations dangereuses, telles que l'installation d'un logiciel ou la révélation d'informations personnelles (par exemple des mots de passe, des numéros de téléphone ou des numéros de carte de paiement).

Envoyer automatiquement [des informations système et du contenu de page](#) à Google afin de faciliter la détection d'applications et de sites dangereux. [Règles de confidentialité](#)

DÉTAILS Retour à la sécurité

depliant_texte_17-....doc ^ 2017-03.pdf ^ releve_815-30046-....pdf ^ 2017-04.pdf ^ releve_815-30046-....pdf ^ Tout afficher X

18:21 2017-05-19



Protection contre l'hameçonnage – Exemple 1

Message de Chrome lors du clic sur le lien

W Catégorie:Sigle de 3 cara x Messagerie - michel_gag x 84.38.130.62 x 84.38.130.62 x

Dangereux | 84.38.130.62/applications/

Applications Vins CIMBCC ~ Agora cPanel Wiki C... test1 ~ + Pocket LP La Presse Météo OLF TSX IMDB IMDB W an W fr W ATH Autres favoris



Ce site est inaccessible

La connexion a été réinitialisée.

Essayez les suggestions ci-dessous :

- Vérifier la connexion
- [Vérifier le proxy et le pare-feu](#)

ERR_CONNECTION_RESET

depliant_texte_17-....doc ^ 2017-03.pdf ^ releve_815-30046-....pdf ^ 2017-04.pdf ^ releve_815-30046-....pdf ^ Tout afficher X



Chrome Partie 2

Protection contre l'hameçonnage Exemple de courriel – mauvais français

Objet : Formulaire de remboursement .

Canada Revenue Agency

Formulaire de remboursement

Après le dernier calcul annuel de l'exercice de votre activité, nous avons déterminé que vous êtes admissible à recevoir un remboursement d'impôt **189.82**.

S'il vous plaît soumettre le remboursement d'impôt et nous permettre de 3-9 jours pour le processus.

Un remboursement peut être retardé pour diverses raisons. Par exemple la soumission des dossiers non valides ou inscrivez après la date limite.

Pour accéder au formulaire pour votre remboursement d'impôt, s'il vous plaît **cliquez ici**>> [Le LIEN au site Web frauduleux a été désactivé.]

Copyright Agence du revenu du Canada. Tous droits réservés. www.cra-arc.gc.ca



Protection contre l'hameçonnage

Exemple de courriel – Scénario ridicule

ATTENTION MY DEAR BENEFICIARY!!! Spam x

PRESIDENT DONALD TRUMP <"www."@adagio.ocn.ne.jp> 18 août (Il y a 7 jours) ☆

Pourquoi ce message apparaît-il dans le dossier Spam ? Il est similaire aux messages qui ont été détectés par nos filtres anti-spam. [En savoir plus](#)

ATTENTION MY DEAR BENEFICIARY!!!

ASSIGNED BY THE PRESIDENT DONALD TRUMP..... OVERDUE FUND RELEASED TODAY

I am MR,PRESIDENT DONALD TRUMP and I am writing to inform you about your Bank Check Draft brought back by the United Embassy from the government of Benin Republic in the white house Washington DC been mandated to be deliver to your home address once you reconfirm it with the one we have here with us to avoid wrong delivery of your check draft Eighteen million united states dollars \$18,000,000,00usd that was assigned to be delivered to your home address by Honorable president Donald Trump the president of this great country this week by a delivery agent MR ROCHAS JESUS Also reconfirm your details for the check delivery by filling the form below and send it immediately to our Email.donaldjtrump112@gmail.com in for verification and for prompt collection of your fund.text me with this number [353-0484](tel:353-0484)

Fill The Form Below:

1. Full Names :
2. Residential Address :
3. Mobile Number:
4. Fax Number :
6. Sex :
7. Age :
8. Nationality :
9. Country :
10. Marital Status :

Accept my hearty congratulation again!

Yours faithfully,
MR DONALD JOHN TRUMP
president USA
1600 Pennsylvania Ave NW, Washington, DC 20500, United State



Chrome - 2ième Partie

Les Extensions



Qu'est-ce qu'une extension?

- Une extension est une application qui modifie, améliore ou ajoute des fonctionnalités à un navigateur Web qui supporte le concept d'extension.
 - Les extensions permettent par exemple de bloquer la publicité des sites Web, d'afficher la météo, etc.
 - Une fois installées, les extensions se mettent à jour automatiquement et de façon transparente. Il n'est pas nécessaire de redémarrer le navigateur après l'installation ou la mise à jour d'une extension.
- **Les extensions sont gratuites sur Chrome.**
- Ces extensions sont publiées et disponibles à travers le **Chrome Web Store**.
- Le **Chrome Web Store** est le magasin virtuel de Google pour Chrome où on peut trouver:
 - toutes les extensions,
 - les thèmes permettant de personnaliser votre environnement Chrome,
- Visiter le **Chrome Web Store** pour découvrir ce qui vous est offert.

[Retour à l'exercice 1](#)



Chrome - 2ième Partie

Les Témoins (cookies)



Les témoins (cookies)

- **Qu'est-ce qu'un témoin?**
 - Le témoin est un fichier constitué de quelques caractères d'information qu'un site Web utilise pour communiquer avec l'ordinateur des gens qui le visitent.
 - Les témoins sont utiles, et dans certains cas, essentiels au bon fonctionnement des sites Web que vous visitez (ex.: sites d'achat en ligne).
 - Certains sites vont même exiger que vous acceptiez leurs témoins avant d'afficher leur page d'accueil.
 - Les témoins ne sont pas des virus ni des espions et ils ne sont pas dangereux.
- **À quoi servent les témoins?**
 - Les témoins sont accessibles et enregistrées par votre navigateur, pour les sites Web que vous consultez, et par les sociétés qui affichent leurs annonces publicitaires sur des sites Web, pour qu'ils puissent reconnaître le navigateur.
 - Les sites Web utilisent les témoins pour:
 - reconnaître votre navigateur comme un ancien visiteur et se souvenir des préférences identifiées lors de consultations précédentes
 - personnaliser le contenu et les publicités qui vous sont présentés
 - adapter la présentation du site Web aux préférences d'affichage de votre appareil (langue utilisée, résolution d'affichage, système d'exploitation utilisé, etc.)
 - mettre en œuvre des mesures de sécurité, par exemple lorsqu'il est demandé de se connecter à nouveau à un site tiers après un certain laps de temps (ex. Facebook)
 - apprendre pour améliorer l'intérêt et la facilité d'utilisation de leur pages Web
 - comptabiliser les activités afin de payer les redevances dues aux différents acteurs impliqués dans la livraison des services et diffusion de publicités.



Les témoins (cookies)

Autres détails à connaître...

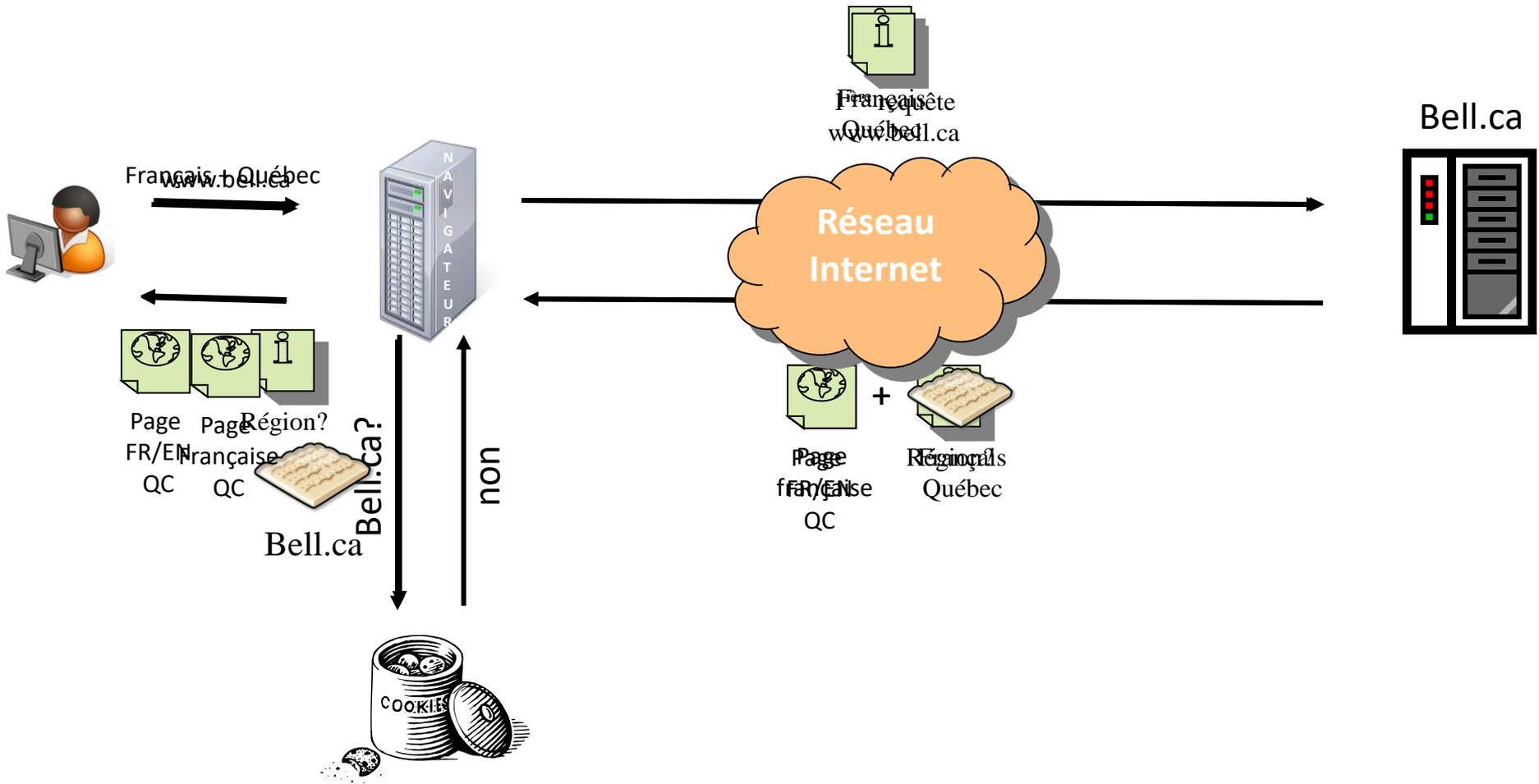
- Un site Web n'écrit jamais directement sur votre ordinateur. C'est votre navigateur qui le fait. Un site ne prend donc jamais le contrôle de votre ordinateur.
- La quantité d'information contenue dans les témoins est minime et ne peut en rien encombrer votre disque dur.
- Un site ne peut lire que les témoins qu'il a lui-même produit et fait enregistrer sur votre ordinateur.
- Les témoins ne peuvent pas endommager vos fichiers ou faire des actions malicieuses comme peuvent le faire des virus.
- La configuration par défaut de Google Chrome est d'accepter et de conserver tous les témoins des sites Web, qu'ils soient propriétaires ou tiers.
- Quand vous effacez les témoins de votre navigateur, vous repartez à zéro votre relation avec les sites Web déjà visités.



Chrome Partie 2

Les témoins – comment ça marche

Première Visite

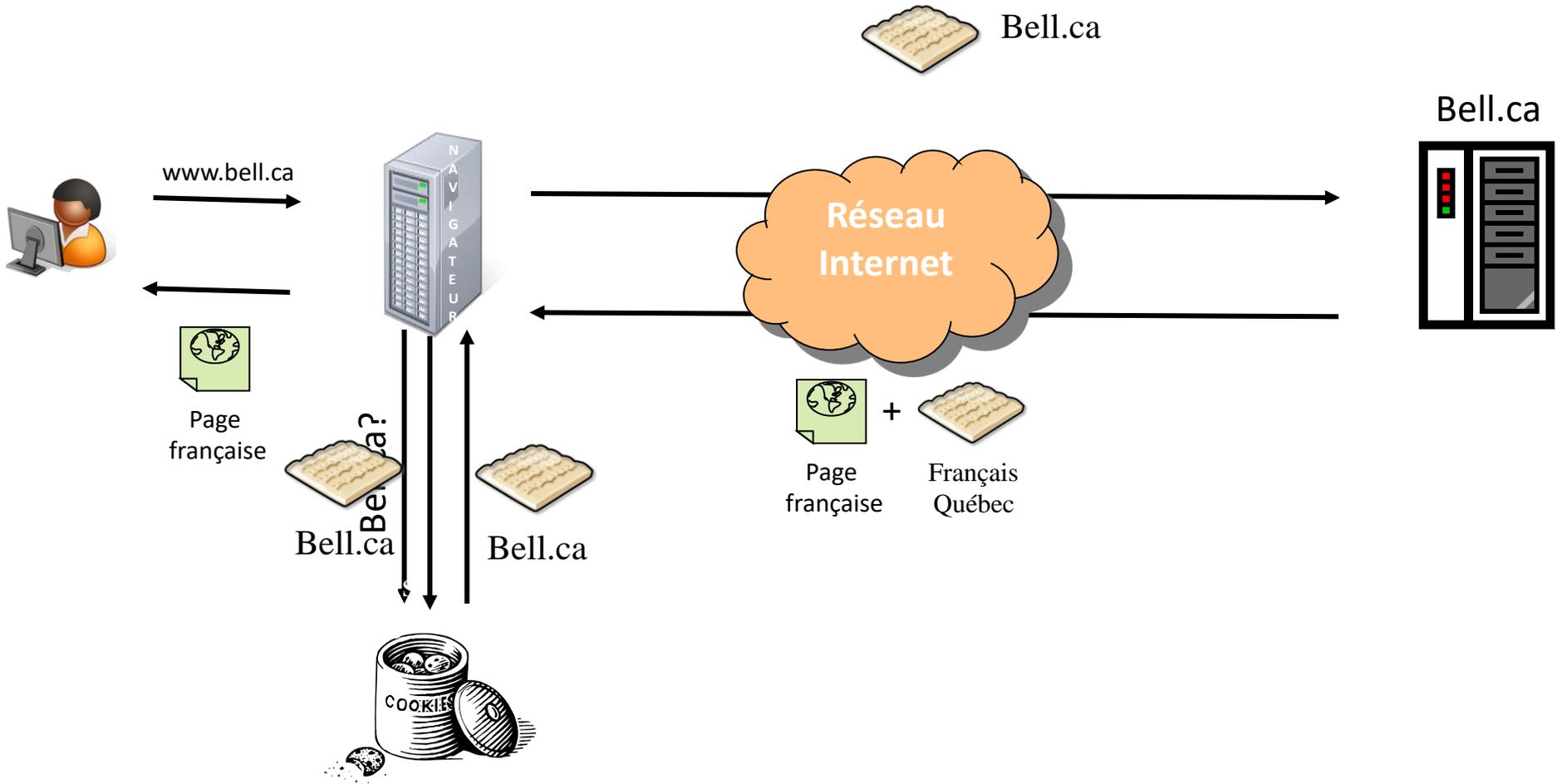




Chrome Partie 2

Les témoins – comment ça marche

Visites Suivantes





D'ici à la prochaine séance de la série Facile...

Afin de profiter au maximum de votre engagement de suivre notre série Facile:

1. S.V.P., refaites les exercices sur votre ordinateur
2. Inscrivez vos questions sur les notes de présentation
3. Venez me rencontrer avec vos questions vendredi prochain, 30 minutes avant le début de la prochaine présentation.



Prochaine séance de la série Facile

Comment se retrouver sur son ordinateur

présentée par Francine Couture, le 28 septembre 2018

Contenu:

Introduction aux notions de base :

- de fichiers et de dossiers
- de l'explorateur de fichiers
- au rangement de l'ordinateur en utilisant:
 - » les différents types de sélection
 - » Le copier-coller
 - » Le couper-coller