

1/ trois articles qui parlent de sécurité sur internet avec leur source (nom du site) et le nom de l'article

article 1	Wimi	8 Sites sur la Cybersécurité
article 2	Lemonde Informatique	Cybersécurité et IA générative
article 3	zataz.com	Jeu concours sur Internet: Attention danger

Introduction à la sécurité sur Internet

Trois articles concernant la sécurité sur internet :

- Article 1 Wimi : 8 sites sur la cybersécurité
- Article 2 Le monde informatique : Cyber sécurité et IA générative
- Article 3 zataz.com : Jeu concours sur internet ; attention danger

Créer des mots de passe forts

The first screenshot shows the LastPass website's account creation success page. It features a green banner at the top stating 'Votre compte a été créé avec succès !'. Below this, the text 'FÉLICITATIONS' is followed by a large 'Bienvenue à LastPass !' heading. A message instructs the user to 'Installer l'extension de navigateur, puis connectez-vous avec le compte que vous venez de créer.' The second screenshot shows the LastPass extension interface in a browser. It includes a sidebar with navigation options like 'Tous les éléments', 'Centre de partage', 'Mots de passe', 'Notes', 'Adresses', 'Cartes de paiement', 'Comptes bancaires', 'Tableau de bord de sécurité', 'Accès d'urgence', 'Paramètres du compte', and 'Options avancées'. The main area displays 'Bienvenue dans LastPass, ideally110523' and a message about organizing the vault. A prominent red button says 'Importer beaucoup de mots de passe à la fois vers LastPass', and a white button below it says 'Ajouter des éléments un par un'. On the right, there's a 'Kit de démarrage' section with progress indicators for novice, experienced, and pro users, and a list of tasks like 'Ajoutez votre premier mot de passe', 'Essayez le remplissage automatique', and 'Visitez votre coffre-fort LastPass'.

Fonctionnalité de sécurité de mon navigateur

Identification des adresses internet malveillants

[www.morvel.com](http://www.morvel.com)

[www.fessebook.com](http://www.fessebook.com)

[www.instagram.com](http://www.instagram.com)

Eviter les logiciels malveillants

3/observation de indicateur de sécurité pour les 3 sites web à consulter et leurs noms

<u>Siten°1:</u>	Indicateur de securité:	analyse google
	HTTPS	aucun contenu suspect

<u>Siten°2:</u>	Indicateur de securité:	analyse google
		aucun contenu suspect

Not secure

<u>Siten°3:</u>	Indicateur de securité:	analyse google
		vérifie un URL en particulier

Not secure

Achats en ligne sécurisés

Principes de base de la confidentialité des médias sociaux

Exercice en cas d'atteinte par un anti-virus

Bien sûr, voici un exercice que vous pouvez suivre pour installer et utiliser un antivirus et un anti-malware sur différents types d'appareils.

**Exercice:**

1. **Recherchez un antivirus et un anti-malware appropriés:**
  - Pour un PC Windows, vous pouvez choisir entre des options comme Avast, AVG, ou Bitdefender pour l'antivirus, et Malwarebytes pour l'anti-malware.
  - Pour un Mac, des options comme Norton, McAfee, ou Avast sont disponibles.
  - Pour un appareil Android, vous pouvez choisir entre AVG, Avast, ou Bitdefender.
  - Pour un appareil iOS, des options comme Avira ou McAfee sont disponibles.
2. **Téléchargez le logiciel:**
  - Rendez-vous sur le site officiel du logiciel que vous avez choisi et téléchargez la version appropriée pour votre appareil.
3. **Installez le logiciel:**
  - Ouvrez le fichier téléchargé et suivez les instructions à l'écran pour installer le logiciel.
4. **Configurez le logiciel:**
  - Une fois installé, ouvrez le logiciel et suivez les instructions pour le configurer. Cela peut inclure la définition de vos préférences pour les analyses automatiques.
5. **Effectuez une analyse:**
  - Effectuez une analyse initiale de votre appareil pour vérifier la présence de virus ou de malwares.
6. **Interprétez les résultats:**
  - À la fin de l'analyse, le logiciel vous fournira un rapport. Si des menaces sont détectées, suivez les recommandations du logiciel pour les éliminer.
7. **Planifiez des analyses régulières:**

- Pour maintenir la sécurité de votre appareil, planifiez des analyses régulières. La fréquence dépendra de votre utilisation de l'appareil.
- 8. **Mettez à jour régulièrement le logiciel:**
- Assurez-vous que votre logiciel est toujours à jour pour bénéficier des dernières définitions de virus et de malwares.