La journée du numérique

IMAGINEZ LE FUTUR DE LA PROFESSION

Le mardi 11 décembre 2018

ORDRE DES EXPERTS-COMPTABLES

Digital first et choc numérique :

Comment intégrer la confiance numérique et la cybersécurité comme pivot de votre transformation digitale

A vos marques, prêts, Cybersécurité !

« Si vous pensez que la technologie peut résoudre vos problèmes de sécurité, alors vous ne comprenez ni les problèmes, ni la technologie… »

Bruce Schneir

1. Comprendre pour mieux agir dans le Cyberespace

La journée du numérique

IMAGINEZ LE FUTUR DE LA PROFESSION

Tendances et risques

Les nouveaux risques liés à la mobilité de nos capacités informatiques

Les risques des usages des environnements virtuels

Les risques liés au manque de sensibilisation et veille des collaborateurs et des dirigeants à la cybersécurité

Les risques liés à l'utilisation des réseaux sociaux et des moteurs de recherche

Risques liés à l’utilisation des réseaux sociaux et moteurs de recherche…

Démarche du fraudeur

1

- Choisir la cible : Identifier le périmètre, le contexte et les mécanismes

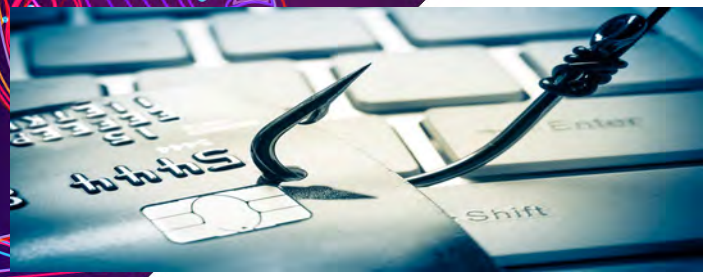
2

- Analyser et comprendre ces mécanismes

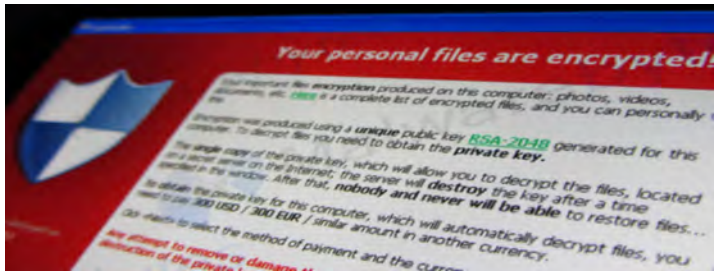
3

- Contourner ces mécanismes

Principaux schémas d’attaques



Hameçonnage
ou *Phishing*



Rançongiciel
ou *ransomware / cryptolocker*

Principaux schémas d’attaques

Fraude au président
ou faux virements (FOVI)

Malware

Les 4 étapes du FOVI

1

L'escroc collecte des informations pour connaître l'entreprise et ses dirigeants (réseaux sociaux, organigramme).

2

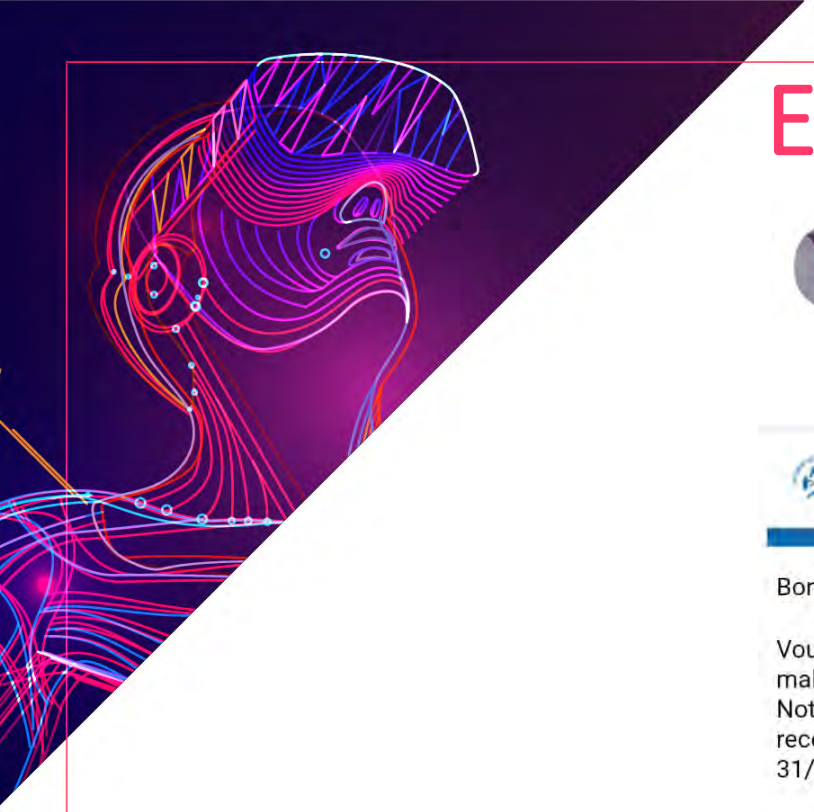
Se faisant passer pour le dirigeant de l'entreprise, l'escroc prétexte une opération financière urgente et confidentielle.

3

Sous la pression ou en confiance, l'entreprise exécute la transaction.

4

L'escroc transfère l'argent vers des comptes basés à l'étranger.



Exemple de Phishing….

Votre Assurance Maladie
laurent@flexr.org

L'Assurance Maladie | Mon compte | mon parcours d'assuré

Bonjour,

Vous avez un remboursement non effectué de la part de votre assurance maladie pour l'exercice 2018
Notre système de gestion des opérations détecte que vous avez le droit à recevoir ce paiement A La cloture de l'exercice 2018 qui aura date le 31/12/2018.

Montant	**287.95 €**
Référence	**Ameli-06885W**

pour accepter le paiement rapide en ligne cliquez sur le lien suivant et enregistrer les informations de remboursement.

https://remboursement.ameli.fr/

Merci de votre confiance,
votre service clients Ameli.fr.

Ameli, SA au capital de 10 640 226 396 euros, 78 rue Olivier de Serres - 75015 paris - 380 129 866 RCS paris.
réf. mail : 16496

Bonne pratiques : Usurpation d'identité

Renforcez les procédures internes et tout particulièrement les procédures de confirmation des banques, modification des RIB fournisseurs et la bonne séparation des fonctions.

Faites un contre-appel vers votre interlocuteur habituel ou un numéro déjà référencé pour vous assurer de l'authenticité des demandes qui vous sont faites.

Ne vous contentez pas des informations affichées sur les emails même si elles semblent être d'apparence officielle. Ne cliquez pas sur les liens, et gardez un esprit critique.

Méfiez-vous des emails ou appels impliquant une totale discrétion et alertez toujours un responsable hiérarchique le cas échéant.

Méfiez-vous des emails ou appels ayant un caractère d'urgence.

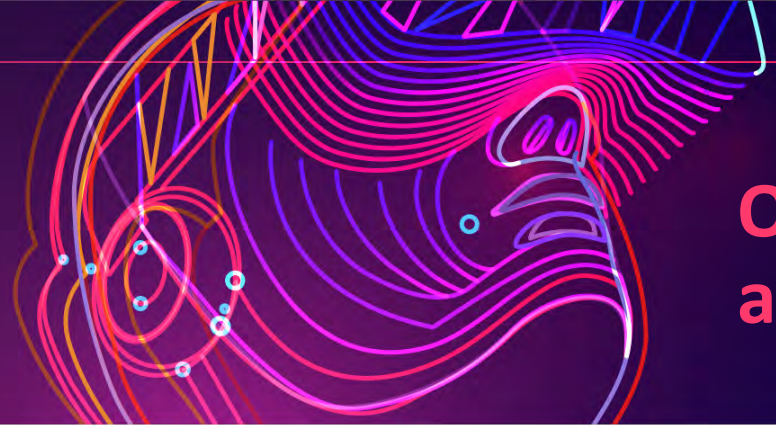
Ça n’arrive pas qu’aux autres !

- Cabinet d’EC et partenaires : cible privilégiée !
  - Par essence une cible du fait des données que l’EC détient :
    - ❑ Données stratégiques, personnelles, R&D de ses clients
    - ❑ RIB clients/fournisseurs/salariés

2. Protection des données et RGPD

Cabinets, où en êtes-vous ?

La journée du numérique
IMAGINEZ LE FUTUR DE LA PROFESSION



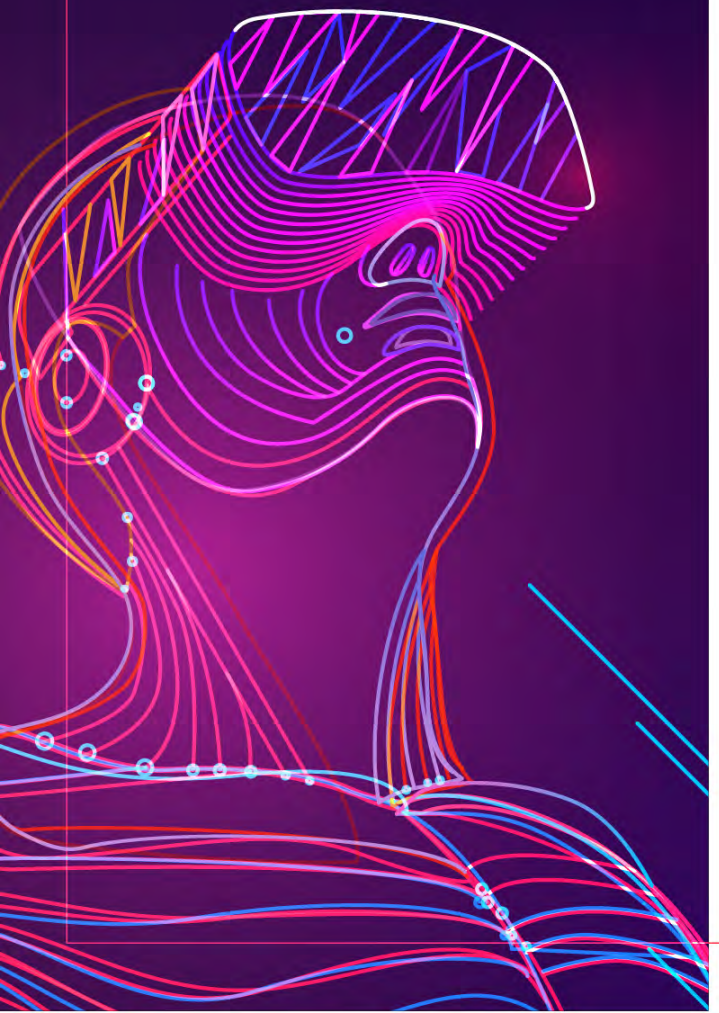
Ou en êtes-vous aujourd'hui ?

- Le RGPD est entré en vigueur le 25 mai dernier
  - Mais des règles de protection des données personnelles s'imposent aux entreprises depuis de nombreuses années … et donc aussi aux experts-comptables !
  - Les experts-comptables doivent depuis longtemps faire des déclarations à la CNIL et respecter les règles de protection des données personnelles dans leur activité quotidienne

- Quelles sont les nouvelles obligations ?
  - Renforcer les droits des personnes physiques dont les données sont traitées
  - Responsabiliser les entreprises

La journée du numérique

IMAGINEZ LE FUTUR DE LA PROFESSION



Nous allons voir si vous avez commencer à réfléchir au sujet

Nous vous proposons de répondre ensemble à quelques questions qui nous ont été posées par des cabinets

- Est-ce que vous faites un traitement de données personnelles lorsque vous vous contentez de consulter un fichier Excel transmis par un client ?
  - Oui ou non ?

- **Oui !**

  - Définition du traitement de données personnelles :
    - **Toute opération** portant sur ces données, quel que soit le procédé utilisé
      - Simple consultation, collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction

  - Attention : le RGPD s'applique au traitement – **automatisé ou non** – des données à caractère personnel
    - Vos dossiers d'archives papier sont donc aussi concernés par le RGPD !

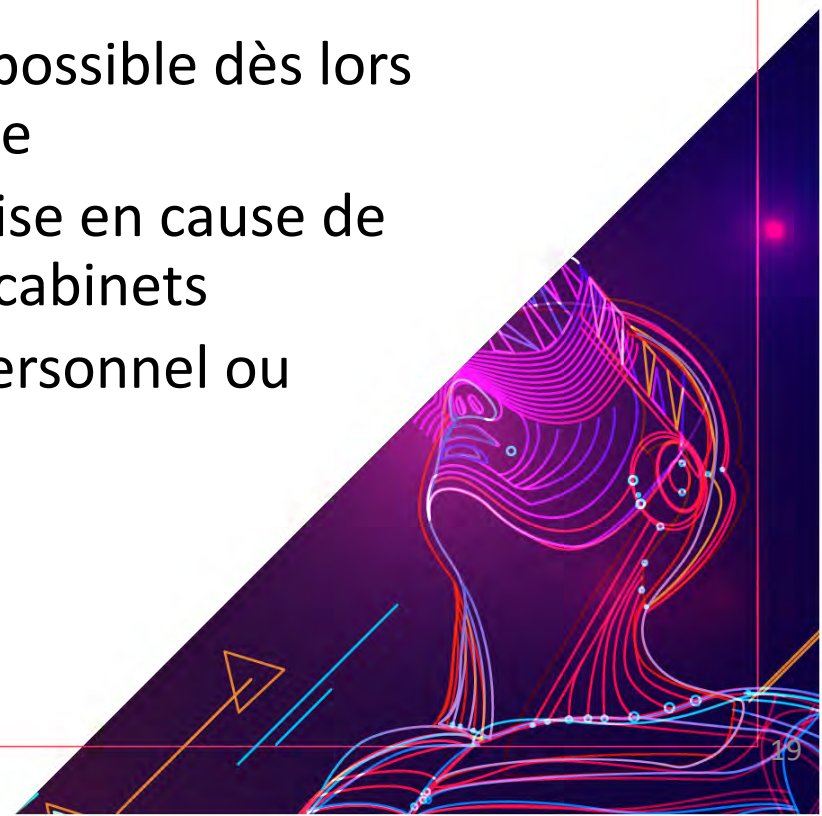
- Votre cabinet doit conserver les documents contenant des données personnelles aussi longtemps que cela peut être utile au client

  - Vrai ou faux ?

- **Faux**

  - **La durée de conservation est fixée en fonction de l'utilité de la donnée au regard du but poursuivi par le traitement**
    - **Principe de minimisation** prévu par le Règlement européen

  - La conservation au-delà de la durée du contrat est possible dès lors qu’elle n’excède pas les durées de la rétention légale
    - Conservation possible pendant la période de mise en cause de la responsabilité civile professionnelle pour les cabinets
    - Suppression ensuite des données à caractère personnel ou anonymisation



- **Exemples de durées de conservation**
  - Données collectées dans cadre de la mission client
    - Gestion des dossiers clients
      - Conservation pendant le temps nécessaire à la gestion de la relation contractuelle.
      - Archives pendant au minimum 8 ans après la fin de mission ou la fin des travaux
    - Gestion des contentieux et réclamations des clients
      - Conservation pendant le temps nécessaire à la gestion du contentieux (délais de recours inclus) après la connaissance d'un litige, jusqu'à la prescription de l'action
  - Données collectées dans cadre de la gestion de votre cabinet
    - Archives des bulletins de paie pendant 5 ans à compter du versement de la paie
    - Pour les CV de candidats non retenus et s'ils n'ont pas demandé la destruction de leur dossier, destruction 2 ans après le dernier contact
    - Gestion courante du personnel du cabinet (annuaire interne, dossiers professionnels, formation continue etc.)
      - Conservation jusqu'au départ du salarié
      - Archives pendant 5 ans après le départ du salarié

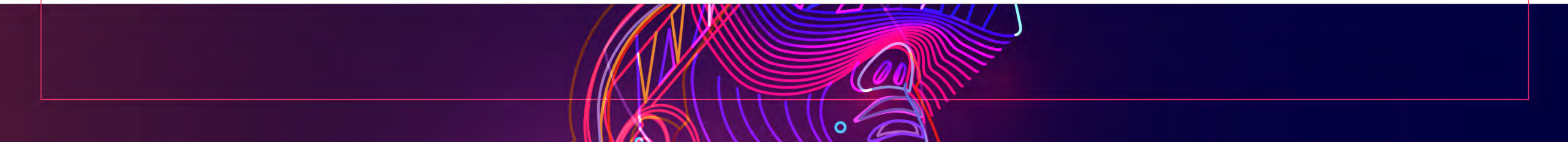
- Votre cabinet doit-il obtenir le consentement préalable des salariés du client pour établir les bulletins de paie ?
  - Oui ou non ?

- Le consentement n’est pas nécessaire car le traitement a un autre fondement que le consentement
  - L’établissement du bulletin de paie résulte d’une obligation légale
  - Le salarié est lié par un contrat de travail avec le client entreprise

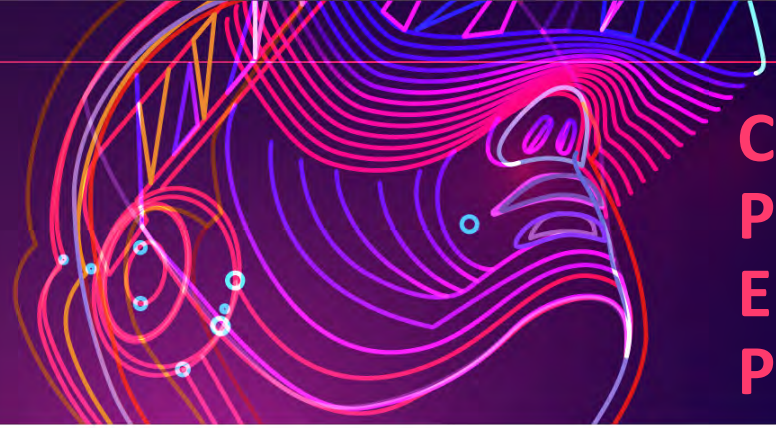
- A noter que le consentement lorsqu’il est la base du traitement doit être recueilli par le responsable de traitement !

- Les points à avoir en tête

- Le consentement n’est pas toujours le fondement du traitement, loin de là !
  - Le traitement de données peut être fondé sur
    - **L’exécution d’un contrat, à la suite de la requête d’une personne physique ou en vue de la conclusion d’un contrat**
    - **Obligation légale du RT**
    - **Intérêt légitime du RT ou d’un tiers supérieur aux intérêts ou libertés et droits fondamentaux de la personne concernée**
    - Pour protéger les intérêts vitaux de la personne concernée ou d’une autre personne
    - Pour une mission d’intérêt public ou officielle du RT
    - Archivage dans l’intérêt public, scientifique, statistique ou historique



La journée du numérique
IMAGINEZ LE FUTUR DE LA PROFESSION



COMMENT METTRE EN PLACE LE REGLEMENT EUROPEEN DES DONNEES PERSONNELLES ?

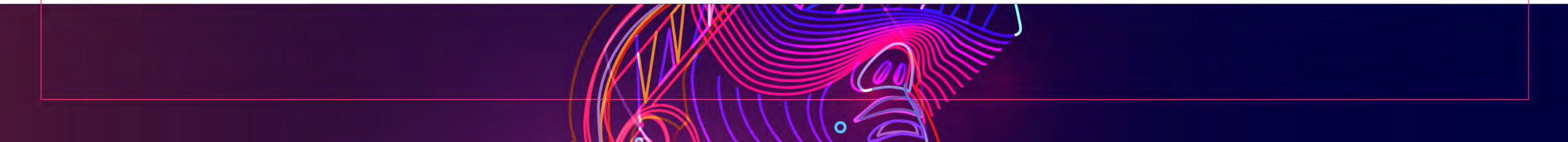
- Il faut procéder par étapes
  - Etape 1
    - Désigner une personne responsable
  - Etape 2
    - Auditer les traitements de données
  - Etape 3
    - Création du registre des traitements
  - Etape 4
    - Réaliser un audit technique et un audit des prestataires
  - Etape 5
    - Arrêter un plan d'action
  - Etape 6
    - Organiser les procédures internes et documenter les actions engagées

La journée du numérique
IMAGINEZ LE FUTUR DE LA PROFESSION

L'établissement de bulletin de paie dans votre registre de traitement

Traitement	Qualité du cabinet	Finalité	Catégories de données personnelles concernées	Destinataires des données	Durée de conservation	Données sensibles	Mesures de sécurité	Mention d'information	Consentement	Transfert des données hors Union Européenne
Etablissement des Bulletins de paie dans cadre mission client	Option: RC ou ST	Gestion du personnel	-Données d'identification -Données économiques et financières	DGFIP Et autres à préciser	Durée à fixer avec le client(= durée de mise en cause de la responsabilité de l'EC)	Option : Oui/Non	Description des mesures techniques/ organisationelles	Non	Non, pas nécessaire de l'obtenir car il s'agit d'une obligation légale	Non Si pas d'hébergement des données dans un cloud dont les serveurs sont situés hors union européenne

- Cette démarche peut être utilisée pour vos cabinets mais aussi pour vos clients !
    - Les règles à mettre en place sont les mêmes dans les cabinets et dans les entreprises clientes
        - Une fois que vous aurez réfléchi en interne sur la mise en place du RGPD, la même démarche est à appliquer dans les entreprises clientes
            - Vous pouvez donc proposer une mission d’accompagnement à la mise en place du RGPD



- Pour vous aider
  - Un guide sur la protection des données personnelles à l'usage des experts-comptables rédigé par le CSO
    - Il comporte de nombreux documents pratiques comme des exemples de questionnaire d'audit des données, d'audit technique, des fiches d'écart pour les audits, de mentions d'information etc.
    - Téléchargeable gratuitement sur Bibliordre

- Un Conseil Sup’ Services dédié au RGPD sur le site du Conseil supérieur – partie privée

  - Fil rouge d’actualité
    - Actualité et veille en la matière
    - Outils et sites
    - FAQ
    - **Questions en ligne**
    - Lien vers le Guide RGPD

3. Quelles bonnes pratiques pour garantir une confiance numérique et se prémunir des cyber-risques ?

L’importance de la sensibilisation : comme 1er rempart

84% des incidents sont liés au facteur humain

La sensibilisation de l’homme doit donc être le pilier incontournable de la cybersécurité

Sensibiliser et alerter : ici

10 commandements tu respecteras

1. La confidentialité du garantiras
2. Un contrat de cyber-assurance tu souscriras
3. Une perte ou un vol tu anticiperas
4. De boucliers tu te muniras
5. Aux cyberattaques tu réagiras
6. Le RGPD tu respecteras
7. Des clés USB (et tous supports physiques externes) tu te méfieras
8. De bonnes pratiques managériales tu adopteras
9. Les usages tu règlementeras
10. Les collaborateurs tu sensibiliseras

EN SAVOIR PLUS

Retrouvez ces dix fiches pratiques en téléchargement sur Bibliordre.fr, la plateforme de téléchargement du Conseil supérieur.

Guide de la cybersécurité pour les experts-comptables :

Objectifs :

- Sensibiliser et alerter les cabinets : tendances et risques, principaux schémas d'attaques, modes opératoires ;
- Proposer des voies d'amélioration et des bonnes pratiques en la matière.
- Présenter les enjeux et opportunités pour le professionnel du chiffre qui peut valoriser sa mission auprès de ses clients et développer des compétences dans la prévention des cyber-risques.

http://www.bibliordre.fr/67congres/medias/publications/files/all/1538380412cybersecurite_experts_comptables.pdf

Webinaire Cyber : Comment se prémunir des cybermenaces et devenir force de proposition pour vos clients ?

À VOUS COGNACQ-JAY
le rendez-vous des experts

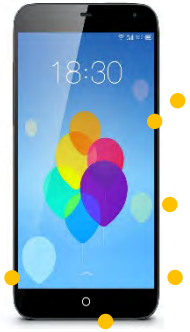
- Objectifs :
  - Sensibiliser et alerter les cabinets : tendances et risques, principaux schémas d'attaques, modes opératoires ;
  - Proposer des voies d'amélioration et des bonnes pratiques en la matière.
  - Présenter les enjeux et opportunités pour le professionnel du chiffre qui peut valoriser sa mission auprès de ses clients et développer des compétences dans la prévention des cyber-risques

https://avouscognacqjay.com/

Et pour aller plus loin : le guide de la survie numérique

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

InternetSansCrainte.fr



ANSSI
Agence nationale de la sécurité des systèmes d'information

CNIL
Commission Nationale de l'Informatique et des Libertés

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

SecNumacadémie.gouv.fr
Formez-vous à la sécurité du numérique

NO MORE RANSOM!
www.nomoreransom.org

Questions - Réponses

Pour conclure…

« Un ordinateur en sécurité est un ordinateur éteint. Et encore… »

Bill Gates

#Capsurlenumerique #Cybersécurité #Conduiteduchangement

Merci de votre participation

La journée du numérique

IMAGINEZ LE FUTUR DE LA PROFESSION

ORDRE DES EXPERTS-COMPTABLES