



Eviter les pièges d'Internet

Internet offre à chacun de formidables possibilités pour découvrir, apprendre, discuter, échanger, mutualiser... mais comme tout environnement, il présente également quelques dangers. Il est important de faire preuve de prudence et d'adopter quelques bons réflexes pour naviguer sur le web en toute sécurité.

La publicité

Un grand nombre de sites web offrent des encarts publicitaires à diverses sociétés de communication pour amortir les frais d'hébergement et gagner de l'argent.

Le célèbre moteur de recherche Google présente justement un modèle économique entièrement basé sur la publicité. Il propose notamment aux webmasters de payer pour placer leur site dans les premiers résultats d'une recherche sur Google. On parle ici de référencement payant. Ces sites sont identifiables par l'étiquette verte « Annonce » présente devant l'adresse URL.

The screenshot shows a Google search interface. The search bar contains the text 'Gîte en bretagne'. Below the search bar, there are navigation links for 'Tous', 'Maps', 'Images', 'Actualités', 'Shopping', 'Plus', 'Paramètres', and 'Outils'. The search results show approximately 18,800,000 results in 0.72 seconds. Three results are visible, each with a green 'Annonce' label and a URL:

- Gîtes en Bretagne | Location de vacances | leboncoin.fr**
www.leboncoin.fr/
leboncoin : des milliers d'annonces en ligne.
Chambres d'hôtes Bretagne · Logement insolite
- Bretagne · Airbnb - Airbnb.fr**
www.airbnb.fr/
Réservez votre logement sur Airbnb Profitez de nos offres spéciales ! Assistance 24h/24 7j/7.
Inscription 100% Gratuite. Paiement sécurisé. 6 millions de logements. Avis de voyageurs.
Photos des logements. Destinations: Lisbonne, Amsterdam, Londres, New York.
- Gîtes en Bretagne | Meilleur Tarif Garanti | booking.com**
www.booking.com/Bretagne/Gîtes
Réservez un **Gîte en Bretagne**. Sans frais de réservation. Commentaires réels.

Ces résultats, bien qu'en tête de page, ne sont pas nécessairement ceux qui répondront le mieux à votre demande. D'autres sites web laissent également des encarts publicitaires sur leurs pages internes. C'est le cas par exemple du site « telecharger.com » qui vous permet de télécharger des logiciels gratuits.





The screenshot shows the 01net.com website interface. At the top, there is a search bar and navigation links for 'VIDÉOS', 'ACTUALITÉS', 'TESTS', 'ASTUCES', 'TELECHARGER.COM', 'JEUX VIDÉO', and 'BONS PLANS'. Below this, there are icons for various operating systems: WINDOWS, MAC, LINUX, ANDROID, IOS, WINDOWS PHONE, SERVICES EN LIGNE, JEUX, and PRO.

The main content area is titled 'Télécharger Windows > Utilitaires > Nettoyeurs et installateurs' and features 'CCleaner' by Piriform Ltd. The page includes a 'Note' with a 5-star rating and '5404 fois téléchargé les 7 derniers jours'. There are two buttons: 'Télécharger gratuitement' (highlighted with a red arrow labeled '1') and 'Acheter la version complète'. A technical specifications table is also present.

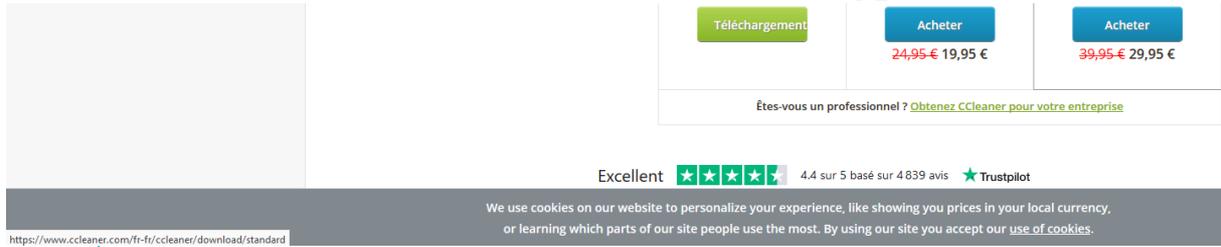
On the right side, there is an advertisement for 'elptoo' with a large blue arrow labeled '2' pointing to a 'CLIQUEZ ICI' button. The ad text includes 'Votre assistant personnel vous aide pour l'installation de CCLEANER' and 'INSTALLATION, CONFIGURATION, PARAMÉTRAGE, ASSISTANCE'. Below the ad, there is a section for 'Inscrivez-vous gratuitement à la Newsletter TELECHARGER' and a 'TOP T... ARGER' button.

Sur cette page figure un encart publicitaire qui peut vous induire en erreur (2). Ce bouton attrayant « Cliquez ici » ne vous permettra pas de télécharger « CCleaner » comme on pourrait le croire au premier regard... mais il téléchargera un autre programme « elptoo » qui s'installera sur votre ordinateur pour vous proposer d'installer dans un second temps « CCleaner ». elptoo est un service payant comme l'indiquent les petites lignes grises situées en-dessous du bouton « Cliquez ici ». Ce clic peut vous coûter cher : au lieu de télécharger un logiciel gratuit, vous vous retrouverez ainsi avec un abonnement de 39€ par mois...

Passez donc votre chemin et cliquez plutôt sur le bouton 1 qui vous guidera vers le site officiel de CCleaner.



Comment vérifier la destination d'un lien hypertexte ?



Au survol d'un lien hypertexte, votre navigateur affichera dans le coin en bas à gauche la destination de celui-ci. Ayez le réflexe d'y jeter un coup d'œil. Si l'adresse URL vous semble suspecte, ne cliquez pas sur le lien !

La sécurité d'un site web

Privilégiez au maximum la consultation des sites officiels : les informations qui s'y trouvent sont régulièrement mises à jour (notamment pour obtenir les dernières versions de logiciels) et la probabilité d'y trouver des virus est faible.

Pour identifier facilement un site officiel d'un logiciel, n'hésitez pas à consulter sa page wikipedia. Vous trouverez sur le côté droit de l'article l'adresse URL ainsi que le nom du développeur.



Site Officiel

Site Frauduleux

Vérifiez également la présence du préfixe **https** dans l'adresse URL. Ce préfixe désormais obligatoire signifie que la connexion est sécurisée et que les données que vous échangez avec le site ne peuvent pas être facilement interceptées.





Le phishing (ou hameçonnage)

Certains criminels informatiques utilisent l'hameçonnage pour voler de l'argent ou des données personnelles qui peuvent être revendues au marché noir.

Pour cela, le criminel envoie à un grand nombre de victimes un mail semblant émaner d'une société digne de confiance. Ce mail est formulé de manière à alarmer le destinataire afin qu'il effectue une action en conséquence. Une approche souvent utilisée est d'indiquer à la victime que son compte a été désactivé à cause d'un problème et que la réactivation ne sera possible qu'en cas d'action de sa part. Le message fournit alors un hyperlien qui dirige l'utilisateur vers une page Web qui ressemble à s'y méprendre au vrai site de la société digne de confiance. Arrivé sur cette page falsifiée, l'utilisateur est invité à saisir des informations confidentielles qui sont alors enregistrées par le criminel.

Ces tentatives de phishing comprennent souvent des fautes d'orthographe. Si vous recevez un de ces mails suspects, jetez-le sans hésitez et n'y répondez pas. Sachez par ailleurs que votre banque ne démarchera jamais par mail : ne renseignez jamais vos coordonnées bancaires à partir d'un mail. Dans le doute, n'hésitez pas à contacter votre conseiller bancaire pour vérifier l'origine du message.

