



**Avantde  
Cliquer**.com

**L'humain au cœur  
de la cybersécurité**

Assistanat

Services Web

Communication

**LC INFOSERV'**

*Au service des entreprises*

**Un programme innovant de sensibilisation **AUTOMATIQUE** créé  
**SUR MESURE** pour développer des réflexes de cybersécurité !**

# Le contexte

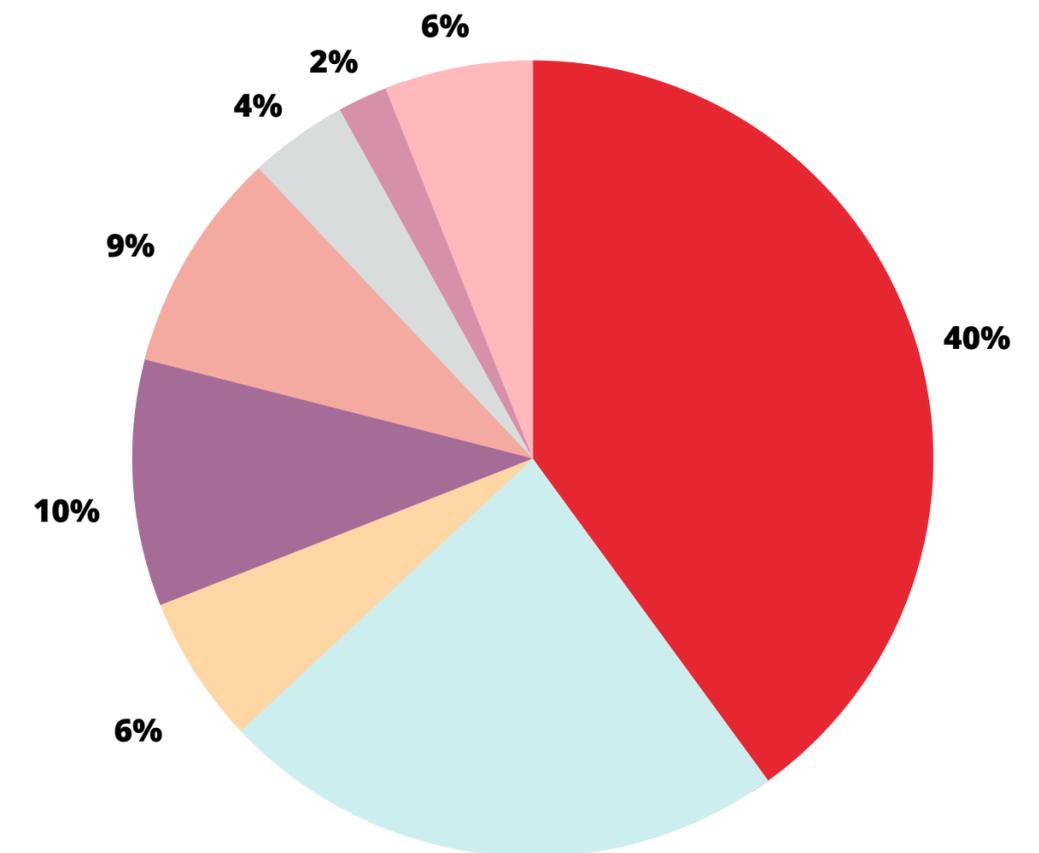
La situation actuelle démontre l'importance des bonnes pratiques à adopter face aux e-mails entrants.

D'après l'ANSSI, c'est 831 intrusions avérées et 40 % des rançongiciels traités ou rapportés à l'ANSSI en 2022 concernent les entreprises, 23% pour les collectivités. Cette tendance est toujours à la hausse.

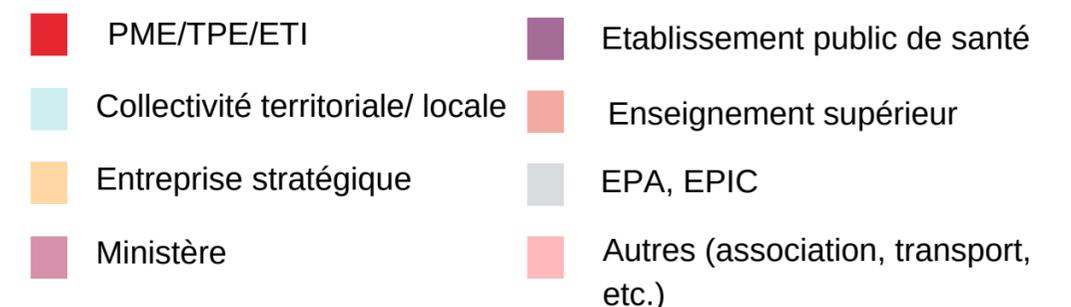
Une attaque provenant d'un e-mail de phishing avec demande de rançon se produit toutes les 10 secondes. La France est désormais le 2ème pays européen le plus touché.

## Pertes considérables :

- ▶▶ L'arrêt de la production pour certains services
- ▶▶ La paralysie totale ou partielle du système
- ▶▶ Le temps perdu par les administrés à recourir au papier/crayon
- ▶▶ L'image de marque
- ▶▶ La perte et parfois la diffusion de données confidentielles
- ▶▶ L'amende de la CNIL en cas de non-respect de la RGPD
- ▶▶ La rançon réclamée par les hackers et le coût de la remise en service



Source : ANSSI



# PROGRAMME DE SENSIBILISATION

## APPRENTISSAGE THÉORIQUE

kit de communication et plateforme d'e-learning

## APPRENTISSAGE PAR L'ACTION

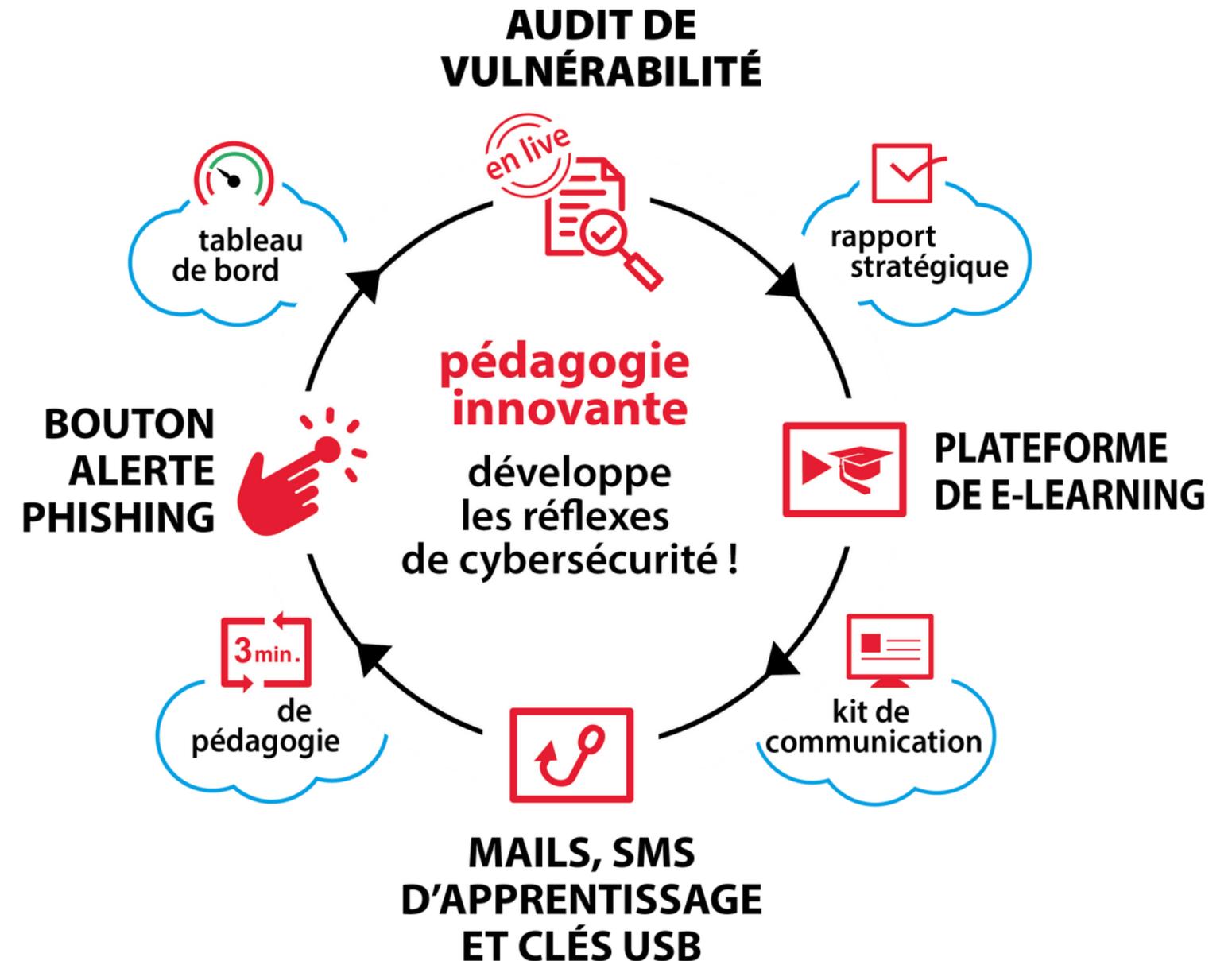
E-mails automatiques ciblés, SMS, USB  
Sensibilisation immédiate sur le poste

## ACCOMPAGNEMENT

Chargé(e) de compte dédié(e),  
Actions spécifiques à l'organisation  
Programme personnalisé

## REMONTÉE D'INFORMATIONS

Tableaux de bord  
Bouton Alerte Phishing



# Déroulé de la prestation

## Etape 1 : Audit



**Durée :** 5 jours ouvrés



**Objectif :** tester la réaction de vos utilisateurs



**Comment :** Envoie de 1 à 4 e-mails de niveau simple parmi 50 à 100 templates.



**Notre conseil :** Ne pas communiquer au préalable auprès de vos utilisateurs.



**Un e-mail envoyé à tous vos utilisateurs sur une durée de quelques heures.**

En cas de clic, une page personnalisée s'ouvre lui expliquant :  
C'est un exercice  
Ça aurait pu avoir de lourdes conséquences  
Restitution anonymisée des résultats prochainement



Les utilisateurs n'ayant pas cliqué, recevront 1 à 3 autres e-mails de test.

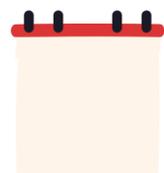


Envois plus sporadiques (15% à 20% de la population n'ayant pas cliqué chaque jour).



**Restitution des résultats de l'audit.**

Envoi d'un rapport et d'une infographie reprenant les principaux résultats de l'audit à communiquer auprès de vos utilisateurs.





Assistanat  
Services Web  
Communication

**LC INFOSERV'**  
Au service des entreprises

# CATALOGUE DU CONTENU

## KIT DE COMMUNICATION

### Affiche des bons réflexes

Avec **AvantdeCliquier.com** & **Apprenez à :**

1. Repérer un e-mail de phishing
2. Créer un mot de passe sécurisé
3. Signaler un incident
4. Vérifier l'identité de vos correspondants
5. Ne pas divulguer vos mots de passe
6. Protéger votre identité numérique
7. Protéger les données de votre organisation
8. Rester vigilant quant à l'usage de périphériques externes
9. Séparer vos usages personnels de vos usages professionnels

Suivez les dernières actus cyber

**L'humain au cœur de votre cybersécurité**

**Restez vigilant(e) lors de vos correspondances**

Plus de 90% des violations de données sont causées par des e-mails. En cas de doute contactez votre responsable informatique.

Apprenez à reconnaître les e-mails de phishing, les e-mails de fraude, les e-mails de phishing, les e-mails de phishing.

Ne cliquez jamais sur un lien suspect, ne téléchargez jamais de fichiers suspects, ne répondez jamais à un e-mail suspect.

Avant de cliquer sur un lien suspect, vérifiez l'adresse de l'expéditeur, vérifiez l'adresse de l'expéditeur, vérifiez l'adresse de l'expéditeur.

CONTACTEZ LE SERVICE INFORMATIQUE, un e-mail à [service.informatique@lcinfoserv.com](mailto:service.informatique@lcinfoserv.com), un téléphone au [0240000000](tel:0240000000), un fax au [0240000000](tel:0240000000).

Le service informatique est à votre disposition.

**Protégez les données personnelles de votre organisation**

Plus de la moitié des violations notifiées auprès de la CNIL, trouvent leur origine dans le piratage, des logiciels malveillants ou de l'hameçonnage.

Puis, viennent les équipements perdus ou volés, les e-mails volés et les publications non contrôlées.

Si vous pensez avoir été victime d'un incident de sécurité sur votre poste de travail, même si c'est votre ordinateur personnel, ne vous inquiétez pas, contactez votre responsable informatique, qui sera ravi de vous accompagner dans la gestion de cet incident.

CONTACTEZ LE SERVICE INFORMATIQUE, un e-mail à [service.informatique@lcinfoserv.com](mailto:service.informatique@lcinfoserv.com), un téléphone au [0240000000](tel:0240000000), un fax au [0240000000](tel:0240000000).

Le service informatique est à votre disposition.

**Les mots de passe**

Ne communiquez jamais votre mot de passe à un tiers.

N'utilisez pas le même mot de passe pour différents accès.

Déconnectez-vous avant de quitter votre poste de travail.

Changez le mot de passe au moindre soupçon de compromission.

Si vous pensez avoir été victime d'un incident de sécurité sur votre poste de travail, même si c'est votre ordinateur personnel, ne vous inquiétez pas, contactez votre responsable informatique, qui sera ravi de vous accompagner dans la gestion de cet incident.

CONTACTEZ LE SERVICE INFORMATIQUE, un e-mail à [service.informatique@lcinfoserv.com](mailto:service.informatique@lcinfoserv.com), un téléphone au [0240000000](tel:0240000000), un fax au [0240000000](tel:0240000000).

Le service informatique est à votre disposition.

**Veillez à dissocier les usages personnels des usages professionnels**

N'utilisez pas d'équipements personnels tels que vos clés USB, disques durs externes... pour un usage professionnel.

Vous risquez de véhiculer des virus informatiques capables de compromettre toute votre organisation.

Si vous pensez avoir été victime d'un incident de sécurité sur votre poste de travail, même si c'est votre ordinateur personnel, ne vous inquiétez pas, contactez votre responsable informatique, qui sera ravi de vous accompagner dans la gestion de cet incident.

CONTACTEZ LE SERVICE INFORMATIQUE, un e-mail à [service.informatique@lcinfoserv.com](mailto:service.informatique@lcinfoserv.com), un téléphone au [0240000000](tel:0240000000), un fax au [0240000000](tel:0240000000).

Le service informatique est à votre disposition.

## Écrans de veille / démarrage personnalisés sur la cybersécurité

## PLATEFORME E-LEARNING

Découvrir la plateforme

Les offres irrésistibles !

Recevez à domicile de fines courbes de phishing pour tester vos agents.

**Les Mots De Passe** 00:03:44

**LES HACKERS** 00:03:19

**Le Poste De Travail** 00:04:19

Le mail proposé aux agents de Mots de Passe.mp4

HACKERS.mp4

Poste de Travail - les Bots...

**Cyberattaque Réanir**

**Les Spams**

**Tout savoir sur le RGPD**  
Règlement Général sur la Protection des Données



Différents modules de 30 minutes sous forme de capsules de 2 à 4 minutes  
Quiz de fin de session délivrant un certificat de suivi  
Audio Français, Anglais & Espagnol - sous titré en plus de 20 langues



Assistanat  
Services Web  
Communication

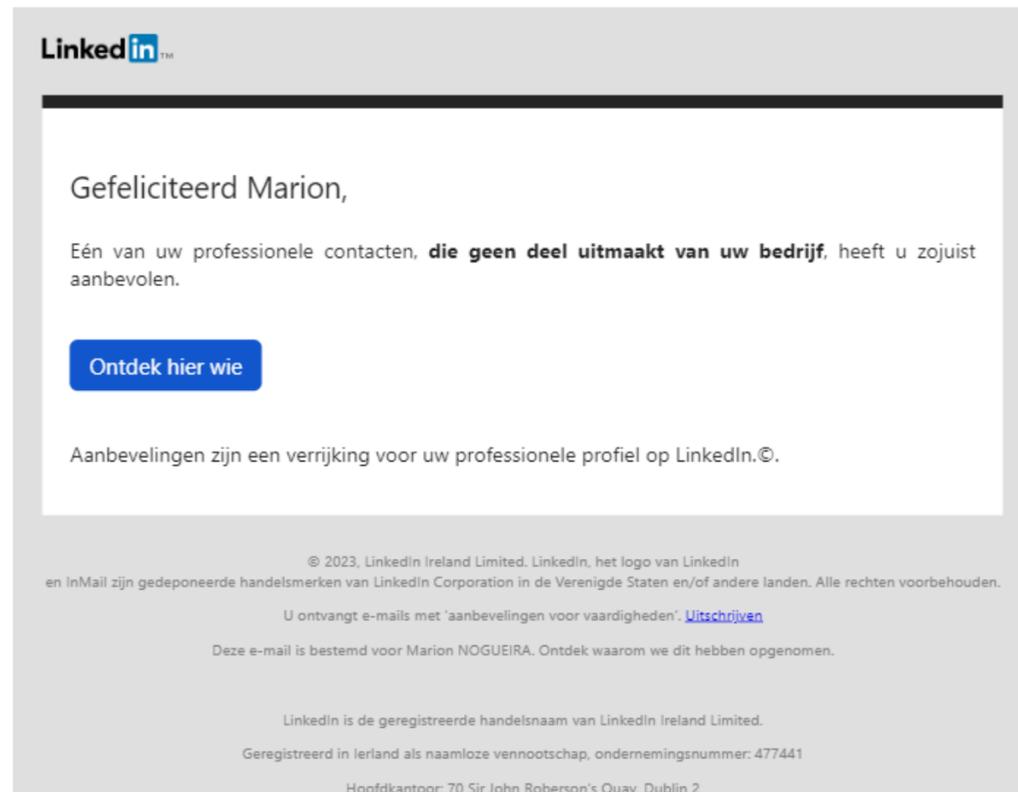
**LC INFOSERV'**  
*Au service des entreprises*

# CATALOGUE DU CONTENU MISE EN SITUATION : E-MAIL



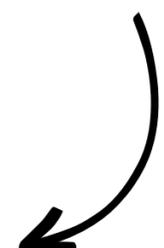
## Algorithme intelligent

- Détecter les faiblesses des utilisateurs
- Niveau de connaissance et besoins
- Développer les réflexes de vigilance
- Corriger le comportement
- Fréquences différentes
- Autant que nécessaire
- Valider les acquis



**Mise en situation multilingue en plus de 20 langues**

**Sensibilisation sur l'instant**  
(vidéo explicative)



# APPRENTISSAGE PAR L'ACTION

## MISE EN SITUATION : E-MAIL

Marion NOGUEIRA, non paiement de votre contravention

Contravention <contravention@cliquezvite.com>  
À: marion.nogueira@cliquezvite.com



Marion NOGUEIRA

Le 15/11/2022 à 8h27, [votre véhicule](#) a été contrôlé à 57 km/h (vitesse retenue de 51 km/h) sur une voie limitée à 50 km/h.

Voici plus de détails sur [votre contravention de 47 €](#).

En cas de non paiement dans les 48 heures, le montant de la contravention sera automatiquement majoré, vous n'aurez plus la possibilité de la contester, et  **votre dossier sera transmis au tribunal de grande instance.**

[Le service recouvrement](#)



Contravention suite à excès de vitesse

Diapositive 1 / 12

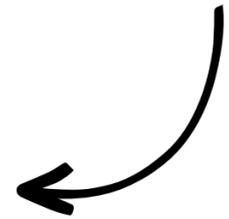
**Votre Logo**

Tentative d'hameçonnage

Pas de panique. Il ne s'agissait que d'un exercice. Mais  **votre clic aurait pu être lourd de conséquences.**

Votre sensibilisation ici

Vous êtes l'un des maillons essentiels de la protection de votre organisation. En étant vigilant, vous contribuez à lutter contre les cyberattaques. Vous êtes invité à suivre une formation de 3 minutes qui vous permettra de mieux comprendre ce qui aurait dû attirer votre attention.



Contravention suite à excès de vitesse

Diapositive 10 / 12

non paiement de votre contravention

Contravention <contravention@cliquezvite.com>

Le 26/09/2022 à 8h27,  **votre véhicule**  a été contrôlé à 57 km/h (vitesse retenue de 51 km/h) sur une voie limitée à 50 km/h.

Voici plus de détails sur  **votre contravention de 47 €.**

En cas de non paiement dans les 48 heures, le montant de la contravention sera automatiquement majoré, vous n'aurez plus la possibilité de la contester, et  **votre dossier sera transmis au tribunal de grande instance.**

**Le service recouvrement**

**Les liens**

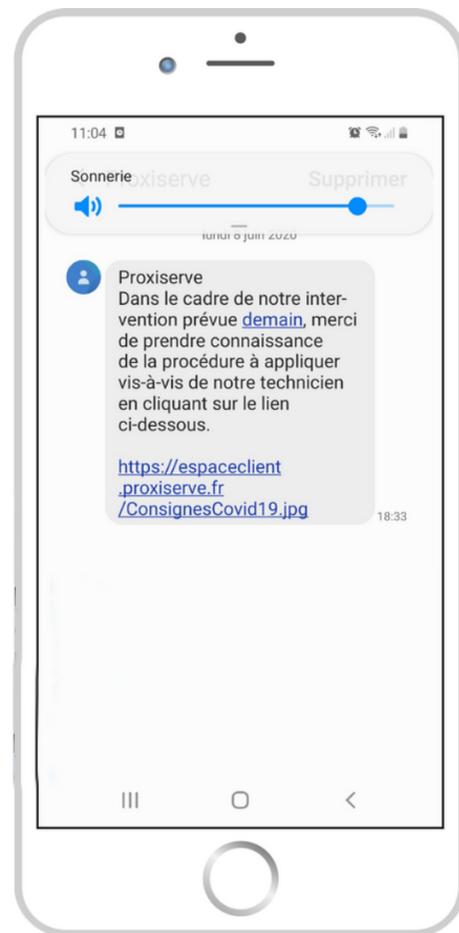
- Passez votre souris au dessus du lien  **sans cliquer** . Vous verrez alors en bas à gauche de votre navigateur que le lien de destination est de type `https://cliquezvite.com/v2/2a7dfc92e0b74b52af83127485eb95a4`.
- A l'évidence cliquezvite.com n'est pas un site connu sur lequel l'Etat procéderait au recouvrement des amendes.
- Méfiez-vous des adresses internet trop longues comportant une série alphanumérique complexe.
- Le https n'est pas un gage de fiabilité de la page de destination. https vous indique simplement que l'information circulant entre votre navigateur et le serveur de cliquezvite.com sera chiffrée.
- Tous les liens renvoient vers la même page de destination ce qui est assez atypique.

# CATALOGUE DU CONTENU

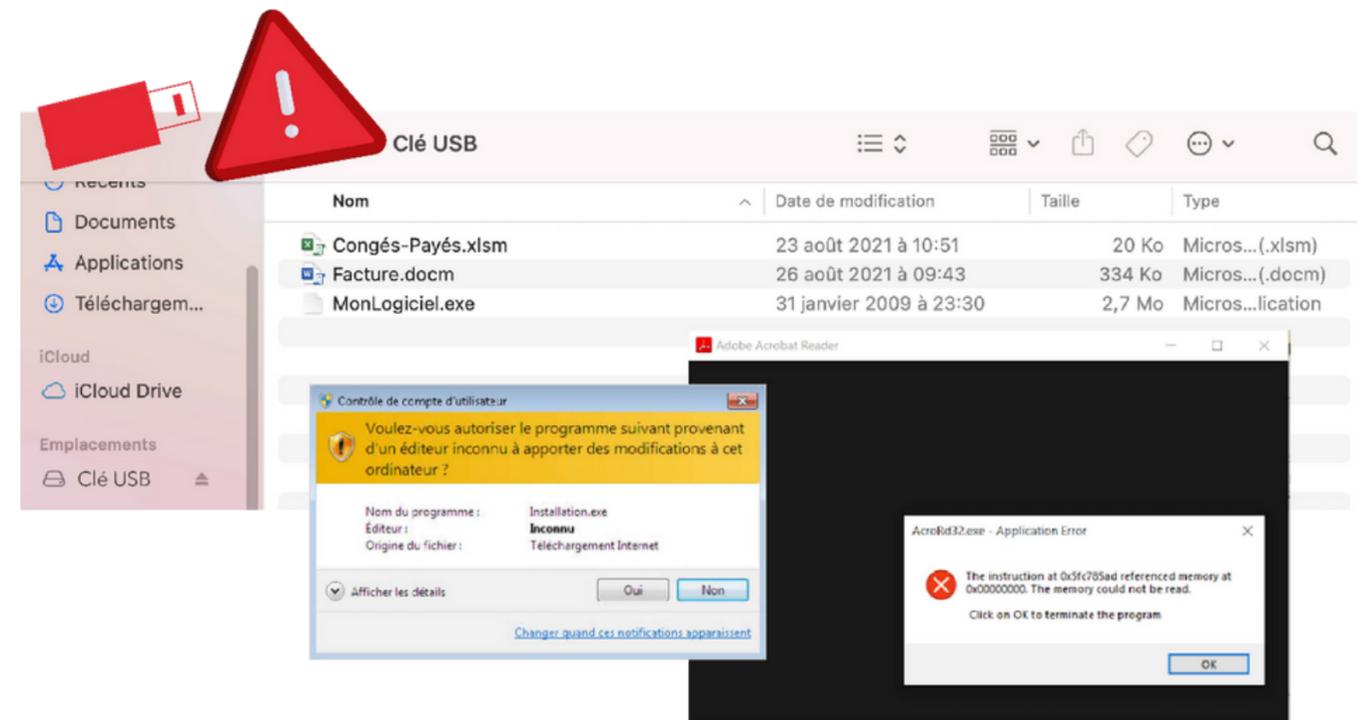
## MISE EN SITUATION SMS - USB

### SMiShing Awareness

Sensibilisation sur l'instant en cas de clic sur le lien



### USB Awareness



2 fichiers pirates à déposer sur vos propres clé USB

Sensibilisation sur l'instant en cas d'activation des macros

# CATALOGUE DU CONTENU

## BOUTON ALERTE PHISHING

### Option supplémentaire

**Add on :**

### Microsoft Office 365

- ▶▶ client lourd, OWA
- ▶▶ application Outlook (Android et iPhone)

### Exchange On Premise

- ▶▶ supérieurs à 2016
- ▶▶ hybride/ non hybride 2016

Félicitations lorsque l'e-mail est lié à la campagne

Quelqu'un a recommandé vos compétences professio...

dimanche 6 septembre 2020 à 21:36  
À : Stéphane TABIA

**Alerte Phishing**

**AvantdeCliquier.com**  
Solution anti-phishing pour les entreprises

## FÉLICITATIONS

Vous le savez votre organisation est accompagnée par la société Avant de Cliquier pour ce qui est de la sensibilisation à la problématique de l'hameçonnage (phishing).

En étant vigilant et en exerçant votre sens critique vous êtes parvenu à déjouer cette mise en situation.

Continuez de signaler les e-mails potentiellement dangereux en cliquant sur le bouton Alerte Phishing. Ainsi vous participerez à la protection de votre organisation.

Vous pouvez maintenant reprendre votre activité.

**LinkedIn**

**Félicitations Stéphane,**

Un de vos contacts professionnels, qui n'appartient pas à votre entreprise, vient de recommander certaines de vos compétences professionnelles.

[Voir de qui il s'agit](#)

Les recommandations permettent à votre profil professionnel d'être mieux vu sur LinkedIn®.

© 2016, LinkedIn Ireland Limited. LinkedIn, le logo de LinkedIn et InMail sont des marques déposées de LinkedIn Corporation aux États-Unis et/ou dans d'autres pays. Tous droits réservés.

Vous recevez des e-mails "Recommandations de compétences". [Se désinscrire](#)

### Message Center Major Change Update Notification

samedi 5 septembre 2020 à 18:59  
À : Stéphane TABIA



Organization: AVANT DE CLIQUER  
**Change to the minimum iOS system requirements for Outlook for iOS and watchOS MC221506**

Major update: Announcement started  
Applied To: All

We are changing the minimum iOS system requirements for Outlook for iOS and watchOS. Outlook for iOS is supported on the two most recent versions of iOS. With iOS 14 currently in beta, Outlook for iOS is preparing to remove support for iOS 12. In addition, once iOS 14 is released to GA, the system requirements for Outlook for iOS will be updated to reflect support for iOS 14. Microsoft will update the minimum system requirements for the Outlook for iOS app from iOS 12 to iOS 13.

**Alerte Phishing**

**AvantdeCliquier.com**  
Solution anti-phishing pour les entreprises

Cher utilisateur,

L'e-mail que vous avez signalé a été transmis à l'équipe informatique à l'adresse phishing@avantdecliquer.com qui va l'analyser dans les plus brefs délais.

En signalant des e-mails potentiellement dangereux, vous participez de manière active à la cybersécurité de votre organisation.

Vous pouvez maintenant reprendre votre activité.

Fichier .eml transféré à l'adresse de signalement ou sur votre outil de ticketing.

# CATALOGUE DU CONTENU ACCOMPAGNEMENT

## Points d'accompagnements avec un(e) chargé(e) de compte :



Restitution et suivi des résultats



Suivi de l'évolution d'apprentissage des utilisateurs



Mise en place de plans d'action d'améliorations des résultats



Ajout d'attaques spécifique à votre organisation et/ou secteur d'activité (type fraude au président)

**Récapitulatif trimestriel personnel qui résume les réactions de l'utilisateur** (suivi formation, nombre d'e-mail remontés, etc) .



**Documenter toutes les actions de sensibilisation en temps réel**

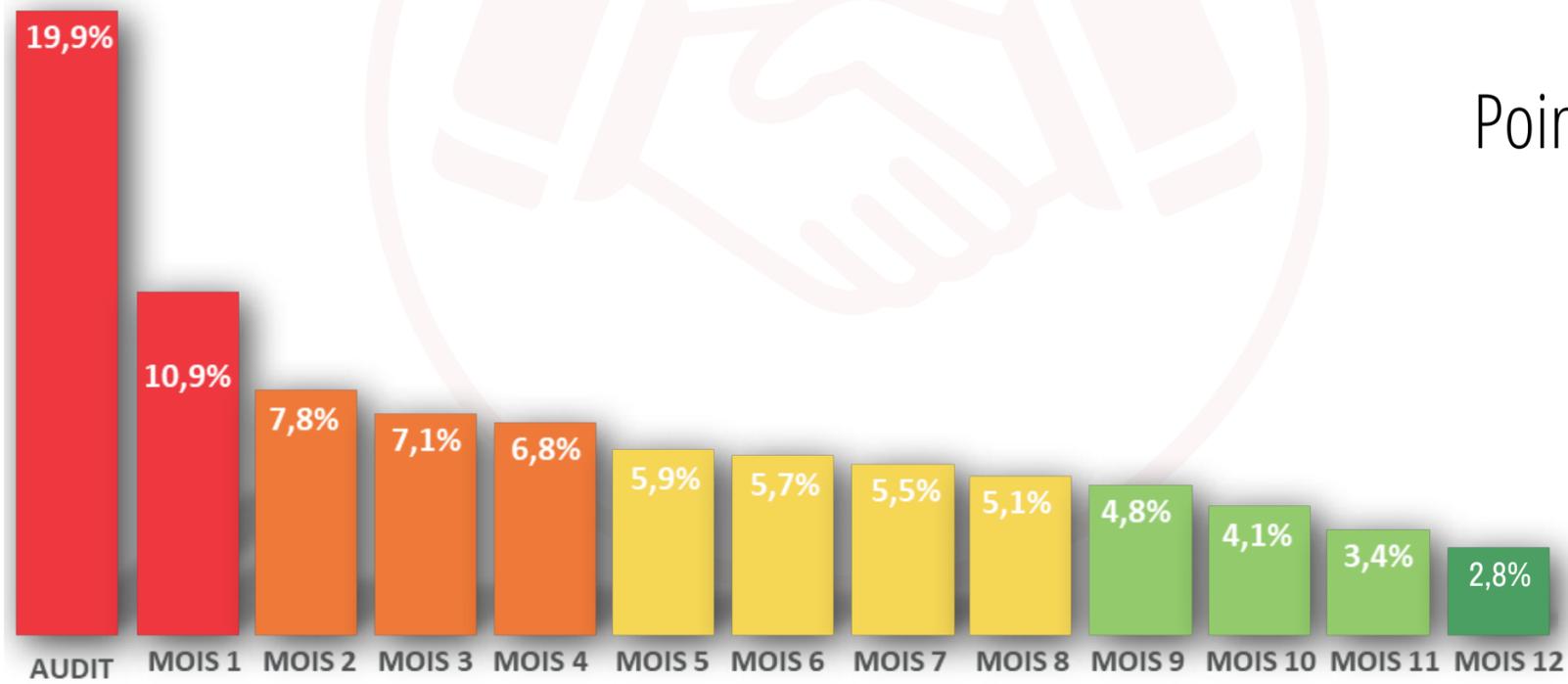


**Découvrir le tableau de bord**



# Pourquoi Avant de Cliquer ?

Taux de clic \*



Durée

- Programme de sensibilisation automatique
- Montée en compétence individuelle sur mesure
- Utilisateur autonome, comportement transformé de façon pérenne
- Attaques spécifiques créées sur mesure
- Point d'accompagnement avec un(e) chargé(e) de compte

Notre mission **diviser par**



**Avantde  
Cliquer**.com

**L'humain au cœur  
de la cybersécurité**

Assistanat

Services Web

Communication

**LC INFOSERV'**

*Au service des entreprises*

**Rendez-vous de présentation ici**

<https://avantdecliquer.com/partenaires/?partenaire=lcinfoserv>