Pourquoi les victime de phishing, se feront encore piéger ?

Pourquoi les victime de phishing, se feront encore piéger ?

Des chercheurs américains ont établi que les internautes se font avoir par des faux e-mails parce qu'ils ont tendance à surestimer leurs capacités à les identifier comme tels.

De : Societe Generale > [mailto:AvisDePaiement@societegenerale.fr]
Envoyé : mercredi 18 mars 2015 12:19
À [redacted]
Objet : Avis de Paiement

SOCIETE GENERALE
Banque & Assurances

ESPACE ENTREPRISES

Bonjour Monsieur / Madame ,

A votre demande, veuillez trouver ci joint le paiement e-conseils pour votre reference.

Se il vous plait, cliquez ici

Cordialement

IMPORTANT : N'UTILISEZ PAS LA FONCTION "repondre a" ,
LAQUELLE NE NOUS PERMET PAS DE TRAITER VOTRE DEMANDE.

Vous pouvez télecharger gratuitement la derniere version du logiciel Acrobat Reader a partir du site d'Adobe a l'adresse suivante :
http://www.adobe.fr/products/acrobat/readstep2.html

Ce message et toutes les pieces jointes (ci-apres le « Message) sont confidentiels et etablis a l'intention exclusive de ses destinataires
utilisation ou diffusion non autorisee est interdite. Si vous avez recu ce Message par erreur, merci de nous en avertir immediatement
declinent toute responsabilite au titre de ce Message s'il a ete altere, deforme, falsifie ou encore edite ou diffuse sans autorisation.

Groupe societe generale

Un e-mail de type phishing prétendant provenir de la Société générale et incitant le destinataire à cliquer sur un lien en lui promettant un paiement.
Le phishing est peut-être une vieille arnaque par e-mail, mais elle marche encore très bien. Pas seulement parce que ces faux e-mails officiels sont de mieux en mieux faits mais aussi parce que les internautes se croient beaucoup plus forts qu'ils ne le sont en réalité pour les détecter… Trois chercheurs américains sont arrivés à cette conclusion après avoir mené une expérience assez pointue auprès de 600 personnes. Le compte rendu a été publié dans Journal of the Association for Information Systems. Et le bilan est sans appel : les internautes se surestiment largement.
L'idée était en effet de voir comment les internautes jugeaient leurs propres compétences à repérer des e-mails frauduleux, plutôt que de voir s'ils étaient capables de déjouer cette arnaque. Pour rappel, les courriers de phishing se présentent comme des courriers officiels de banque, d'assurance, de site d'e-commerce, d'opérateurs de télécommunication, parfois des impôts, avec texte à tonalité toute administrative, mentions légales et logo officiel pour les plus soignés. Ils demandent généralement au destinataire de cliquer sur un fichier attaché (en réalité un virus) ou de mettre à jour ses informations en cliquant sur un lien renvoyant vers un formulaire. L'internaute n'aura plus qu'à remplir. Le plus souvent, il est question de saisir des identifiants et des données bancaires… La force de cette arnaque réside dans le fait que c'est la victime qui a donné elle-même les informations. Il suffit pour cela que le mail soit bien fait, bien rédigé, l'adresse de l'expéditeur assez trompeuse.

Une étude en forme de sondage

Les trois chercheurs américains, issus de l'université du Texas (à Arlington et San Antonio) et de l'université Columbia, ont demandé à six cents participants de se soumettre à un sondage concernant l'examen de seize e-mails (présentés sous forme de fichier image). Tous étaient d'authentiques messages réellement envoyés, mais la moitié était du phishing, l'autre moitié de vrais e-mails d'entreprises.
De chaque message, les personnes ont dû dire si elles pensaient qu'il émanait réellement de l'entreprise censée l'avoir envoyé ou s'il était faux. Elles devaient aussi noter leur propre jugement sur une échelle de 50 à 100 : 50, si elles avaient répondu au hasard sur la fiabilité de l'e-mail, 100 si elles étaient parfaitement sûres de leur coup. Les chercheurs ont également demandé aux répondants à quel point ils étaient familiers (de « pas du tout » à « très ») de l'entreprise expéditrice et, à la fin, les participants étaient tenus d'estimer le pourcentage de bonnes réponses qu'ils pensaient avoir fournies.
Les enquêteurs ont également noté le temps mis par chaque participant à répondre à la première question (l'e-mail est-il légitime ou non), et ce pour les seize e-mails. Le tout était agrémenté de questions plus génériques sur la capacité des répondants à distinguer, dans l'absolu, des e-mails légitime d'emails de phishing, sur leurs activités en ligne, leur expérience, en tant que victime, du phishing.

Avoir été victime d'e-mails de phishing n'aide pas plus à les repérer

« *Nous avons comparé chaque jugement des répondants sur la confiance qu'ils avaient dans leurs propres réponses à la justesse effective de la réponse,* explique Jingguo Wang, de l'université du Texas à Arlington. *Nous avons découvert que 80% des participants avaient une confiance moyenne plus élevée que le taux de justesse de leurs réponses.* » Et quand il s'est agi pour les participants d'estimer combien de bonnes réponses ils avaient donné quant à la légitimité ou non des e-mails, les chercheurs se sont aperçus que 45% s'étaient surestimés.
L'enseignement de cette étude ? « *La confiance qu'ont les internautes dans leur propre jugement et dans leur efficacité à détecter du phishing n'est qu'un faible indicateur de ce qu'il en est vraiment, on ne peut pas se fier à cette confiance* » continue Jingguo Wang. Pire: même le fait que des participants aient eux-mêmes été victimes de phishing ne les aide pas à mieux reconnaître ce type d'e-mail. Le meilleur moyen d'apprendre à les détecter reste donc des séances de formation en bonne et due forme, à la fois sur la forme des messages eux-mêmes et sur la surconfiance des internautes, sur les raisons qu'ils ont de s'estimer si habiles à déceler ce genre de mails alors qu'ils ne sont pas tant que ça.
Original de l'article mis en page : Pour détecter du phishing, l'internaute moins fort qu'il ne le croit – Sciencesetavenir.fr

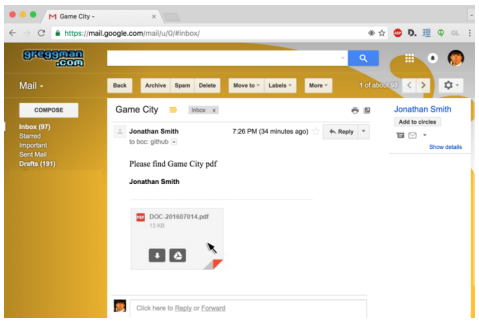
---

Original de l'article mis en page : Pour détecter du phishing, l'internaute moins fort qu'il ne le croit – Sciencesetavenir.fr

Comment se protéger d’une nouvelle arnaque au phishing sur Gmail ?

Comment se protéger d’une nouvelle arnaque au phishing sur Gmail ?

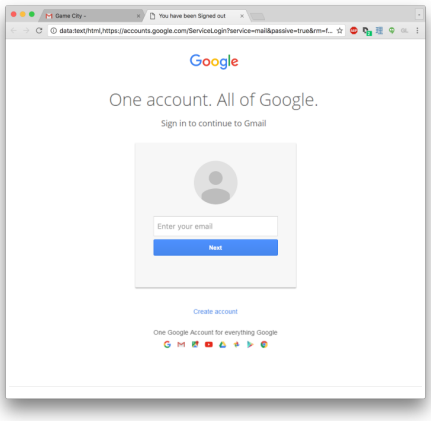
Une arnaque au phishing particulièrement élaborée vise les utilisateurs de la messagerie de Google.



Crédit : Greggman

Ce mail semble contenir une pièce jointe

Une arnaque au phishing au mode opératoire à la sophistication inédite sévit depuis plusieurs semaines sur la messagerie Gmail. L'attaque, qui vise à dérober des informations personnelles afin de les réutiliser à l'insu de l'utilisateur, prend la forme d'un mail envoyé par un contact contaminé. **Il continent une pièce-jointe et un message lapidaire du type « voici le pdf demandé ».** Un clic sur la pièce-jointe renvoie l'utilisateur vers une page à l'apparence de Google Drive et lui demande de s'identifier pour la visualiser. Une fois l'opération effectuée, l'assaillant prend possession du compte de la victime, peut à son tour envoyer le mail de hameçonnage à tous ses contacts et se livrer à des usurpations d'identité ou à des escroqueries.



Crédit : Greggman

Cette page ressemble à la page d'accueil Gmail

Comme l'explique un blogueur américain qui s'est fait piéger par l'arnaque, la pièce-jointe est en fait une image intégrée dans le corps du mail associée à un lien renvoyant automatiquement vers une page web. L'url contient « https://accounts.google.com » et laisse à penser qu'il s'agit du véritable site de Google. Mais elle débute par data « :text/html » et contient un script aspirant l'identifiant et le mot de passe de la victime lorsqu'ils sont renseignés dans le formulaire.

Dans un communiqué, Google dit avoir pris connaissance du problème. « Nous continuons de renforcer nos moyens de défense contre cela. Nous faisons de notre mieux pour protéger nos utilisateurs de différentes manières, en détectant les messages de phishing grâce au deep learning, en adressant des alertes de sécurité lorsque plusieurs liens suspicieux arrivent dans les mails, en repérant des tentatives de connexion douteuses, etc. Les utilisateurs peuvent aussi activer la validation en deux étapes pour ajouter une protection supplémentaire à leur compte », écrit Google dans un communiqué.

Comment fonctionne le phishing

Contraction des mots « fishing » (pêche en français) et « phreaking » (terme désignant le piratage des lignes électroniques) – le phishing est **une technique dite de « hameçonnage » basée sur de faux mails** qui visent à collecter les données bancaires ou les mots de passe des clients. À partir de ces documents, les pirates peuvent ensuite se livrer à des usurpations d'identité et à des escroqueries.

Ces faux courriels se présentent souvent comme des courriers envoyés par une source sûre, comme le Trésor public ou les banques. Trompées par l'expéditeur supposé, les victimes fournissent souvent elles-mêmes leurs propres données personnelles. Une autre possibilité consiste à envoyer des SMS ou des mails malveillants en masse qui contiennent un lien permettant d'installer, sans le savoir, un logiciel pirate qui pourra récupérer les données personnelles des personnes ainsi trompées.

Surveiller les mails et leur orthographe

Il s'agit donc de surveiller les mails et leur contenu. Les courriels émanant d'une structure officielle (la banque, EDF, ou la caisse d'allocations familiales par exemple) ne demandent jamais à leurs clients de saisir leurs informations personnelles directement dans un mail mais depuis un site Internet crypté. Dans ce cas, **un petit cadenas apparaît systématiquement à gauche de l'URL** du site pour garantir la confidentialité des informations.

Par ailleurs, en cas d'information importante, une banque ou un opérateur contactent généralement leurs clients par courrier ou par téléphone. Les mails utilisés dans le cadre des tentatives d'escroqueries font souvent état de **situations alarmistes** et comportent des **fautes d'orthographes** ou de syntaxe laissant penser que le message a été rédigé par un logiciel de traduction automatique.

Vérifier les adresses électroniques et les URL des sites internet

Dans certains cas de phishing, les victimes sont redirigées vers un faux-site, qui ressemble comme deux gouttes d'eau au site officiel. Il faut alors vérifier que l'URL est bien la même que celle du site copié. En général, elle est beaucoup plus longue et compliquée et on peut remarquer que, dans le corps du mail, le texte affiché sous forme de lien ne correspond pas du tout au lien réel, dont l'adresse s'affiche lorsqu'on positionne le curseur dessus. Dans le cas de l'arnaque aux faux mails de la Cpam, on peut s'apercevoir que l'adresse de réclamation ne correspond pas à celle d'un organisme officiel puisqu'elle se termine en « gmail.com ».

Original de l'article mis en page : Une nouvelle arnaque au phishing sur Gmail, comment s'en protéger

---

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 : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Une nouvelle arnaque au phishing sur Gmail, comment s’en protéger

---

Simulation de virus informatique mutant en Polynésie

	Simulation de virus informatique mutant en Polynésie

---

La Polynésie victime d'un virus très agressif … Rien de bien grave puisqu'il s'agit d'un exercice : la simulation d'une cyber attaque.

Cette semaine, à l'appel de l'Agence nationale de sécurité des systèmes informatiques, une cellule de crise a réuni au Haut-Commissariat l'ensemble des acteurs économiques, de l'administration et du secteur privé.
Ainsi, cette semaine, dans la salle de crise située au 3ème étage du bâtiment du Haut-commissariat, les équipes ont simulé un exercice de cyberattaque.

Exercice de cyber-attaque

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 : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Bilan de la simulation d'une cyberattaque au fenua – polynésie 1ère

Le site pirate Films-regarder.co fermé. La SRPJ de Bordeaux à frappé

	Le site pirate Films-regarder.co fermé. La SRPJ de Bordeaux à frappé

Sa mise hors-ligne avait questionné plusieurs internautes sur Twitter depuis quelques heures. L'explication nous est venue de l'ALPA : le site de streaming films-regarder.co a baissé pavillon, suite à l'interpellation de son administrateur.

L'Association pour la lutte contre la piraterie audiovisuelle (ALPA) nous indique en effet que « *les investigations menées par la Direction interrégionale de la police judiciaire de Bordeaux ont abouti à la fermeture du site films-regarder.co* ».

Pour l'ALPA, « bras armé » de l'industrie du cinéma et de l'audiovisuel, ce site créé en 2013 « *dont la popularité n'a cessé d'augmenter proposait l'accès à près de 800 films et 700 séries télé piratés. Les titres étant régulièrement renouvelés en fonction des nouvelles sorties* ».

Il profitait d'une certaine popularité, un million de visiteurs uniques par mois (chiffres Médiamétrie NetRatings) et d'après les calculs de l'association, il « *totalisait 2, 2 millions de visionnages d'œuvres contrefaites dans le même temps* ». Du coup, le préjudice calculé par les ayants droit, selon les nouvelles normes en vigueur depuis notamment la loi sur la contrefaçon, est estimé à 30 millions d'euros.

200 000 euros perçus pendant 18 mois

« *L'administrateur du site a reconnu avoir agi seul et avoir perçu environ 200 000 euros pendant les 18 derniers mois d'activité du site. Les revenus provenaient de régies publicitaires étrangères et étaient versés sur des comptes à l'étranger* ». Il a été présenté au procureur de la République de Toulouse, qui a sollicité l'ouverture d'une information judiciaire. « *L'intéressé a été mis en examen et placé sous contrôle judiciaire* » ajoute l'ALPA dans son communiqué.

Conformément au Code de la propriété intellectuelle, il risque, outre les dommages et intérêts, jusqu'à trois ans de prison et 300 000 euros d'amende.

Libertyland.co, voirfilms.org et voirfilms.co

Soulignons que l'ALPA a également adressé à Google Inc une notification DMCA pour lui demander le déréférencement de Libertyland.co, voirfilms.org et voirfilms.co.

Seulement, suivant à la lettre la demande, l'entreprise américaine s'est contentée de déréférencer uniquement les pages d'accueil de ces sites, non les sous sections qui restent indexées sur les différentes versions du moteur.

Original de l'article mis en page : Films-regarder.co fermé, son administrateur interpellé et mis en examen

---

Réagissez à cet article

Fake Apps Take Advantage of Mario Run Release

Fake Apps Take Advantage of Mario Run Release

Earlier this year, we talked about how cybercriminals took advantage of the popularity of Pokemon Go to launch their own malicious apps. As 2016 comes to a close, we observe the same thing happening to another of Nintendo's game properties: Super Mario.…[Lire la suite]

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.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Le recours au vote électronique facilité

Depuis son introduction en 2004, le recours au vote électronique pour les élections professionnelles n'a cessé de

progresser.

Cette modalité de vote est favorisée tant par la loi, la loi Travail ayant considérablement élargi son utilisation, que par la jurisprudence qui se montre assez souple en la matière.

Elargissement du vote électronique avec la loi Travail

Initialement, la possibilité de recourir à un vote électronique devait être prévue exclusivement par un accord d'entreprise ou de groupe qui comporte un cahier des charges prévoyant les modalités du vote électronique.

La jurisprudence a précisé que l'accord sur le vote électronique est un accord de droit commun, soumis à la majorité de 30 % et au droit d'opposition. Elle a précisé également que cet accord devait faire l'objet d'un dépôt avant la signature du protocole d'accord préélectoral qui prévoit le recours au vote électronique[1].

Cette règle demeure mais depuis le 7 décembre 2016[2], les employeurs d'au moins 11 salariés peuvent, en l'absence d'accord collectif, décider unilatéralement de recourir au vote électronique pour l'élection des délégués du personnel et du comité d'entreprise.

Même si la loi et le décret manquent de clarté sur ce point, il nous semble que l'employeur doit préalablement essayer de négocier un accord avec les syndicats représentatifs avant de mettre en place unilatéralement le vote électronique.

La nouvelle loi précise par ailleurs que la décision de l'employeur de recourir au vote électronique pour les

élections peut s’étendre aux élections partielles. Cette clarification devrait permettre d’éviter un contentieux sur le sujet le moment venu.

L’employeur qui décide de mettre en œuvre unilatéralement le vote électronique reste soumis aux mêmes règles que celles applicables en cas de conclusion d’un accord collectif. Il doit notamment établir un cahier des charges qui respectera les dispositions réglementaires relatives au vote électronique. L’ensemble des prescriptions techniques destinées à préserver la sincérité et la sécurité du scrutin, telles que le chiffrement et le scellement du système ou encore le transfert et le traitement des données, demeurent par conséquent inchangées.

Toutefois, quelques autres règles doivent être adaptées. L’employeur devra ainsi informer toutes les organisations syndicales représentatives dans l’entreprise ou dans les établissements concernés de l’accomplissement des formalités déclaratives préalables auprès de la CNIL.

La loi Travail prévoit enfin que le cahier des charges devra être tenu à la disposition des salariés sur le lieu de travail et mis sur l’intranet, s’il en existe un dans l’entreprise. Cette nouvelle disposition, qui se justifie pleinement en cas de recours unilatéral au vote électronique, est également applicable, compte tenu de la rédaction de la loi, en cas de conclusion d’un accord. Cette nouvelle règle devrait permettre aux salariés de mieux s’approprier le dispositif, ce qui devrait favoriser la participation…[Lire la suite]

A Lire aussi :
Nouveautés dans l’organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L’Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?
La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle
Notre sélection d'articles sur le vote électronique

Vous souhaitez organiser des élections par voie électronique ?
Cliquez ici pour une demande de chiffrage d'Expertise

Vos expertises seront réalisées par **Denis JACOPINI** :

- Expert en Informatique **assermenté et indépendant** ;
- **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;
- ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;
- qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solution de vote électronique ;
- et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.

Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

Fake Apps Take Advantage of Mario Run Release

Fake Apps Take Advantage of Mario Run Release

Earlier this year, we talked about how cybercriminals took advantage of the popularity of Pokemon Go to launch their own malicious apps. As 2016 comes to a close, we observe the same thing happening to another of Nintendo's game properties: Super Mario.…[Lire la suite]

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.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Le recours au vote électronique facilité

Depuis son introduction en 2004, le recours au vote électronique pour les élections professionnelles n'a cessé de

progresser.

Cette modalité de vote est favorisée tant par la loi, la loi Travail ayant considérablement élargi son utilisation, que par la jurisprudence qui se montre assez souple en la matière.

Elargissement du vote électronique avec la loi Travail

Initialement, la possibilité de recourir à un vote électronique devait être prévue exclusivement par un accord d'entreprise ou de groupe qui comporte un cahier des charges prévoyant les modalités du vote électronique.

La jurisprudence a précisé que l'accord sur le vote électronique est un accord de droit commun, soumis à la majorité de 30 % et au droit d'opposition. Elle a précisé également que cet accord devait faire l'objet d'un dépôt avant la signature du protocole d'accord préélectoral qui prévoit le recours au vote électronique[1].

Cette règle demeure mais depuis le 7 décembre 2016[2], les employeurs d'au moins 11 salariés peuvent, en l'absence d'accord collectif, décider unilatéralement de recourir au vote électronique pour l'élection des délégués du personnel et du comité d'entreprise.

Même si la loi et le décret manquent de clarté sur ce point, il nous semble que l'employeur doit préalablement essayer de négocier un accord avec les syndicats représentatifs avant de mettre en place unilatéralement le vote électronique.

La nouvelle loi précise par ailleurs que la décision de l'employeur de recourir au vote électronique pour les

élections peut s’étendre aux élections partielles. Cette clarification devrait permettre d’éviter un contentieux sur le sujet le moment venu.

L’employeur qui décide de mettre en œuvre unilatéralement le vote électronique reste soumis aux mêmes règles que celles applicables en cas de conclusion d’un accord collectif. Il doit notamment établir un cahier des charges qui respectera les dispositions réglementaires relatives au vote électronique. L’ensemble des prescriptions techniques destinées à préserver la sincérité et la sécurité du scrutin, telles que le chiffrement et le scellement du système ou encore le transfert et le traitement des données, demeurent par conséquent inchangées.

Toutefois, quelques autres règles doivent être adaptées. L’employeur devra ainsi informer toutes les organisations syndicales représentatives dans l’entreprise ou dans les établissements concernés de l’accomplissement des formalités déclaratives préalables auprès de la CNIL.

La loi Travail prévoit enfin que le cahier des charges devra être tenu à la disposition des salariés sur le lieu de travail et mis sur l’intranet, s’il en existe un dans l’entreprise. Cette nouvelle disposition, qui se justifie pleinement en cas de recours unilatéral au vote électronique, est également applicable, compte tenu de la rédaction de la loi, en cas de conclusion d’un accord. Cette nouvelle règle devrait permettre aux salariés de mieux s’approprier le dispositif, ce qui devrait favoriser la participation…[Lire la suite]

A Lire aussi :
Nouveautés dans l’organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L’Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?
La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle
Notre sélection d'articles sur le vote électronique

Vous souhaitez organiser des élections par voie électronique ?
Cliquez ici pour une demande de chiffrage d'Expertise

Vos expertises seront réalisées par **Denis JACOPINI** :

- Expert en Informatique **assermenté et indépendant** ;
- **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;
- ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;
- qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solution de vote électronique ;
- et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.

Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

La CIA donne accès à des millions de pages sur son histoire et ses opérations secrètes

La CIA propose un moteur de recherche pour explorer sa base de données, composée de 930 000 documents confidentiels qui ont été déclassifiés. L'agence lève ainsi le voile sur une partie de son histoire, bien souvent méconnue.…[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.

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.

Le Net Expert
INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

L’Anssi épingle le fichier biométrique défendu par Cazeneuve

L’Anssi épingle le fichier biométrique défendu par Cazeneuve

Très décrié depuis sa découverte, le décret instituant le fichier TES (Titres Électroniques Sécurisés) a entraîné un intense débat en France sur l’usage de la biométrie et la protection des données qui y sont attachées.…[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.

Le Net Expert
INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article