

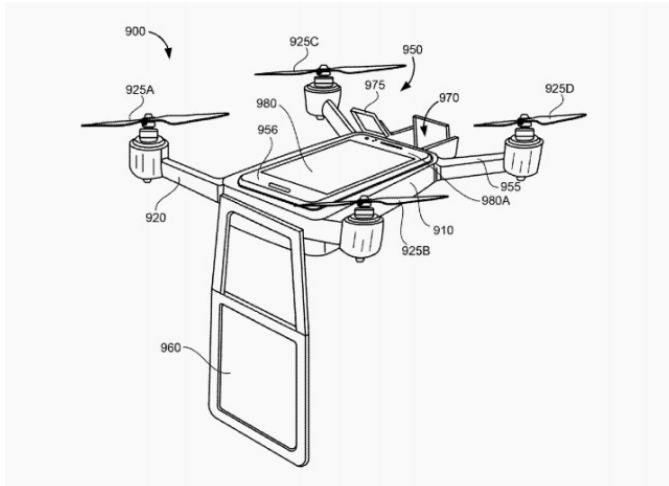
Google imagine un drone de télé-présence



Il y a quelques mois, Google a obtenu un brevet concernant un concept de drone capable de servir de support pour de la télé-présence.

Google a un intérêt marqué pour les drones. En la matière, son projet le plus avancé s'appelle Wing et consiste à mettre au point un système de livraison de colis par les airs. Dévoilé en 2013, il doit faire ses débuts commerciaux l'année prochaine. D'ici là, grâce au feu vert de l'administration de l'aviation civile, Google va pouvoir effectuer des tests sur le territoire américain.

La firme de Mountain View a d'autres idées dans son sac. Il reste néanmoins à leur donner corps. C'est le cas par exemple de ce brevet repéré par Quartz qui décrit le principe d'un drone de type quadricoptère qui embarque plusieurs terminaux et équipements de façon à pouvoir afficher sur un écran l'image d'un interlocuteur situé à un autre endroit. En gros, c'est de la télé-présence déployée sur un drone.



On identifie sans peine l'écran et la tablette sur le drone...[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

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



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Google imagine un drone de télé-présence – Tech – Numerama

Drone piégé utilisé par l'EI contre deux militaires français



Drone
piégé
utilisé
par l'EI
contre
deux
militaires
français

Selon des informations du Monde, deux militaires français qui étaient en opération auprès des Kurdes en Irak ont été rapatriés en France après avoir été grièvement blessé par un drone piégé de l'État islamique.

C'est un mode d'action que les forces de l'ordre redoutent sur le territoire national, et qui semble désormais déployé sur le terrain de l'adversaire. Le Monde affirme ce mardi que deux militaires français ont été gravement blessés par un drone qui avait été piégé par des militants de l'État islamique, en Irak. L'un des deux serait entre la vie et la mort. « Les deux commandos ont été touchés par un drone volant piégé, envoyé par un groupe lié à l'EI, dans des circonstances qui restent à préciser. Les militaires auraient intercepté le drone, avant que celui-ci explose à terre. Ce mode d'action contre des forces françaises est en tout état de cause inédit », rapporte le quotidien, qui précise que ses informations sont confirmées par d'autres médias. Ce piège aurait été tendu aux commandos parachutistes qui intervenaient auprès des forces kurdes à Erbil, dans le nord de l'Irak, entre Mossoul et Kirkouk. La ville est la capitale de la région autonome du Kurdistan.

Le Monde indique que le ministère de la Défense ne souhaite pas confirmer cette attaque d'un nouveau genre et le rapatriement des deux soldats à l'hôpital militaire de Percy-Clamart, non seulement par souci de protéger les familles, mais aussi peut-être en raison des « moyens employés pour cette attaque » (on peut ajouter que de manière plus générale s'agissant des propagandes de guerre, les armées n'aiment jamais communiquer sur leurs propres pertes, préférant mettre en avant leurs réussites pour conserver le moral des troupes et le soutien des populations).

LA CRAINTE D'UN ATTENTAT PAR DRONE

La crainte est sans doute que le mode opératoire, relativement peu coûteux et surtout peu risqué pour les attaquants, ne donne des idées sur le front irakien ou syrien, mais aussi en occident. L'hypothèse qu'une petite bombe puisse être transportée par un drone sans savoir d'où il a décollé et d'où il est contrôlé est soulevée depuis longtemps par les experts de la sécurité aérienne. Elle avait notamment été évoquée en France lors du survol des centrales nucléaires par des drones. Depuis, le législateur s'est emparé du sujet en élaborant une proposition de régulation des drones en cours d'examen, qui prévoit notamment l'obligation d'identifier les drones à distance ou de brider leur utilisation dans certaines zones réglementées. Mais par définition les lois n'ont aucune influence contre ceux qui veulent les violer, et il paraît bien difficile d'empêcher totalement le transport de bombes par drone, sauf à utiliser des moyens technologiques encore balbutiants et impossibles à déployer sur tout le territoire comme des brouilleurs, des lasers, des perturbateurs de signaux GPS, des filets, ou même des aigles.

UNE RÉPONSE ARTISANALE À L'UTILISATION DE « ROBOTS TUEURS » ?

Le fait que les troupes de l'EI utilisent des bombes montées sur des drones n'est aussi, hélas, qu'une réponse attendue à l'utilisation croissante des drones et autres engins militaires conduits à distance par les troupes alliées. En août dernier, l'armée irakienne était fière de présenter un fusil mitrailleur monté sur un véhicule conduit à 1 km de distance, qui permettait d'aller tuer sans risquer de se faire tuer, ce qui est aussi l'objectif des avions de combat semi-autonomes, des navires de guerre ou des nouveaux chars d'assaut. L'utilisation de drones piégés n'est à cet égard qu'une réponse artisanale de même nature.

Il faut ajouter qu'en droit international, l'utilisation de telles armes n'est pas interdite dès lors qu'elles visent à tuer des militaires combattants, et non des civils. La question de la régulation des « robots tueurs » a déjà fait l'objet de débats dans la communauté internationale, dans le cadre de révisions des conventions de Genève, mais les perspectives d'un accord sont excessivement lointaines. La seule piste évoquée, encore très incertaine, est l'obligation qui pourrait être faite qu'un humain reste en permanence aux commandes des engins robotisés, pour ne pas parvenir à des guerres menées par IA interposées.

[Article source]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

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



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contenus, détournements de clientèle...)
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Le Net Expert
INFORMATIQUE
Conseil et Accompagnement en
Protection des Données Personnelles

[Contacter-nous](#)

Réagissez à cet article

Original de l'article mis en page : L'État islamique aurait piégé un drone et blessé grièvement deux militaires français – Politique – Numerama

52 % des DSI Français acceptent moins de sécurité pour plus de mobilité

Denis JACOPINI



DENIS JACOPINI

EXPERT INFORMATIQUE ASSERMENTÉ SPÉCIALISÉ EN CYBERCRIMINALITÉ

vous informe

52 % des DSI
Français
acceptent moins
de sécurité pour
plus de mobilité

C'est une nouvelle à la fois peu surprenante et inquiétante : plus de la moitié des responsables informatiques en France cèdent du terrain sur le plan sécuritaire pour avantager la mobilité et le Bring Your Own Device.

« Rendre les salariés et les opérations plus agiles »

On ne cesse de le répéter depuis des années : le BYOD est loin d'être toujours un choix, il n'est pas rare qu'il s'impose de lui-même. Rejeter cette situation, c'est risquer une utilisation sous-marine, multipliant ainsi les risques. L'accepter, c'est limiter les risques en question en encadrant le BYOD.

Dans une étude menée par le cabinet Vanson Bourne pour le compte de VMware (plus de détails en fin d'article), nous apprenons que 52 % des responsables informatiques français font face à une telle pression vis-à-vis de la mobilité d'entreprise « qu'ils sont prêts à prendre des risques inconsidérés vis-à-vis de la sécurité des données de leur organisation ».

Ces risques sont en grande partie pris pour contenter les cadres dirigeants qui souhaitent absolument accéder aux données pro via leurs propres terminaux, « même si cela va à l'encontre des stratégies de leur entreprise » et que cela multiplie les risques de cyberattaques.

Mais les gains en valent la chandelle puisque les DSI cèdent. 51 % d'entre eux estiment ainsi que les bénéfices sont supérieurs aux risques. « Transformation numérique et mobilité sont indissociables. Les organisations doivent sans cesse chercher à développer leurs activités et à innover. Elles prennent donc des risques à court terme sur le plan de la sécurité afin de rendre les salariés et les opérations plus agiles » explique notamment Sylvain Cazard, directeur général de VMware France.

Pour s'adapter au marché et aux désirs de certains salariés, les DSI n'hésitent donc pas à prendre plus de risques. Il faut dire que près d'un quart des responsables informatiques estiment que le manque de mobilité des salariés réduit leur productivité. Un argument qui fait mouche et pousse logiquement les DSI à lâcher du lest côté sécurité.

Des salariés mal formés, des patrons sous-informés

Bien évidemment, les responsables n'ont pas à laisser la porte ouverte au premier pirate informatique venu. Une plus forte pédagogie auprès des salariés devient ainsi indispensable si l'entreprise ne souhaite pas voir toutes ses données partir dans la nature. Ce point est d'autant plus majeur sachant que l'étude indique que 60% des salariés mobiles précisent ne pas connaître la politique de sécurité de leur entreprise... Une statistique douloureuse et effrayante qu'il convient de ne pas minimiser.

Plus grave encore pour les dirigeants d'entreprises, une ancienne enquête de Vanson Bourne montrait que 25 % des DSI français ont confié ne pas informer leur patron en cas de cyberattaque. Ceci alors même que 29 % des DSI et 21 % des employés estiment que leurs patrons sont responsables en cas de fuite de données. Une incohérence qui en dit long sur la complexité de la problématique...[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

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



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : BYOD : 52 % des DSI
Français acceptent moins de sécurité pour plus de mobilité

Décryptage du règlement européen sur les données personnelles

Denis JACOPINI  vous informe	Décryptage du règlement européen sur les données personnelles
--	--

L'Association Française des Correspondants à la protection des Données Personnelles (AFCDP) a réalisé une version française commentée du règlement européen sur les données personnelles. Elle est disponible gratuitement en ligne

A compter du 25 mai 2018, le nouveau Règlement Européen 2019/679 sur la protection des données personnelles s'appliquera dans toutes les entreprises de l'Union Européenne. Ce texte modifie considérablement la législation en vigueur et fait peser des obligations nouvelles sur les responsables de traitements. L'AFCDP (Association française des correspondants à la protection des données personnelles) a réalisé une version française commentée de ce texte.

Le résultat de ce travail est librement accessible sur le site de l'association. Outre une rapide introduction et un index très complet, bien pratique pour retrouver des thèmes précis, l'essentiel du document est constitué par le texte même du Règlement. Les commentaires apparaissent dans une colonne sur le tiers de la page, en regard de la portion commentée. Si parfois, surtout au début, les commentaires se limitent à quelques mots, à d'autres moments ces commentaires explicitent en profondeur et contextualisent un article du Règlement.

Ne nous cachons pas que la simple mise en page du document en français est des plus agréables pour travailler. Les DSI et les directions juridiques ont en effet fort à faire d'ici 2018 et télécharger dès à présent ce document est donc des plus utiles.

Article original de Bertrand Lemaire



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)



Réagissez à cet article

Le premier label Coffre-Fort Numérique a été délivré



Un coffre-fort numérique est un espace de stockage numérique sécurisé, dont l'accès est limité à son seul utilisateur et aux personnes physiques qu'il a spécialement habilitées à cet effet....[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** sur la mise en conformité CNIL, des formations sur la protection des données Personnelles et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **obligations et moyens de se mettre en conformité avec le RGPD, futur règlement européen relatif à la Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Plus d'informations sur notre page formations.



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Pourquoi les vols de données sont en forte hausse ?



Pourquoi les vols de données sont en forte hausse ?

Une étude du Ponemon Institute pour Varonis révèle que la plupart des collaborateurs disposent d'accès trop importants, ce qui multiplie les dommages lorsque leurs comptes sont compromis

Trois entreprises sur quatre ont été victimes de la perte ou du vol de données importantes au cours des deux dernières années. Selon une nouvelle enquête menée auprès de plus de 3 000 collaborateurs et informaticiens aux États-Unis et en Europe, cela représente une très forte augmentation depuis 2014. Le rapport publié aujourd'hui a été rédigé par le Ponemon Institute et sponsorisé par Varonis Systems, Inc., principal fournisseur de solutions logicielles permettant de protéger les données contre les menaces internes et les cyberattaques.

Selon l'enquête, l'augmentation de la perte et du vol des données est en grande partie due aux compromissions de comptes internes. Celles-ci sont aggravées par des accès aux informations critiques bien plus permissifs que nécessaire par les collaborateurs et les tiers. Sans oublier le constant défaut de supervision des accès et de l'activité dans les systèmes de messagerie et les systèmes de fichiers, là où se trouvent les données les plus sensibles et les plus confidentielles.

Parmi les principales conclusions :

- 76 % des informaticiens indiquent que leur entreprise a fait l'expérience de la perte ou du vol de ses données au cours des deux dernières années. Ce chiffre représente une augmentation importante par rapport aux 67 % d'informaticiens interrogés ayant donné la même réponse lors de l'étude de 2014 réalisée par Ponemon pour le compte de Varonis.
- Les informaticiens indiquent que la négligence des collaborateurs a deux fois plus de chances d'entraîner la compromission des comptes internes que tout autre facteur, y compris les attaquants externes ainsi que les collaborateurs ou les prestataires malveillants.
- 78 % des informaticiens déclarent être très préoccupés par les ransomware, un type de logiciels malveillants qui bloque l'accès aux fichiers jusqu'au paiement d'une somme d'argent. 15 % des entreprises ont déjà fait l'expérience des ransomware et seule une petite moitié d'entre elles a détecté l'attaque au cours des 24 premières heures.
- 88 % des utilisateurs finaux indiquent que leur travail exige l'accès et l'emploi d'informations propriétaires telles que des données relatives aux clients, des listes de contacts, des renseignements sur les collaborateurs, des rapports financiers, des documents commerciaux confidentiels ou d'autres actifs informationnels critiques. C'est nettement plus que les 76 % enregistrés dans l'étude de 2014.
- **62 % des utilisateurs finaux indiquent avoir accès à des données de l'entreprise qu'ils ne devraient probablement pas pouvoir consulter.**
- Seuls 29 % des informaticiens interrogés indiquent que leur entreprise applique un modèle strict de moindre privilège pour s'assurer que les collaborateurs ont accès aux données de l'entreprise en fonction de leur besoin de les connaître.
- Seulement 25 % des entreprises supervisent toute l'activité relative à la messagerie et aux fichiers, alors que 38 % ne supervisent aucune activité.
- 35 % des entreprises ne disposent d'aucun enregistrement interrogeable de l'activité du système de fichiers, ce qui les rend incapables de déterminer les fichiers chiffrés par ransomware (entre autres choses).

Le rapport d'étude intitulé « *Closing Security Gaps to Protect Corporate Data: A Study of U.S. and European Organizations* » se fonde sur des entretiens menés en avril et mai 2016 auprès de 3 027 employés aux États-Unis, au Royaume-Uni, en France et en Allemagne. L'ensemble des personnes interrogées comprend 1 371 utilisateurs finaux ainsi que 1 656 informaticiens et professionnels de la sécurité informatique issus d'entreprises de tailles variant de quelques douzaines à plusieurs dizaines de milliers d'employés. Ils proviennent de divers secteurs, dont les services financiers, le secteur public, le secteur des soins de santé et des sciences de la vie, la vente au détail, le secteur industriel, le secteur technologique et l'industrie du logiciel...[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

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



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Régissez à cet article

Original de l'article mis en page : Vols de données en forte hausse, cause principale: les menaces internes | Docaufutur

Les 15 mesures clés de la loi Numérique



Les 15
mesures
clés de
la loi
Numérique

Vous n'avez guère suivi les débats autour du projet de loi Numérique, qui vient tout juste d'être définitivement adopté par le Parlement ? Voici un panorama de quinze mesures emblématiques. Élan en faveur de l'Open Data...[Lire la suite]

Denis JACOPINI anime des **conférences**, des **formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages...)** pour mieux **s'en protéger** (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.



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Enfin un outil pour savoir si votre webcam n'est pas piratée



Enfin
un
outil
pour
savoir
si
votre
webcam
n'est
pas
piratée

L'outil, Oversight, alerte les utilisateurs d'un Mac d'une tentative de contrôle à distance de leur webcam, lors d'une session vidéo légitime.

Masquer la webcam de son ordinateur est une méthode low-tech contre les techniques d'espionnage consistant à activer à distance la caméra d'un ordinateur. Une méthode très utilisée, le directeur du FBI et le président de Facebook peuvent en témoigner... Dévoilé cette semaine, lors de la conférence Virus Bulletin de Denver, l'outil Oversight, conçu par Patrick Wardle, directeur de recherche de Synack et ancien employé de la NASA et de la NSA américaine, vise à déjouer le piratage potentiel des webcams sous OS X par un malware.

Oversight plus fort que le LED ?

Ce type de programme malveillant peut surveiller discrètement le système et repérer les sessions vidéo initiées par l'utilisateur du Mac, selon Wardle. Par exemple, lors d'une communication utilisant FaceTime ou Skype. Le malware peut alors enregistrer les sessions vidéo et audio, sans être repéré. Car l'indicateur LED de l'appareil est déjà allumé pour signaler que la webcam est active...

Oversight notifie l'utilisateur lorsqu'une application tente d'accéder à la webcam et au microphone intégré. C'est à l'utilisateur de décider de maintenir le flux vidéo, ou de le bloquer. Si un malware présent dans le système est conçu pour agir lorsque la webcam et le micro sont activés par l'utilisateur, Oversight est censé lancer deux notifications : l'une lorsque des applications légitimes de communication se lancent, l'autre lorsque le logiciel malveillant est activé...[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

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



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

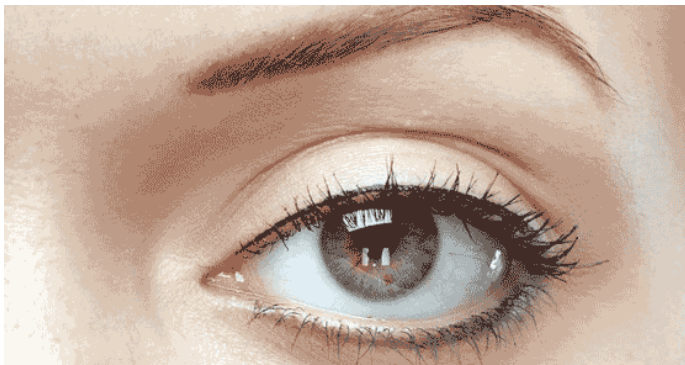


[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Un outil pour vérifier que votre webcam n'est pas détournée

Arte utilise l'Intelligence Artificielle pour répondre aux téléspectateurs



Arte
utilise l'Intelligence
Artificielle pour
répondre aux
téléspectateurs

La chaîne de télévision franco-allemande ARTE souhaite déployer un « Bot apprenant » pour répondre aux questions courantes de ses téléspectateurs.

Bot – Dans le prolongement du hackathon en ligne, proposé en juin dernier et conjointement avec Microsoft, ARTE a lancé, avec l'équipe gagnante, le développement d'un « Bot apprenant » capable de répondre rapidement et avec pertinence aux questions les plus courantes de ses téléspectateurs. Ce nouvel outil conversationnel devra permettre à ARTE d'instaurer un nouveau type de relation avec son public, fondé sur la permanence et l'ubiquité de ses services. Porté par les solutions d'Intelligence Artificielle de Microsoft, ce nouveau Bot va, à termes, simplifier l'accès aux programmes de la chaîne, enrichir l'expérience des téléspectateurs et favoriser les échanges...[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

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



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)



Réagissez à cet article

Original de l'article mis en page : Bot : L'Intelligence Artificielle au service de la relation avec les téléspectateurs d'Arte – Data Security BreachData Security Breach

Quelles failles pour les voitures connectées ?



Quelles
failles
pour les
voitures
connectées

L'édition du salon de l'auto interpelle le grand public sur les nouveaux pirates de la route. Voitures connectées : les cybercriminels dans l'angle mort ?

Nul doute, la voiture connectée est encore l'une des stars du salon de l'auto cette année. Comme tout ce qui attire à internet et aux objets connectés, il est légitime de se poser quelques questions notamment sur la sécurité liée au partage des données ainsi qu'à cette forme de déplacement autonome. Un véhicule connecté est en effet doté d'un accès à Internet ainsi que, plus généralement, d'un réseau local sans fil. L'accès Web offre divers services supplémentaires tels que la notification automatique des embouteillages, la réservation de parking, la surveillance du style de conduite (pouvant par ailleurs avoir une incidence sur le montant des primes d'assurance automobiles) etc.

De multiples raisons peuvent motiver les cybercriminels à tenter de pirater des voitures connectées :
L'appât du gain : il s'agit de bloquer l'accès au véhicule jusqu'à ce la victime paie une rançon.
L'espionnage : l'activation du micro ou de la caméra équipant le véhicule peut donner accès à des informations exclusives et des données sensibles.

La violence physique : les attaques peuvent avoir pour but de blesser le conducteur, ses passagers, ou encore d'endommager d'autres véhicules sur la route.

C'est en analysant ses raisons que la société russe développe une approche de la sécurité interne des véhicules connectés. Elle repose sur deux principes : D'abord l'isolement veille à ce que deux entités indépendantes (applications, pilotes, machines virtuelles) ne puissent interférer l'une avec l'autre en aucune façon. Ensuite, le contrôle des communications signifie que deux entités indépendantes ayant à communiquer dans le système doivent le faire conformément à des règles de sécurité. L'utilisation de techniques de cryptographie et d'authentification pour l'envoi et la réception des données fait également partie intégrante de la protection du système.

Pour respecter notre travail, merci de ne reprendre que l'intro. Pour lire la suite de cet article original direction ->

<http://www.datasecuritybreach.fr/voitures-connectees-cybercriminels-langle-mort/#ixzz4MV1xJas6>

Under Creative Commons License: Attribution Non-Commercial No Derivatives

Follow us: @datasecub on Twitter

...[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

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



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)



Réagissez à cet article

Original de l'article mis en page : Voitures connectées : les cybercriminels dans l'angle mort ? – Data Security Breach