

# Votre voix pour remplacer vos mots de passe



## Votre voix pour remplacer vos mots de passe

La Banque Postale est la première institution à avoir obtenu l'autorisation de la Commission nationale informatique et libertés (CNIL) pour tester en France une technologie évaluant la voix de ses clients pour leur permettre de se connecter à leur compte en ligne.

La Banque postale inscrit son innovation dans un nouveau service de paiement en ligne baptisé « Talk to Pay » (littéralement « parler pour payer »). Un dispositif qui se rapproche de l'outil mis en ligne pendant l'été 2016 par MasterCard, qui permet de confirmer un paiement en ligne grâce à la reconnaissance faciale.

[lire la suite]

### Commentaire de Denis JACOPINI :

Un pas de plus vers la biométrie qui, comme les objets connectés, peut nous faire vivre certes dans un monde connecté mais également dans un monde piraté.

Du jour au lendemain nos informations biométriques (empreintes, iris, voix...) peuvent se retrouver piratées et recopiées sans compter que la voix peut changer avec le temps et avec les saisons (rhume, allergie, ).

**Notre métier :** Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Source : *Cybersécurité : les 6 techniques qui pourraient remplacer le mot de passe*

---

# Bordeaux : des drones pour mettre des amendes sur les routes



Comment les drones vont changer nos vies Progressivement, les avions sans pilote se déploient dans de multiples secteurs d'activité, mais le marché, prometteur, peine encore à décoller, freiné par la législation...[Lire la suite ]

---

**Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data

Protection Officer (DPO) dans votre établissement..  
(Autorisation de la Direction du travail de l'Emploi et de la  
Formation Professionnelle n°93 84 03041 84)  
Plus d'informations sur sur cette page.

---



Réagissez à cet article

---

**Un ado attaque sa mère en  
justice parce qu'elle lui  
avait confisqué son  
smartphone**

	<b>Un ado attaque sa mère en justice parce qu'elle lui avait confisqué son smartphone</b>
---	---

---

**Parfois les adolescents ont des réactions bien surprenantes face à certaines situations. En Espagne, un ado de 15 ans a attaqué sa mère en justice pour lui avoir confisqué son smartphone. Une réaction disproportionnée que le juge n'a pas manqué de souligner. Non seulement le jeune homme a perdu son procès, mais il a en plus eu droit à un joli sermon.**

Ah l'adolescence ! Cette période difficile de passage à l'âge adulte laisse place parfois à des réactions bien étonnantes. Néanmoins, certains ados vont tout de même plus loin que d'autres. Et dans le genre relation conflictuelle avec les parents, celui-ci est plutôt bien classée.

En Espagne, à Almeria, **un adolescent de 15 ans a porté plainte contre sa mère** parce que cette dernière lui avait confisqué son smartphone. Oui, c'est assez hallucinant, mais c'est bien vrai. Toute la presse locale en Andalousie en a parlé.

## **Un ado porte plainte contre sa mère qui l'avait privé de son smartphone**

Il s'agit pourtant d'une histoire on ne peut plus banale. L'adolescent à l'origine de la plainte avait des mauvais résultats scolaires depuis quelques temps. Afin de le recadrer, **sa mère lui a confisqué son smartphone**. Une mesure que de nombreux parents peuvent prendre, rien de plus normal.

Mais plutôt que de pester contre sa mère et d'aller bouder à l'arrêt de bus avec ses copains, le jeune garçon de 15 ans a décidé d'aller porter plainte contre sa mère. Face à une demande si surprenante, les policiers ont tenté de raisonner le jeune homme, mais ce dernier a bien validé la plainte pour mauvais traitements.

## **Le juge félicite la mère**

La plainte validée, la mère et l'adolescent sont passés devant le juge Luis Columna. L'histoire ne nous dit pas s'ils y sont partis ensemble en voiture. Toujours est-il qu'après avoir écouté les deux partis, **le juge a non seulement donné raison à la mère, mais il l'a en plus félicitée...**[lire la suite]

---

**Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur  
: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Source : *Insolite : un ado attaque sa mère en justice parce qu'elle lui avait confisqué son smartphone*

---

# Des clés de déchiffrement pour le ransomware Crysis mises en ligne

x	Des clés de déchiffrement pour le ransomware Crysis mises en ligne
---	--

---

**Au total, 200 clés principales ont été publiées sur Internet. Elles permettent à des victimes du ransomware de déchiffrer leurs fichiers et de récupérer ainsi le contrôle de leurs données.**

Le monde a été secoué par WannaCry, un ransomware qui a causé des perturbations et des bouleversements dans d'importants services et des entreprises au cours de la dernière semaine. Mais il y a de bonnes nouvelles pour les victimes d'un autre rançongiciel baptisé Crysis, avec la diffusion auprès du public de 200 clés principales.

Publiées sur le forum BleepingComputer, les clés peuvent être utilisées par les victimes du ransomware, ainsi que par les entreprises de sécurité spécialisée dans la création d'outils de déchiffrement.

Les clés, téléchargées sur Pastebin, sont valides, ont confirmé des chercheurs en sécurité. Les utilisateurs des clés ont également confirmé qu'ils avaient pu recouvrer l'accès à leurs fichiers.

Si vous avez été affecté par cette souche de ransomware, vous pouvez télécharger un outil de déchiffrement fourni par l'éditeur de sécurité ESET...[lire la suite]

---

**Notre métier :** Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur  
: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Source : *Ransomware Crysis : des clés principales mises en ligne – ZDNet*

---

# Chrome Flaw Allows Sites to

# Secretly Record Audio/Video Without Indication

x	<b>Chrome Flaw Allows Sites to Secretly Record Audio/Video Without Indication</b>
---	---

---

**Sounds really scary! Isn't it? But this scenario is not only possible but is hell easy to accomplish. A UX design flaw in the Google's Chrome browser could allow malicious websites to record audio or video without alerting the user or giving any visual indication that the user is being spied on.**

AOL developer Ran Bar-Zik reported the vulnerability to Google on April 10, 2017, but the tech giant declined to consider this vulnerability a valid security issue, which means that there is no official patch on the way.

## **How Browsers Works With Camera & Microphone**



Before jumping onto vulnerability details, you first need to know that web browser based audio-video communication relies on WebRTC (Web Real-Time Communications) protocol – a collection of communications protocols that is being supported by most modern web browsers to enable real-time communication over peer-to-peer connections without the use of plugins. However, to protect unauthorised streaming of audio and video without user's permission, the web browser first request users to explicitly allow websites to use WebRTC and access device camera/microphone.

Once granted, the website will have access to your camera and microphone forever until you manually revoke WebRTC permissions.

In order to prevent 'authorised' websites from secretly recording your audio or video stream, web browsers indicate their users when any audio or video is being recorded.

*« Activating this API will alert the user that the audio or video from one of the devices is being captured, » Bar-Zik wrote on a Medium blog post. « This record indication is the last and the most important line of defense. »*

*In the case of Google Chrome, a red dot icon appears on the tab, alerting users that the audio or video streaming is live.*

## **How Websites Can Secretly Spy On You**



*The researcher discovered that if any authorised website pop-ups a headless window using a JavaScript code, it can start recording audio and video secretly, without the red dot icon, giving no indications in the browser that the streaming is happening...[lire la suite]*

---

**Notre métier :** Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

*Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)*

*Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>*



Réagissez à cet article

**Source : Chrome Flaw Allows Sites to Secretly Record Audio/Video Without Indication**



---

# Des centaines de caméras de vidéo surveillance françaises piratées par... Hitler !



---

**Piratage : Plus de 1500 caméras de vidéo surveillance d'entreprises Françaises infiltrées par un pirate informatique. Il a signé son forfait « Heil Hitler » sur les écrans de contrôle.**

Je vous contais, il y a peu, de la vente d'accès à des caméras de vidéo surveillance. Un grand classique, malheureusement ! Les pirates profitent de la feignantise de certains utilisateurs à lire le mode d'emploi de leur appareil. Des utilisateurs qui ne changent pas le mot de passe usine, ou ne pensent même pas à l'activer. Bilan, l'accès aux images et à la webcam se font en deux clics de souris...[lire la suite sur ZATAZ]


---

**Notre métier :** Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>

---

 Réagissez à cet article

Source : *ZATAZ Vidéo surveillance : des centaines de caméras françaises piratées par... Hitler ! – ZATAZ*

---

# Des banques autorisées par la Cnil à tester la reconnaissance vocale



## Des banques autorisées par la Cnil à tester la reconnaissance vocale

La Cnil indique avoir autorisé neuf établissements bancaires à expérimenter la reconnaissance vocale pour s'authentifier lors d'une connexion à un compte ou pour effectuer certaines transactions.

Lorsque vous vous connectez à votre compte bancaire, vous entrez certainement le numéro de votre compte, un mot de passe et éventuellement d'autres informations, comme votre code postal, pour être redirigé sur votre caisse régionale. Quand vous effectuez un virement bancaire ou un paiement quelconque, peut-être validez-vous la transaction en tapant un code. Ces méthodes d'authentification mises en place pour s'assurer que c'est bien vous qui cherchez à accéder au compte ou qui donnez certains ordres ne sont pas la panacée en matière de sécurité informatique mais elles ont le mérite d'être familières pour le grand public et facilement renouvelables en cas de besoin. Or aujourd'hui, elles sont concurrencées par la biométrie...[lire la suite]

**Notre métier :** Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Source : *Neuf banques autorisées par la Cnil à tester la reconnaissance vocale – Business – Numerama*

---

# 10 règles à respecter pour utiliser un drone en toute sécurité

✕	10 règles à respecter pour utiliser un drone en toute sécurité
---	--

---

1. Ne pas survoler les personnes
2. Respecter les hauteurs maximales de vol
3. Ne pas perdre de vue son drone, ne pas l'utiliser de nuit
4. Ne pas utiliser son drone au-dessus de l'espace public en agglomération
5. Ne pas utiliser son drone à proximité d'un aérodrome
6. Ne pas survoler de sites sensibles ou protégés
7. Respecter la vie privée des autres
8. Ne pas diffuser les prises de vue sans l'accord des personnes concernées et ne pas en faire une utilisation commerciale
9. Vérifier les conditions d'assurance
10. Se renseigner en cas de doute

## **L'utilisation d'une caméra**

Les prises de vue (photos ou vidéos) sont possibles en aéromodélisme dès lors que ces **prises de vue sont réalisées sans usage commercial ou professionnel.**

Le droit à la vie privée des autres personnes doit être respecté. **Les personnes présentes doivent être informées** si l'aéromodèle est équipé d'une caméra ou de tout autre capteur susceptible d'enregistrer des données les concernant.

Par ailleurs, **toute diffusion d'image permettant de reconnaître ou identifier les personnes (visages, plaques d'immatriculation ...)** doit faire l'objet d'une autorisation des personnes concernées ou du propriétaire dans le cas d'un espace privé (maison, jardin etc.) et doit respecter la législation en vigueur (notamment la **loi du 6 janvier 1978 modifiée dite « Informatique et Libertés »**).

La violation de la vie privée est passible d'un an d'emprisonnement et 45 000 euros d'amende...[lire la suite]

---

**Notre métier :** Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur  
: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Source : *Quelle réglementation pour les drones en 2017 ?*

# Lyrebird, une technologie pour faire dire n'importe quoi à n'importe qui

Lyrebird, une technologie pour faire dire n'importe quoi à n'importe qui

« Alors que l'IA commence à comprendre et synthétiser toutes sortes de choses, de la voix humaine au style des grands peintres, nous entrons dans une ère où tout ce qui peut être numérisé peut être imité par une IA », écrivent les chercheurs dans un article publié le 18 mai.

Ils en veulent pour preuve des avancées technologiques comme Lyrebird et Face2Face, qui rendent crédibles la possibilité de fabriquer des images et des sons difficiles à distinguer de la réalité dans un futur proche. « *L'ère post-vérité ne fait que commencer* », prennent-ils le soin de nous avertir.

Sources : DT R&D/Medium

**Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>




Réagissez à cet article

Source : *Cet appareil vous avertit quand une IA tente de se faire passer pour un humain*

---

**Les victimes de Cyberattaque  
sont aussi responsables de  
manquement à leur obligation  
de sécurité**

	<p>Les victimes de Cyberattaque sont aussi responsables de manquement à leur obligation de sécurité</p>
---	---

---

**Demain, les sociétés victimes d'une cyberattaque pourront être plus facilement attaquées en responsabilité par les clients lésés. Ce sera la double peine..**

Difficile d'échapper à la nouvelle, les médias ont largement relayé l'information de la cyberattaque à large échelle perpétrée en fin de semaine dernière. Cette attaque a pris la forme pernicieuse d'un « ransomware », c'est-à-dire d'un cryptage de données couplé à une demande de rançon. Et gare à ceux qui ne voulaient pas obéir, la menace d'une destruction des données concernées était supposée les ramener dans le droit chemin.

Selon les informations disponibles par les médias, l'attaque aurait visé des entreprises qui utilisaient encore l'ancien système d'exploitation Windows XP, un système pour lequel Microsoft avait cessé de proposer des mises à jour depuis peu de temps. Mais comme le fait remarquer l'avocat Adrien Alberini au journal suisse Le Temps, cette situation complexe donne lieu à ce qu'on peut qualifier de « paradoxe de la cyberattaque »: aussi surprenant que cela puisse paraître, les entreprises cibles d'une cyberattaque s'exposeront au final à un risque de sanctions significatives.

Ce paradoxe – la victime doublement victime en quelque sorte – s'explique en réalité par le renforcement du droit de la protection des données. Mais ces nouvelles exigences en matière de protection de données ne seront pas faciles à respecter, d'où le risque d'une attaque en responsabilité pour les entreprises victimes d'une cyberattaque. En bref, peu de chefs d'entreprises le savent, mais une réglementation modernisée en matière de protection des données – dénommée GDPR (General Data Protection Regulation) – entrera en vigueur l'année prochaine en Europe...[lire la suite]

---

**Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Source : *Cyberattaque: le paradoxe de la double peine pour les entreprises – High-tech – Trends-Tendances.be*