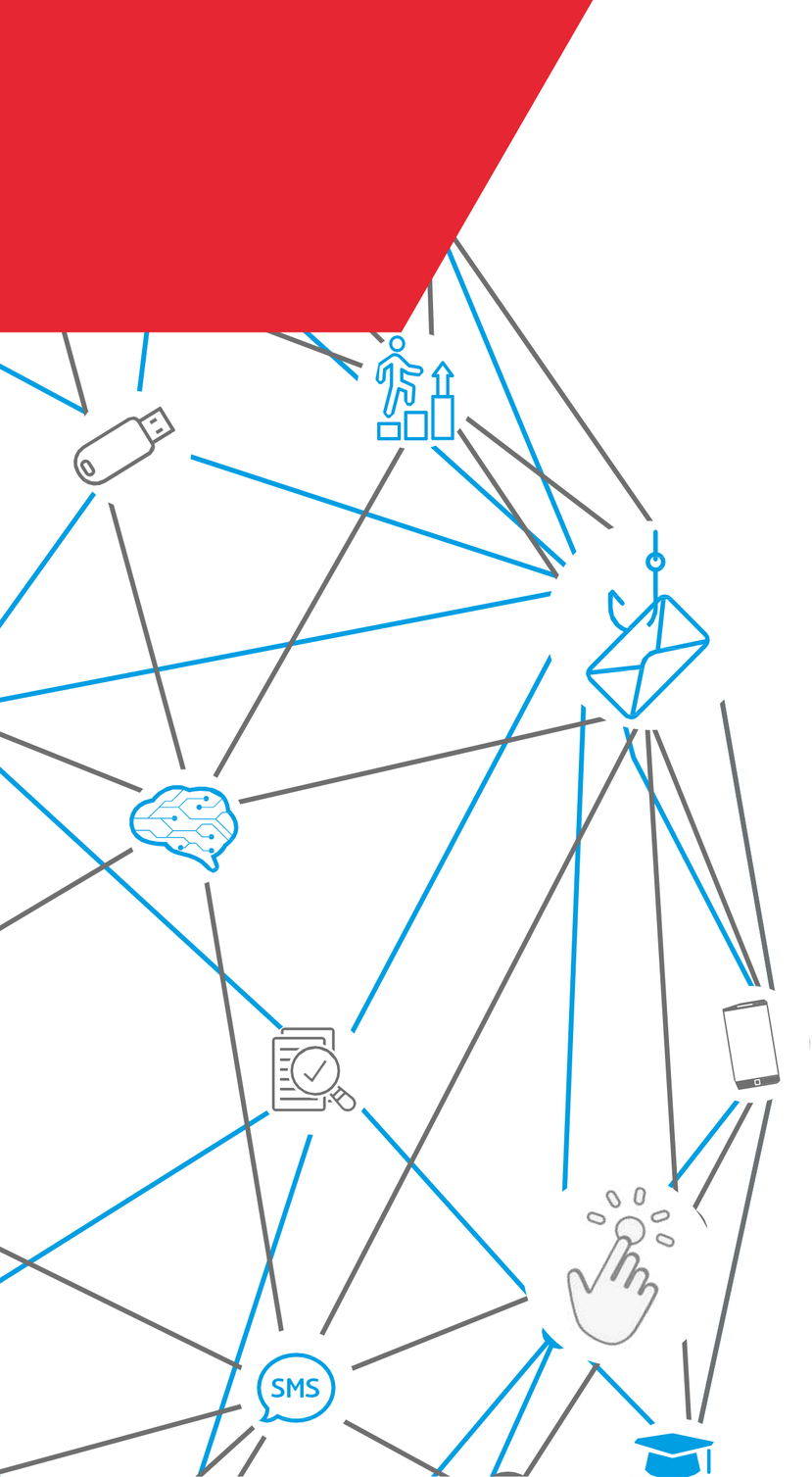


AvantdeCliquer.com

L'humain au cœur de la cybersécurité

Le programme de sensibilisation innovant sur 12 mois permettant une autonomie de l'utilisateur face aux attaques par phishing.

Solution mise en avant dans différents secteurs d'activités

2018

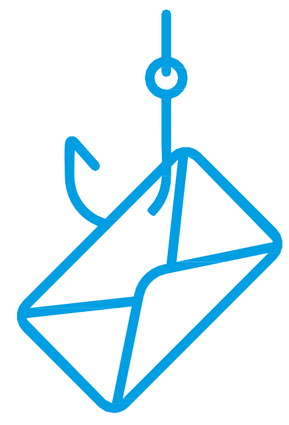
2019

2020

Secteur industriel :
Lauréat de l'intelligence économique et prix coup de cœur de la 13ème édition des trophées de l'agroalimentaire

(630 entreprises de l'agroalimentaire)

2021



80% des cyberattaques

proviennent d'un e-mail de phishing

qu'un utilisateur sensibilisé n'aurait pas cliqué

Les techniques de phishing ont évolué

Le constat d'un chercheur du CNRS :
https://drive.google.com/open?id=15wkC8b8oVr7u_wzb-JaBazgovdhrTPjS

Notre mission

Division par dix du risque de cyberattaque
Permettre sans effort aux DSI, RSSI, DPO et à la gouvernance... de respecter l'obligation légale de sensibilisation des utilisateurs.

Conséquences d'une cyberattaque avérée

Rançongiciels

Une rançon de 1 M € payée en France en 2019

Dégradation de l'image

dans les médias de manière durable

Patrimoine immatériel

Vol de méthodes, de brevets,
d'informations confidentielles

Fraude au président

Détournement de fonds

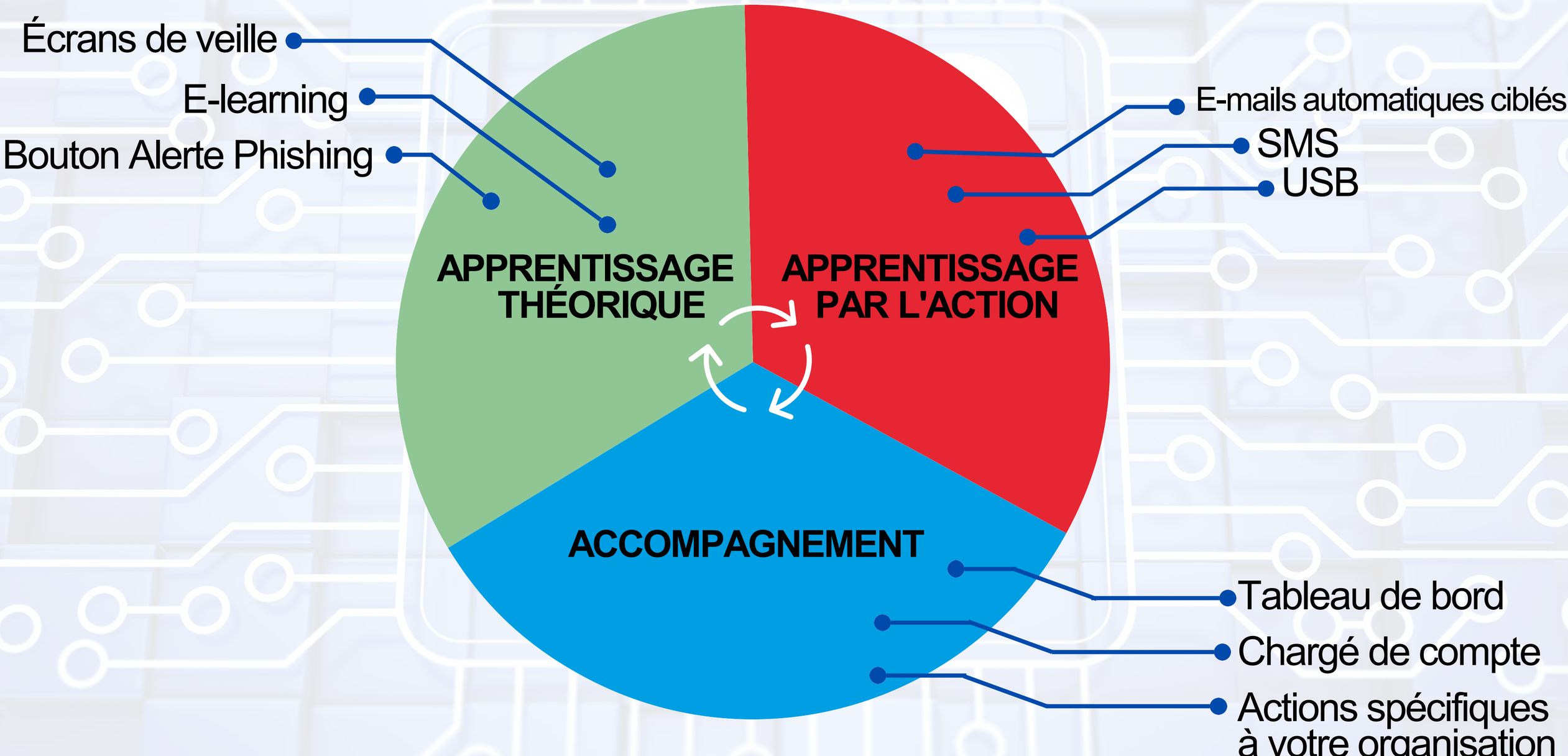
Perte de confiance

des administrés, des partenaires, des équipes, des fournisseurs

Blocage

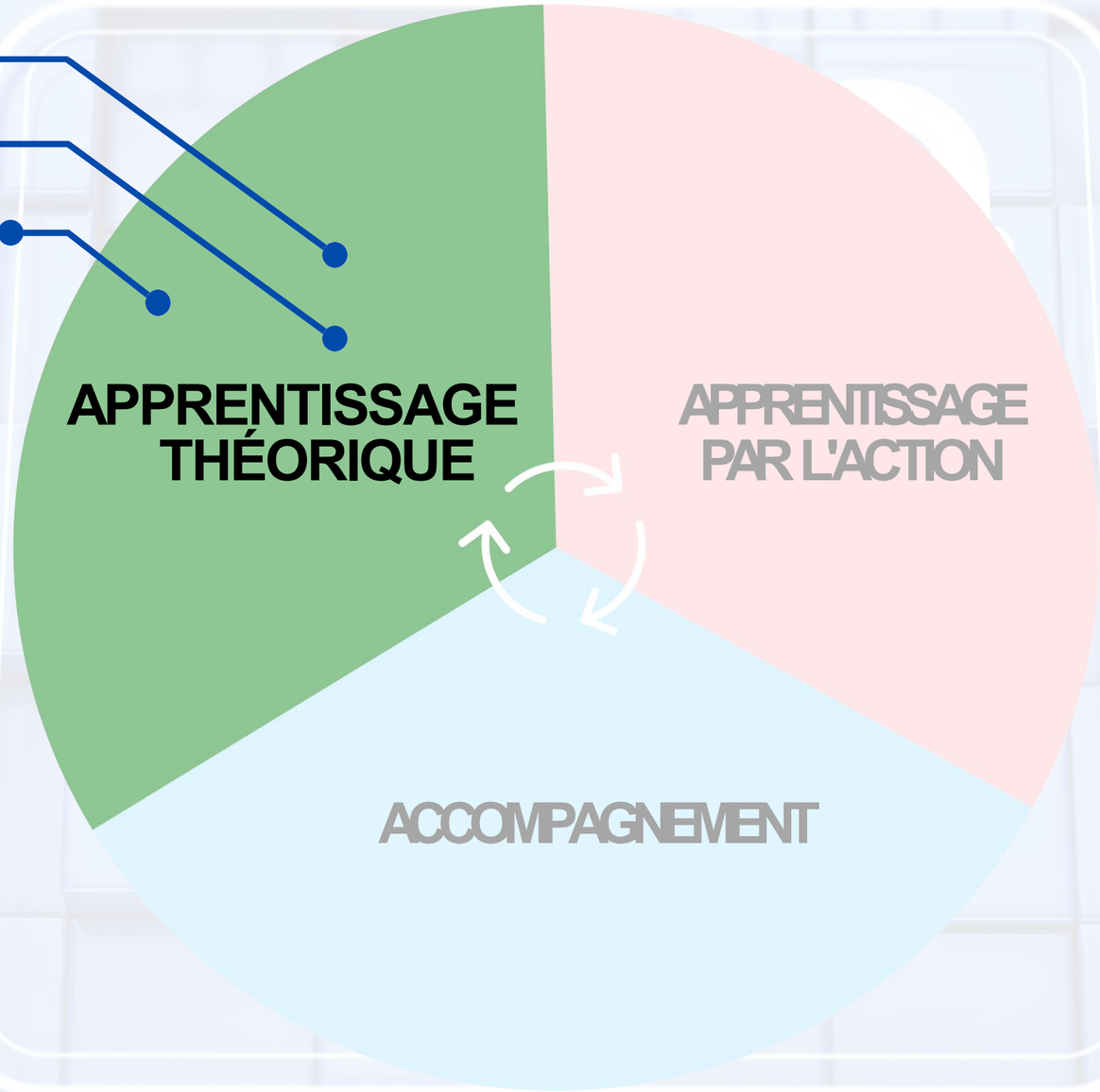
de la production, des expéditions,
de la comptabilité, des paies...

Sensibilisation à la cybersécurité en 3 parties



Première partie : l'apprentissage théorique

Écrans de veille
E-learning Phishing
E-Learning Cybersécurité



APPRENTISSAGE THÉORIQUE
ÉCRANS DE VEILLE PÉDAGOGIQUES

Écrans de veille ou de démarrage personnalisés sur la cybersécurité

- Au nombre de 9
- Disponibles dans 7 langues : Français, Anglais, Allemand, Espagnol, Ukrainien,
- Roumain et Russe Possibilité de traduire dans d'autres langues

APPRENTISSAGE THÉORIQUE
E-LEARNING

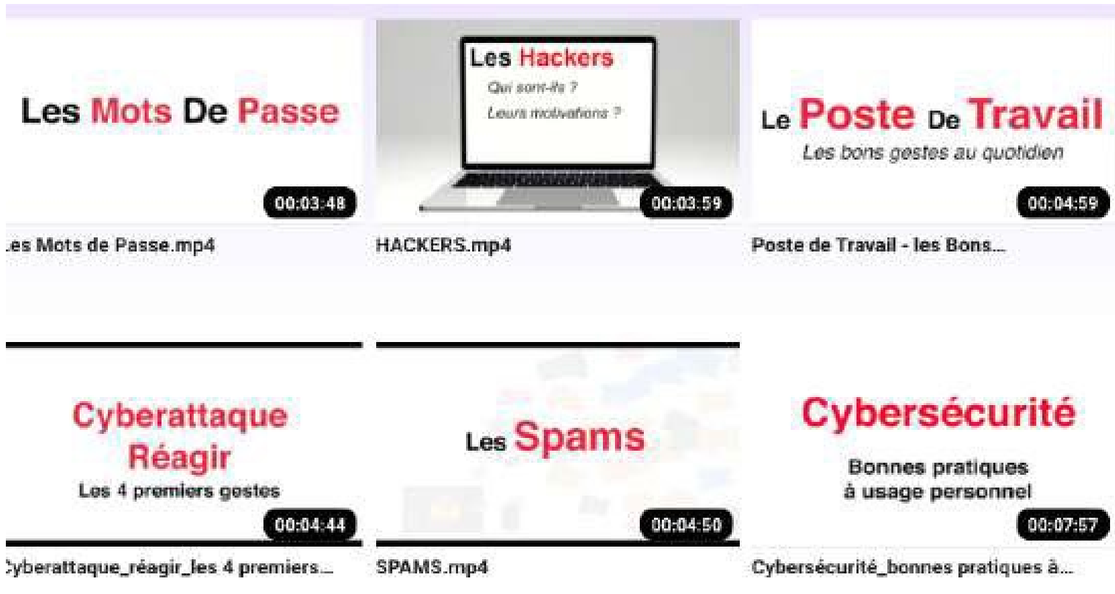
Accès à la plateforme e-learning sur le phishing

- Module phishing de 30 minutes sous forme de capsules de 1 à 3
- minutes Quiz de fin de session délivrant un certificat de suivi
- Disponible en plusieurs langues : Allemand, Anglais, Bulgare, Chinois simplifié,Coréen, Espagnol, Hongrois, Italien, Japonais, Néerlandais, Polonais, Portugais, Roumain, Russe, Turc et Ukrainien

APPRENTISSAGE THÉORIQUE
E-LEARNING

Accès à des vidéos de e-learning sur la cybersécurité

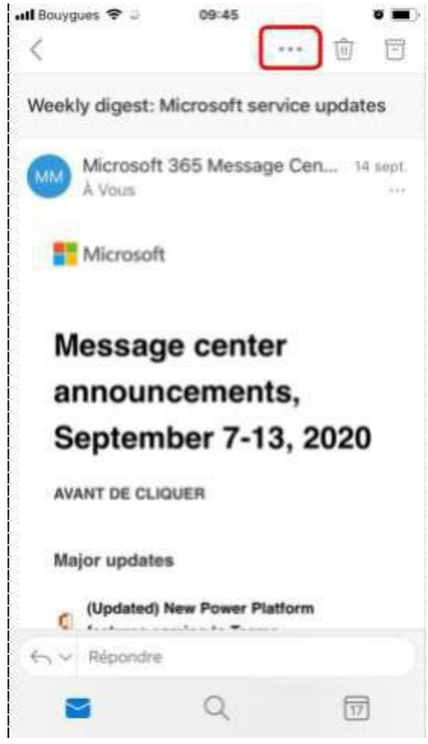
- Modules cybersécurité de 3 à 5 minutes abordant les mots de passe, le poste de travail, la cybersécurité dans la vie personnelle...

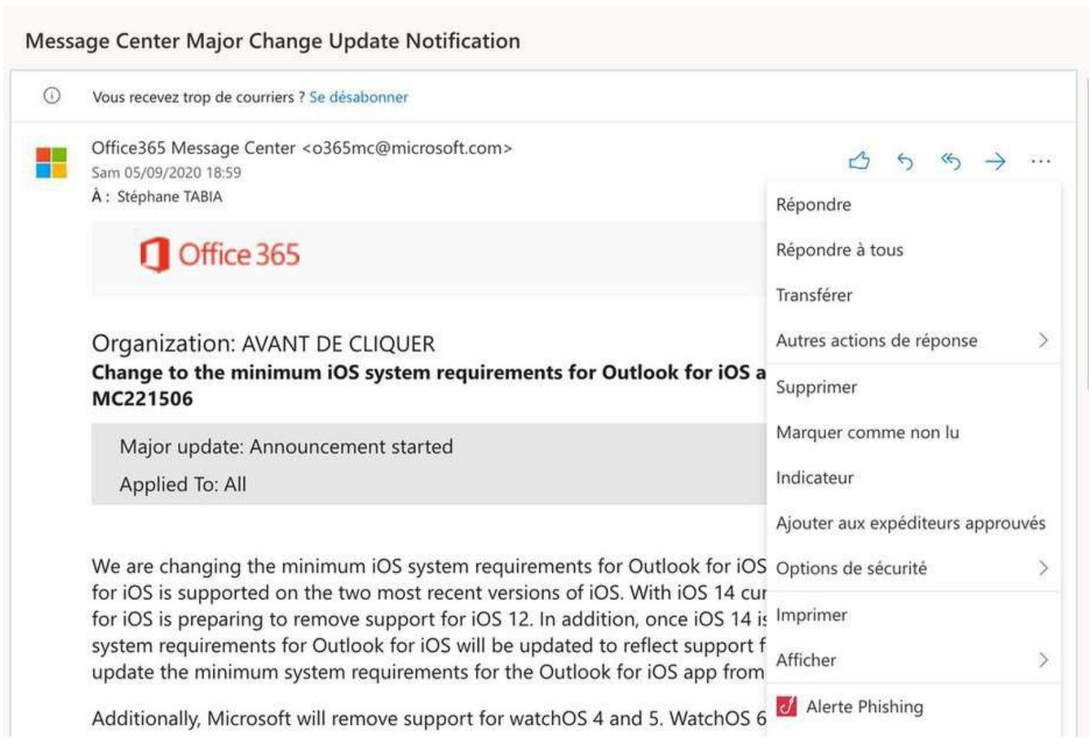


APPRENTISSAGE THÉORIQUE
BOUTON ALERTE PHISHING
(option supplémentaire)

Fonctionnement du Bouton Alerte Phishing

- Fonctionne dans 95% des cas sur Microsoft Office 365, que cela soit sur le client lourd, OWA, l'application Outlook sur Android et iPhone.
- Le déploiement se fait en 10 minutes.
- Fonctionne dans 90% des cas sur Exchange On Premise (2016 et plus). Le déploiement peut nécessiter quelques heures.

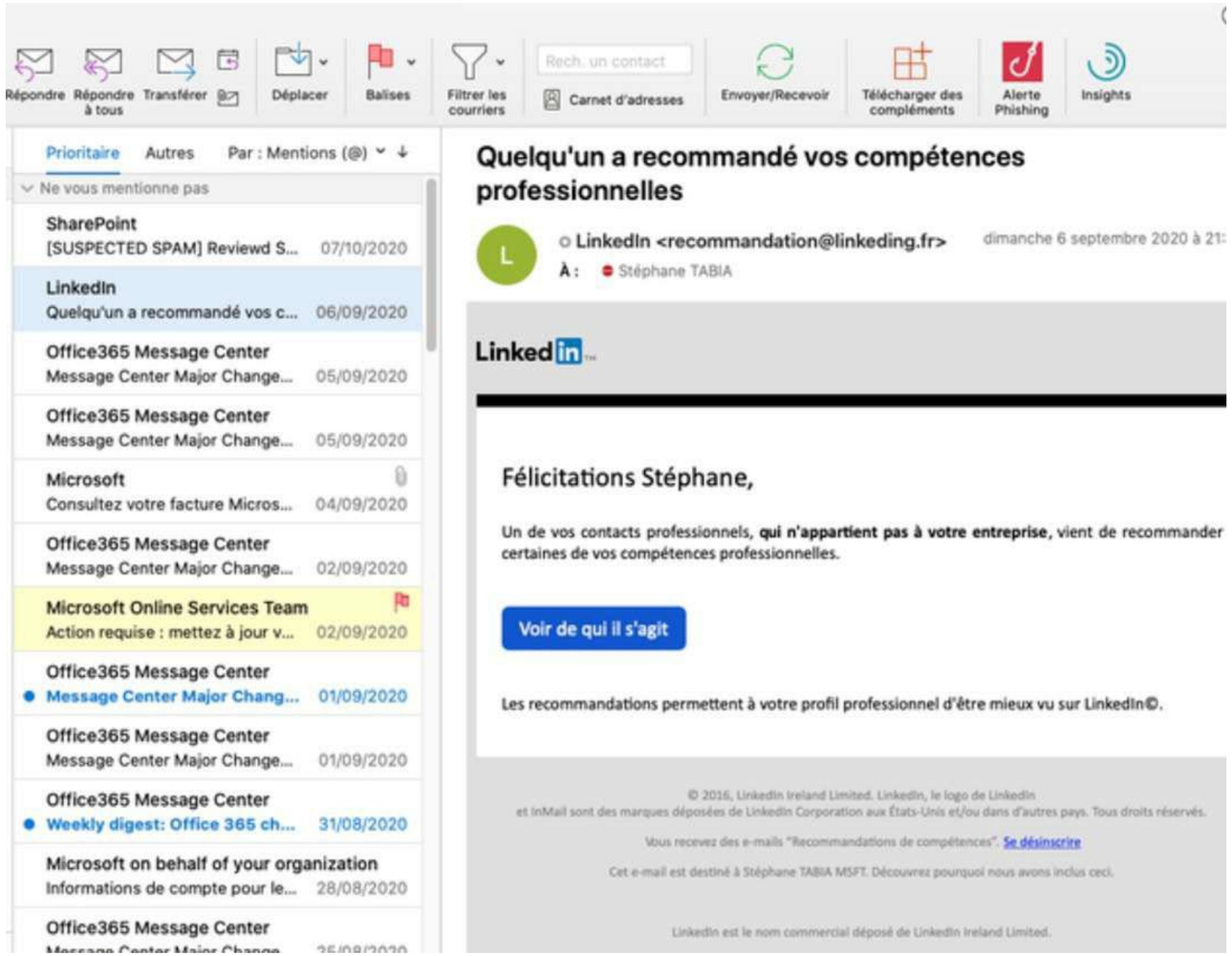


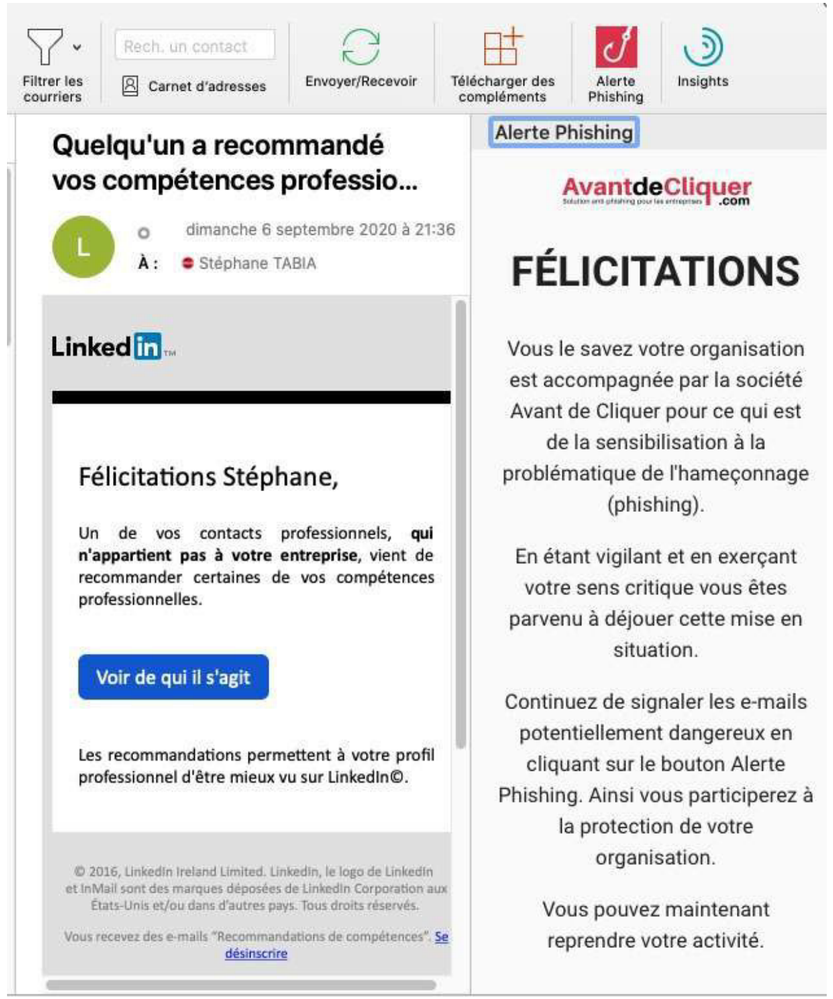


APPRENTISSAGE THÉORIQUE
BOUTON ALERTE PHISHING
(option supplémentaire)

Fonctionnement du Bouton Alerte Phishing

- Un utilisateur signalant un e-mail lié à la campagne est félicité sur l'instant.

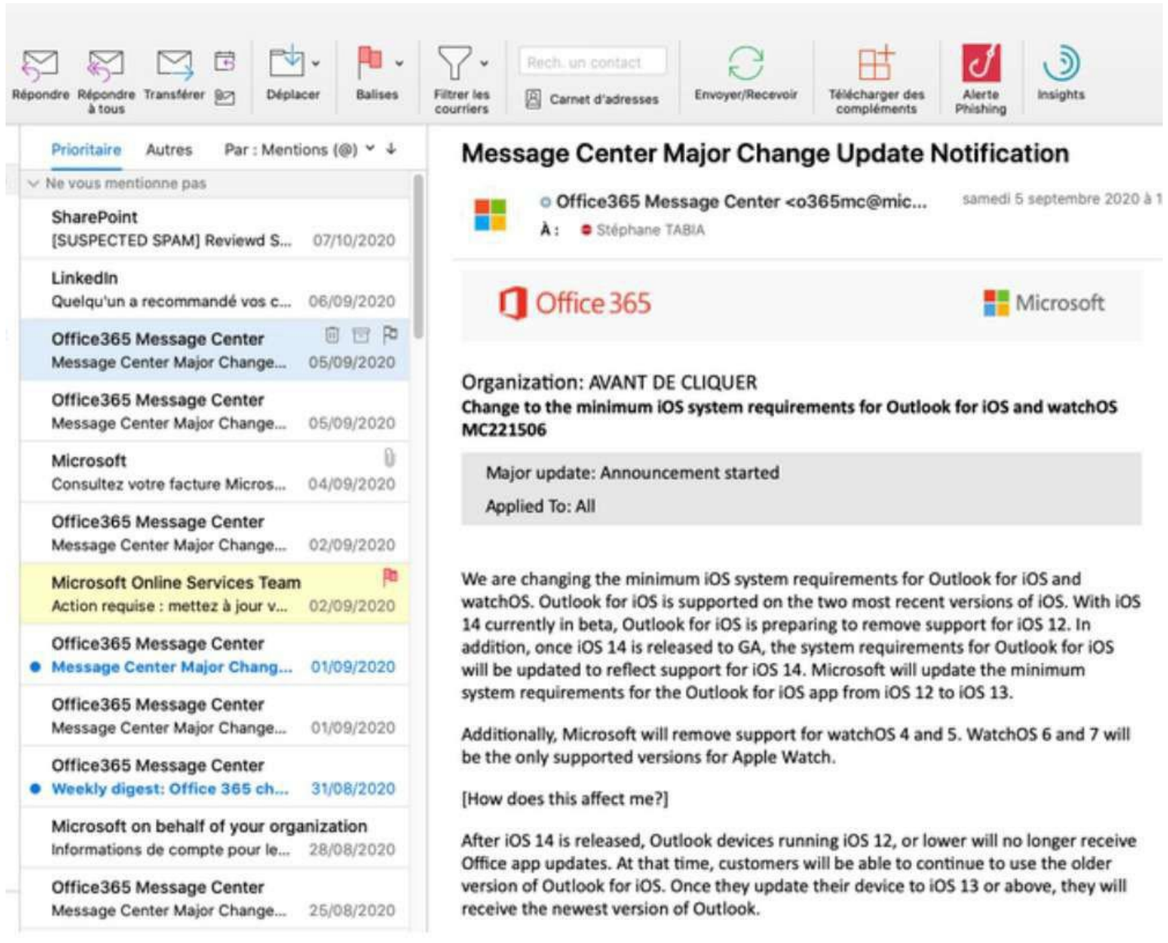


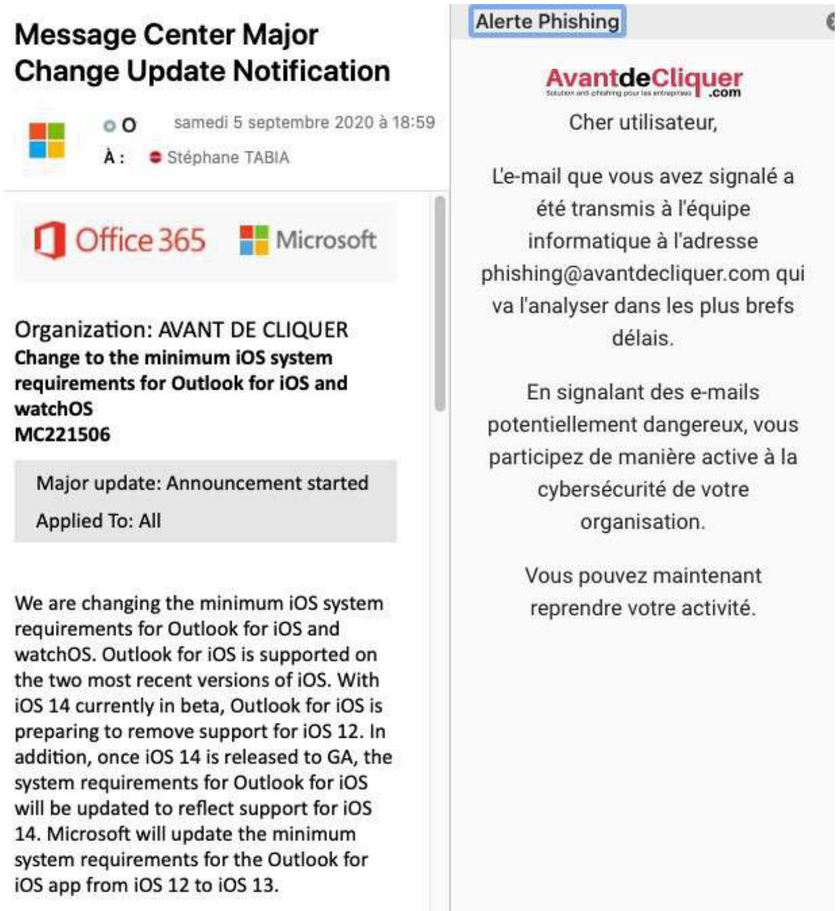


APPRENTISSAGE THÉORIQUE
BOUTON ALERTE PHISHING
(option supplémentaire)

Fonctionnement du Bouton Alerte Phishing

- Le fichier .eml (ou l'e-mail si le transfert d'eml n'est pas compatible avec votre environnement) est immédiatement transféré à l'adresse de signalement de votre choix ou sur votre outil de ticketing.





APPRENTISSAGE THÉORIQUE

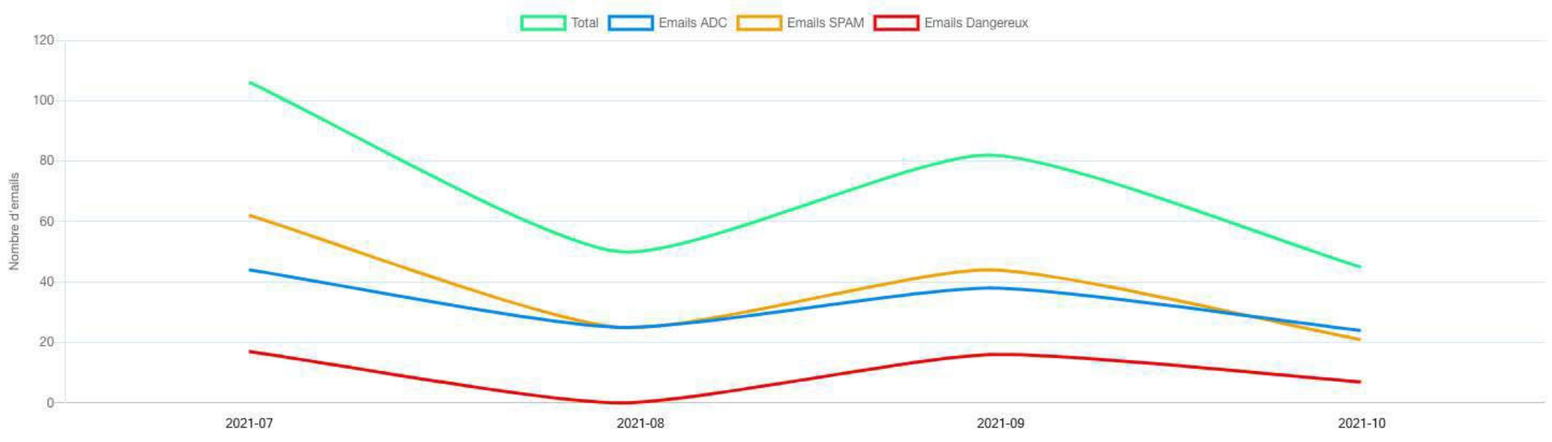
BOUTON ALERTE PHISHING

(option supplémentaire)

Fonctionnement du Bouton Alerte Phishing

Statistiques globales

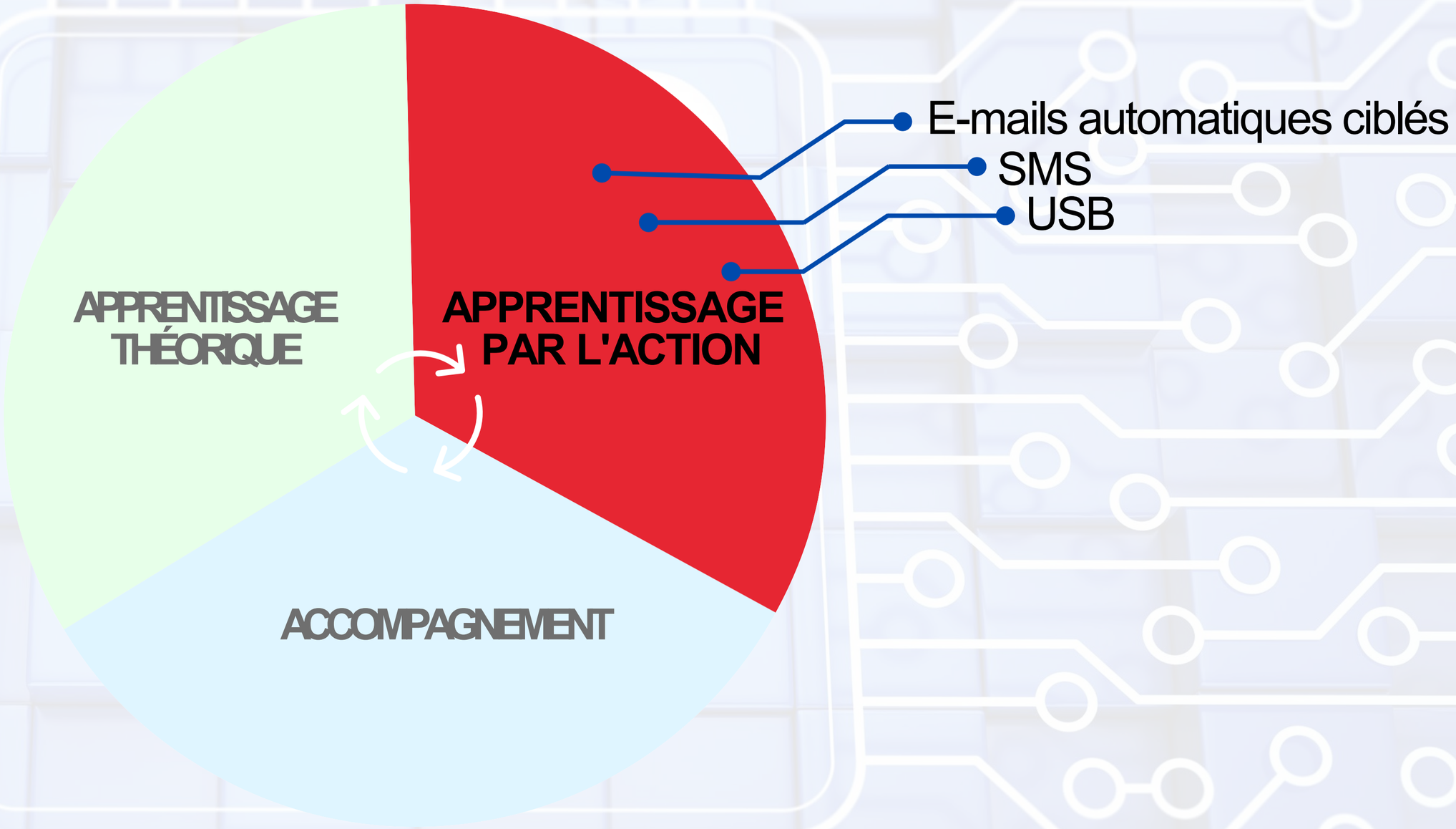
Date	Signalements total	Emails ADC	Emails SPAM	Emails dangereux	Personnes ayant signalé
07/2021	106	44	62	17	1
08/2021	50	25	25	0	1
09/2021	82	38	44	16	1
10/2021	45	24	21	7	1



Le bouton d'alerte phishing permet :

- de valoriser les utilisateurs qui vous remontent des informations
- de recevoir en temps réel des fichiers .eml vous permettant d'avoir des informations sur les entêtes
- de réagir plus vite en cas d'attaque, y compris dans le cadre du télétravail
- de quantifier le nombre d'attaques réelles que les utilisateurs auront permis de déjouer
- de communiquer en interne

Deuxième partie : l'apprentissage par l'action



APPRENTISSAGE PAR L'ACTION
MISE EN SITUTATION : E-MAIL

Étape 1 : Audit de vulnérabilité

- Évaluation de la cyber-résistance face au phishing
- Pas d'information préalable des utilisateurs
- Envoi de 1 à 4 e-mails par utilisateur sur une période de 5 jours ouvrés
- Les utilisateurs qui cliquent sont dirigés vers une page indiquant qu'il s'agissait d'un exercice de sensibilisation
- Envoi d'un rapport détaillé
- Restitution des résultats en partage d'écran par un expert

APPRENTISSAGE PAR L'ACTION

MISE EN SITUTATION : E-MAIL

Étape 2 : Communication

- Nous vous fournissons un plan de communication pour l'ensemble de votre organisation avec infographie des résultats
- Nous insistons sur le fait que la sensibilisation est également utile dans la sphère personnelle
- Les utilisateurs sont informés des étapes suivantes
    - Démarrage de l'outil SaaS

APPRENTISSAGE PAR L'ACTION

MISE EN SITUTATION : E-MAIL

Algorithme intelligent

Étape 3 : Envoi automatique par l'outil SaaS

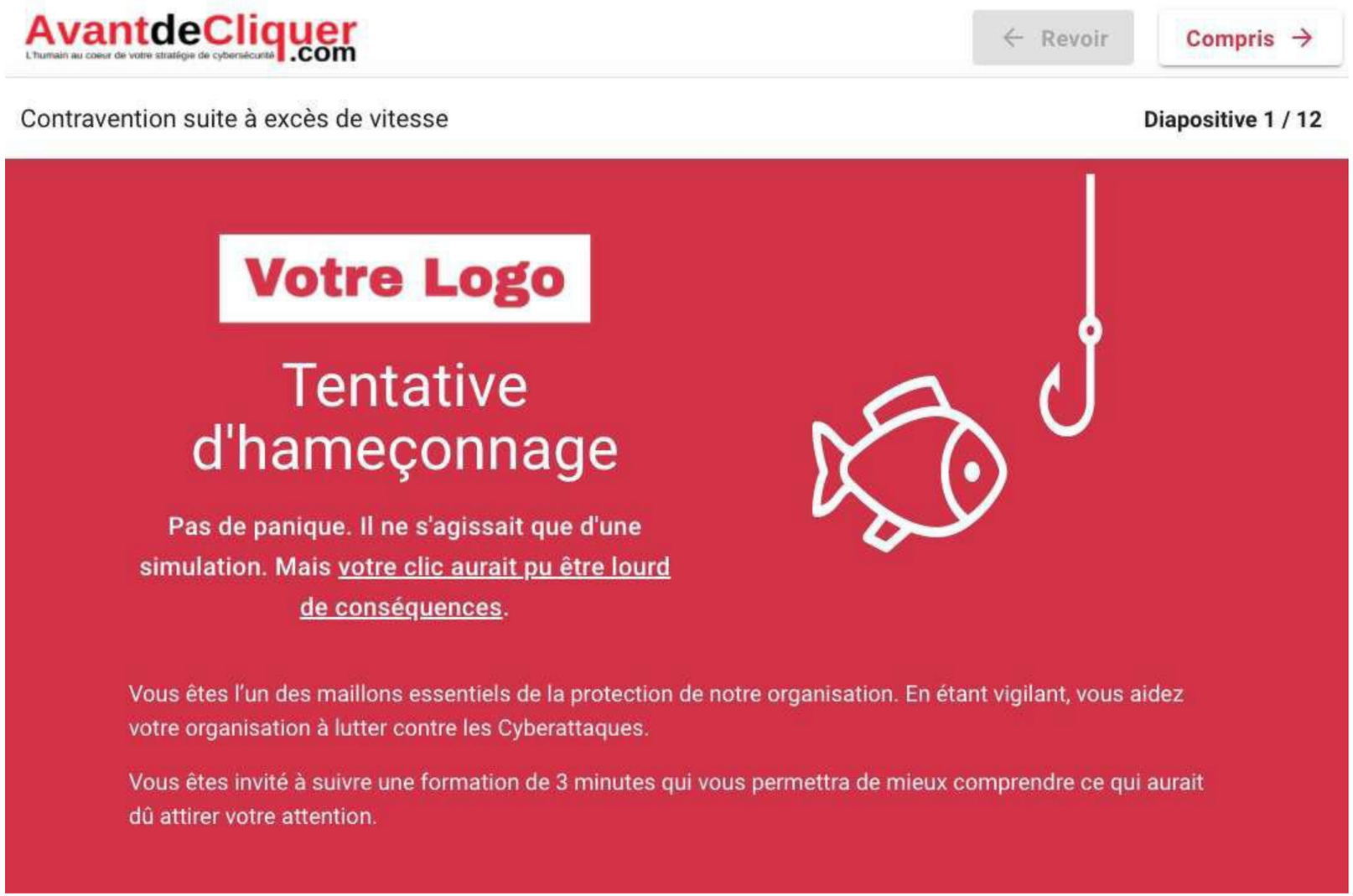
Automatiquement, tout au long de l'année, Avant de Cliquer envoie des e-mails d'apprentissage afin de :

- Focusser les maillons les plus faibles
- Détecter les faiblesses des utilisateurs
- Corriger le comportement (sensibilisation de 3 minutes pédagogiques)
- Valider les acquis (envois de mises en situation permettant de confirmer l'assimilation de telles ou telles caractéristiques)

APPRENTISSAGE PAR L'ACTION

MISE EN SITUTATION : E-MAIL

Étape 3 : Envoi automatique par l'outil SaaS



APPRENTISSAGE PAR L'ACTION

MISE EN SITUTATION : E-MAIL

Algorithme intelligent

Étape 3 : Envoi automatique par l'outil SaaS

- Différents selon le niveau de connaissance et des besoins
- A des fréquences différentes
- Autant que nécessaire
- Afin de développer les réflexes de cyber-vigilance des utilisateurs
- Sans intervention de votre part

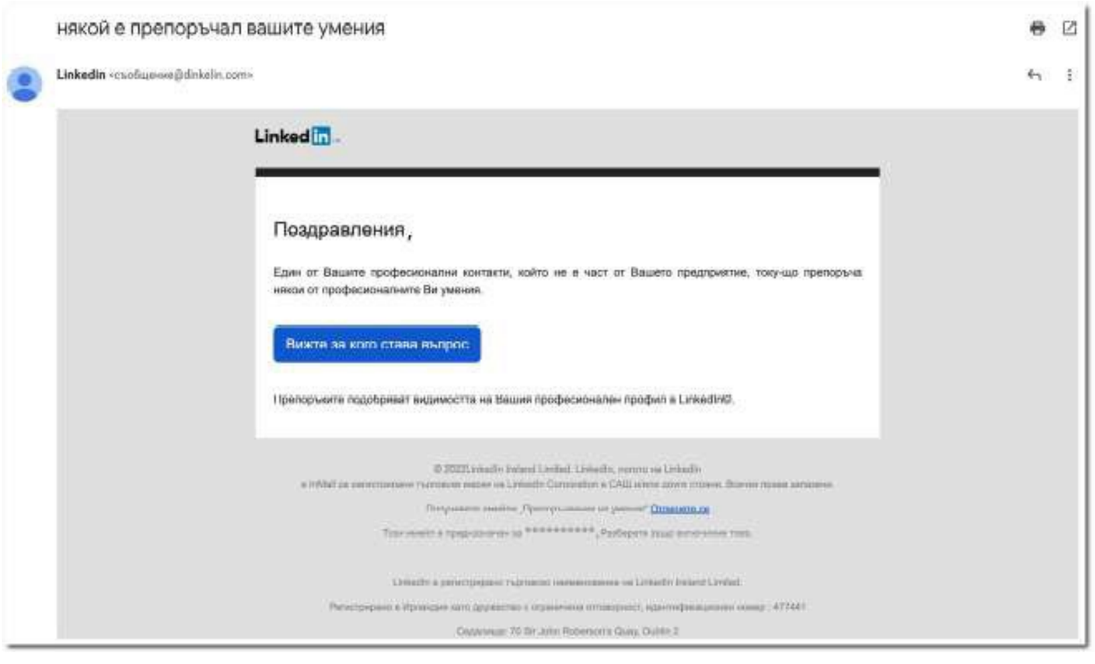
APPRENTISSAGE PAR L'ACTION

MISE EN SITUTATION : E-MAIL

Mise en situation multilingue

La solution Avant de Cliquer est disponible en Français ainsi qu'en 16 autres langues :

Allemand	Chinois simplifié	Hongrois	Neerlandais	Roumain	Ukrainien
Anglais	Coréen	Italien	Polonais	Russe	
Bulgare	Espagnol	Japonais	Portugais	Turc	

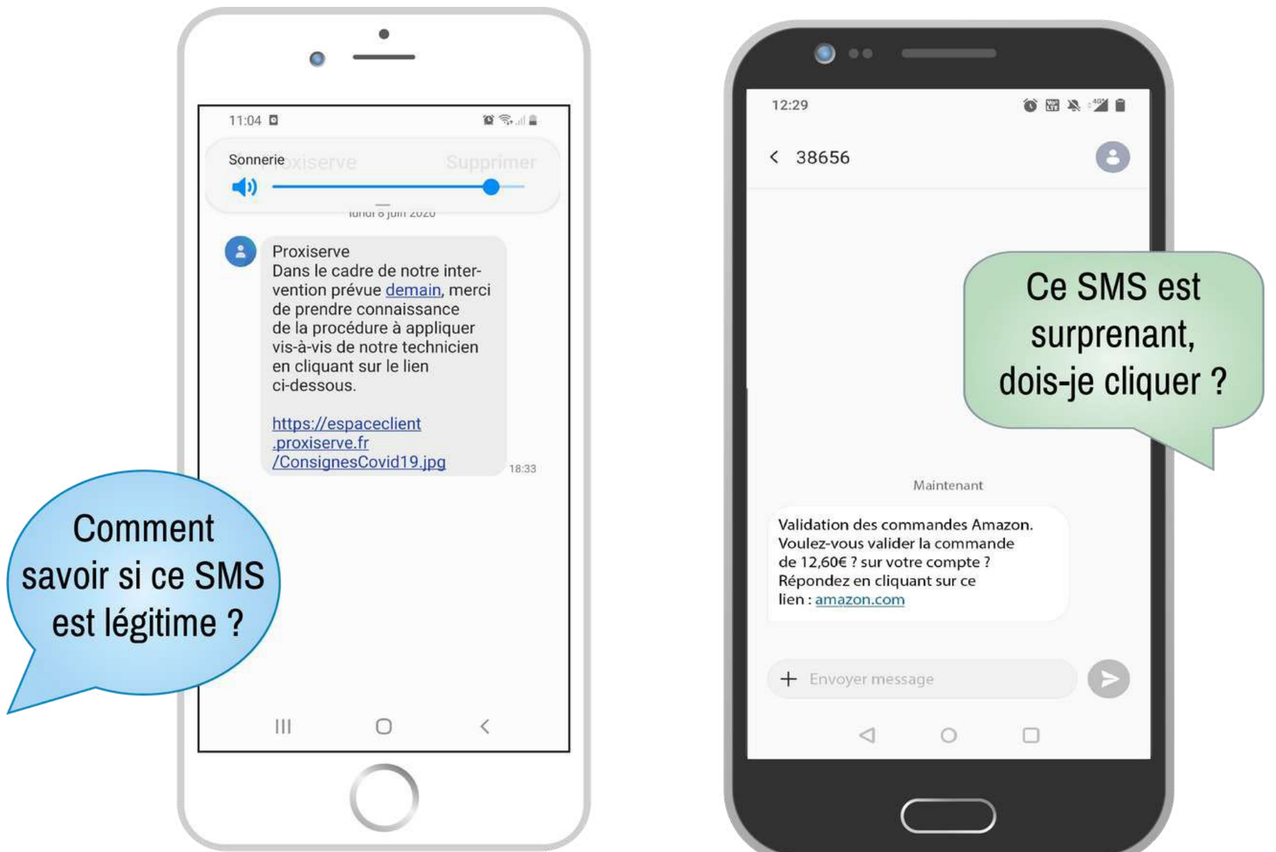


APPRENTISSAGE PAR L'ACTION

MISE EN SITUTATION : SMS

SMiShing Awareness

Envoi de campagne de SMS sur les téléphones mobiles de vos utilisateurs pour les sensibiliser au Smishing :



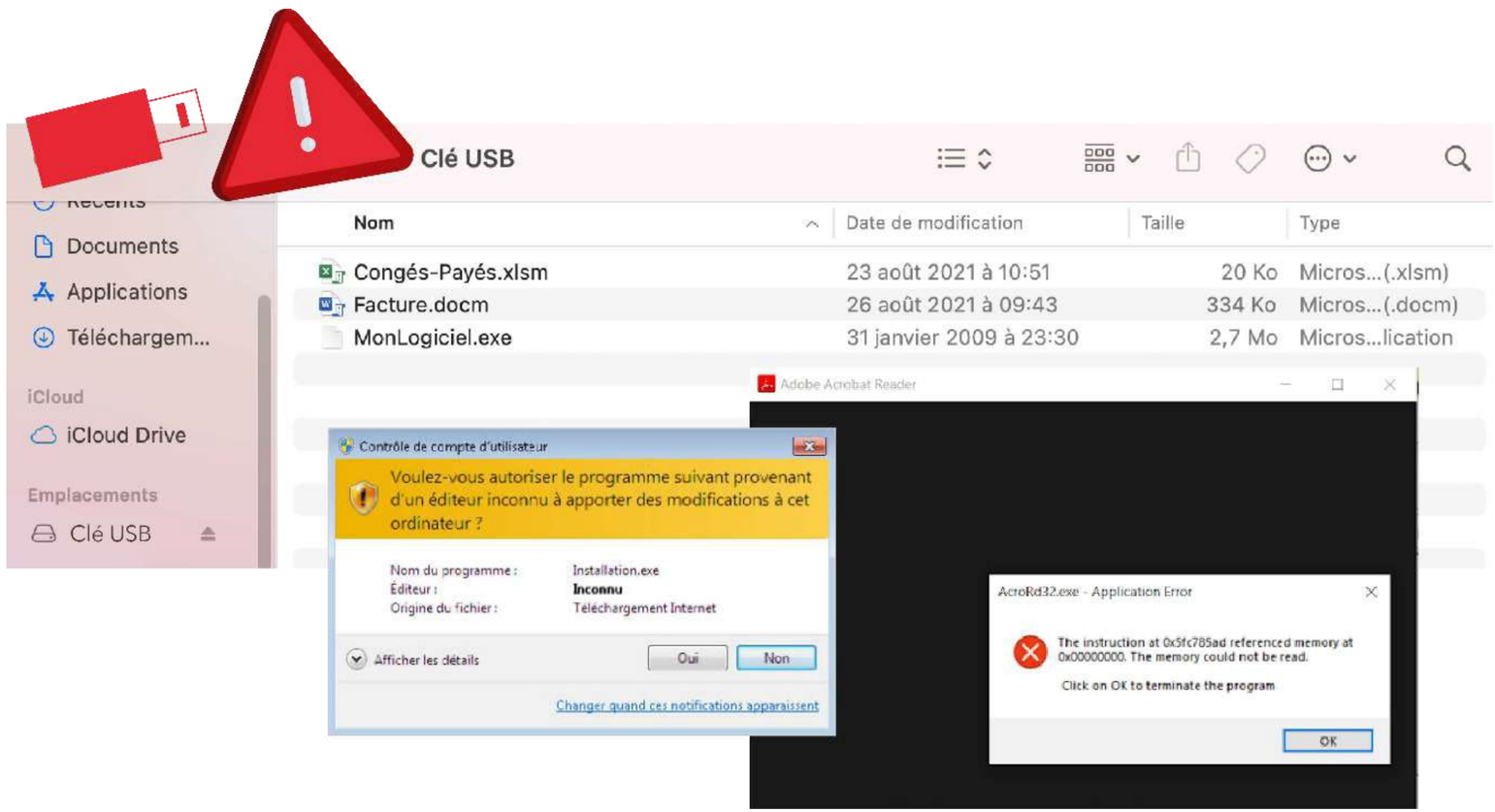
Au clic sur le lien du SMS, l'utilisateur est renvoyé vers une page de formation en ligne lui expliquant pourquoi il n'aurait pas dû cliquer.

APPRENTISSAGE PAR L'ACTION

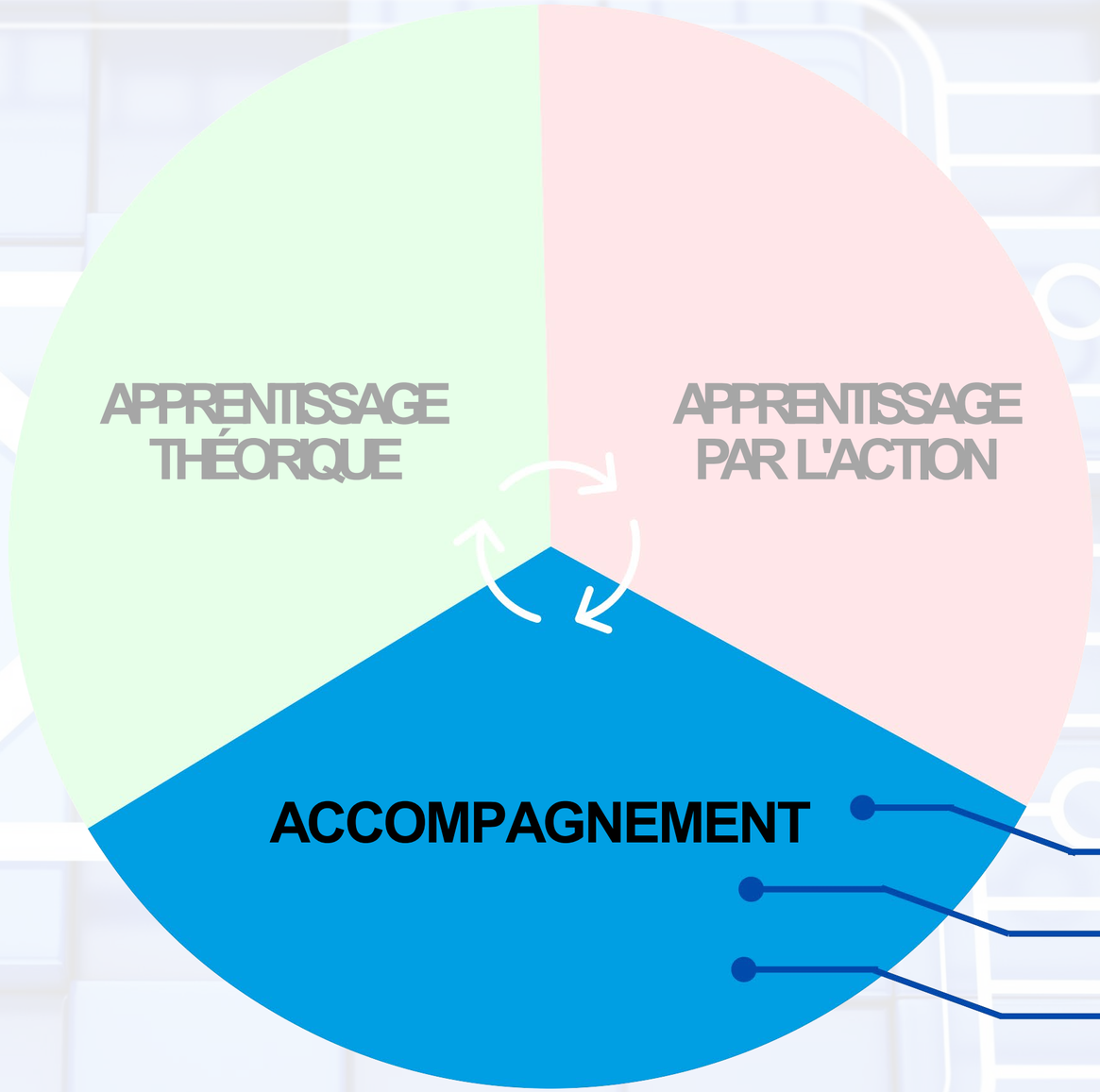
MISE EN SITUTATION : CLÉ USB

USB Awareness

Mise à disposition de faux fichiers pirates à déposer sur clé USB pour sensibiliser vos utilisateurs face aux risques d'utilisation de ces supports
Sensibilisation pédagogique de 3 minutes sur poste de travail



Troisième partie : l'accompagnement



- Tableau de bord
- Chargé de compte
- Actions spécifiques à votre organisation

ACCOMPAGNEMENT

TABLEAU DE BORD

Ce tableau de bord permet de documenter toutes les actions de sensibilisation mises en place.

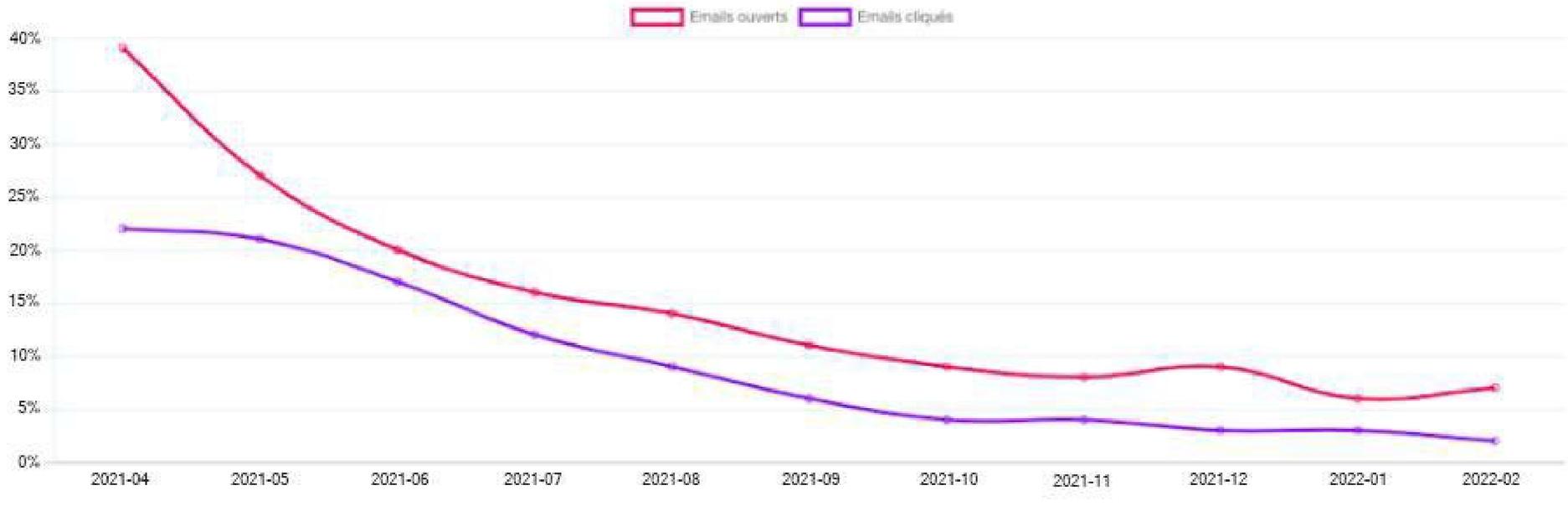
Niveau de risque

Emails

Emails envoyés	5169
Emails ouverts	817 (16 %)
Emails cliqués	516 (10 %)
Sensibilisations initiales	83 %
Sensibilisations sur l'instant	4423 / 5820 (76%)

Evolution des clics

Valeurs en %



ACCOMPAGNEMENT
SUIVI DE VOTRE CHARGÉ DE COMPTE

Un chargé de compte dédié vous accompagnera tout au long de la prestation afin de réaliser chaque mois :

- la restitution et suivi des résultats
- le suivi de l'évolution d'apprentissage des utilisateurs
- la mise en place de plans d'action d'améliorations des résultats

ACCOMPAGNEMENT PERSONNALISATION AVEC VOTRE CHARGÉ DE COMPTE

Après 2 mois d'utilisation de l'outil SaaS, ajouts d'attaques spécifiques en complément :

- spécifique à votre organisation et/ou secteur d'activité (type fraude au président)
- spécifique à un groupe d'utilisateurs en particulier
- création de templates personnalisés (contenu, signature, nom de domaine, formulaire spécifique...)

Mise en place

Mise en place rapide

J

Paramétrage de la plateforme

Moins de 500 utilisateurs --> 3 heures
De 500 à 2000 utilisateurs --> 5 heures
Plus de 2000 utilisateurs --> 1 journée

J+10 Lancement de l'audit sur 1 semaine

J+12 Plan de communication

J+15 Déploiement des outils favorisant la culture-cyber

J+22 Lancement des mises en situation sur la durée

La sécurité

- Le mot de passe de l'administrateur est hashé et changé tous les 180 jours.
- L'administration n'est accessible que via l'IP que vous nous indiquez.
- Test de pénétration réalisé régulièrement.
- Les données sont stockées en France et n'en sortent pas.
- La plateforme a été codée en prenant en compte les principes de privacy et de security by design. Tous les liens sont en https.
- Les intervenants n'ont accès qu'aux informations strictement nécessaires à l'accomplissement de leurs missions.
- A la fin du contrat, les données sont détruites de manière irréversible, ce que nous vous confirmons par l'envoi d'un recommandé avec accusé de réception.

Conçu, crée et hébergé en

Bulletin d'alerte du 31/01/19

- La fin d'année 2018 ainsi que le début d'année 2019 sont marqués par une recrudescence inédite des attaques de type rançongiciel.
- Cette profusion d'attaques est facilitée par la vente sur Internet de rancongiciels "prêts-à- l'emploi" (Ransomware-as-a-Service, RaaS)...
- Le choix des cibles est de plus en plus réfléchi [...], les attaques par rançongiciels actuelles sont plus souvent ciblées.
- Les rançons demandées sont [..] plus importantes qu'avant, oscillant entre 50000 et 170000 dollars (payables en cryptomonnaie).

https://www.cert.ssi.gouv.fr/alerte/CERTFR-2019-ALE-003

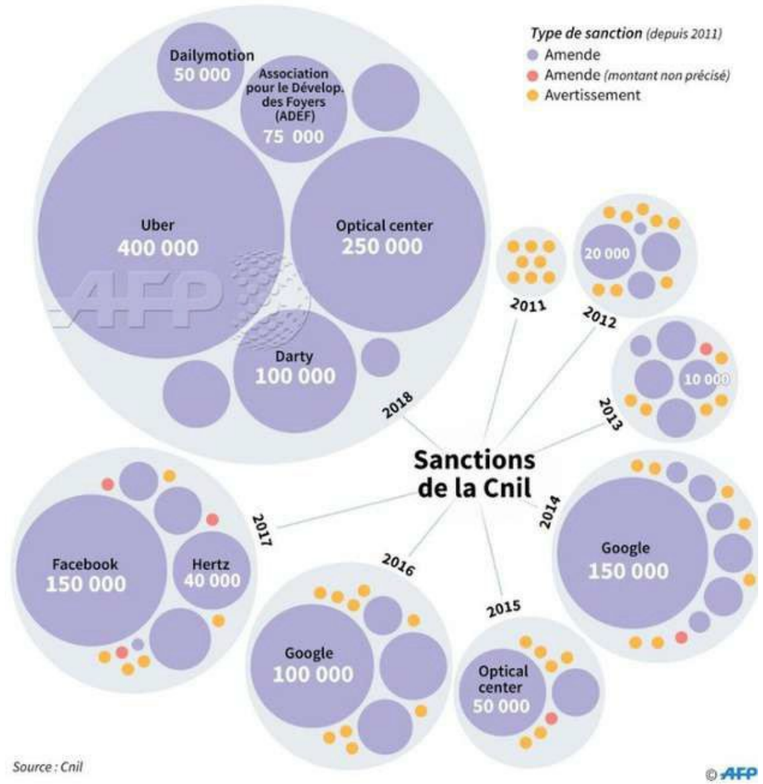
Solutions préconisées par l'ANSSI

- Assurer un bon niveau de sécurité
- Sensibiliser les utilisateurs
- Effectuer des sauvegardes

https://www.cert.ssi.gouv.fr/information/CERTFR-2017-INF-001/

Le cadre réglementaire et au delà

- Article 24, 25 et 32 du RGPD qui impose la mise en place de solutions organisationnelles de protection des données personnelles
- Risques d'amendes de la CNIL en cas de fuite de données



Pour résumer AvantdeCliquer.com L'humain au cœur de la cybersécurité c'est :

Efficace

Simplicité de mise en place

Solution non chronophage

Aucune installation chez vous

Télétravail

Montée en compétences personnalisée et adaptée à tout public

RGPD

Remontées qualifiées

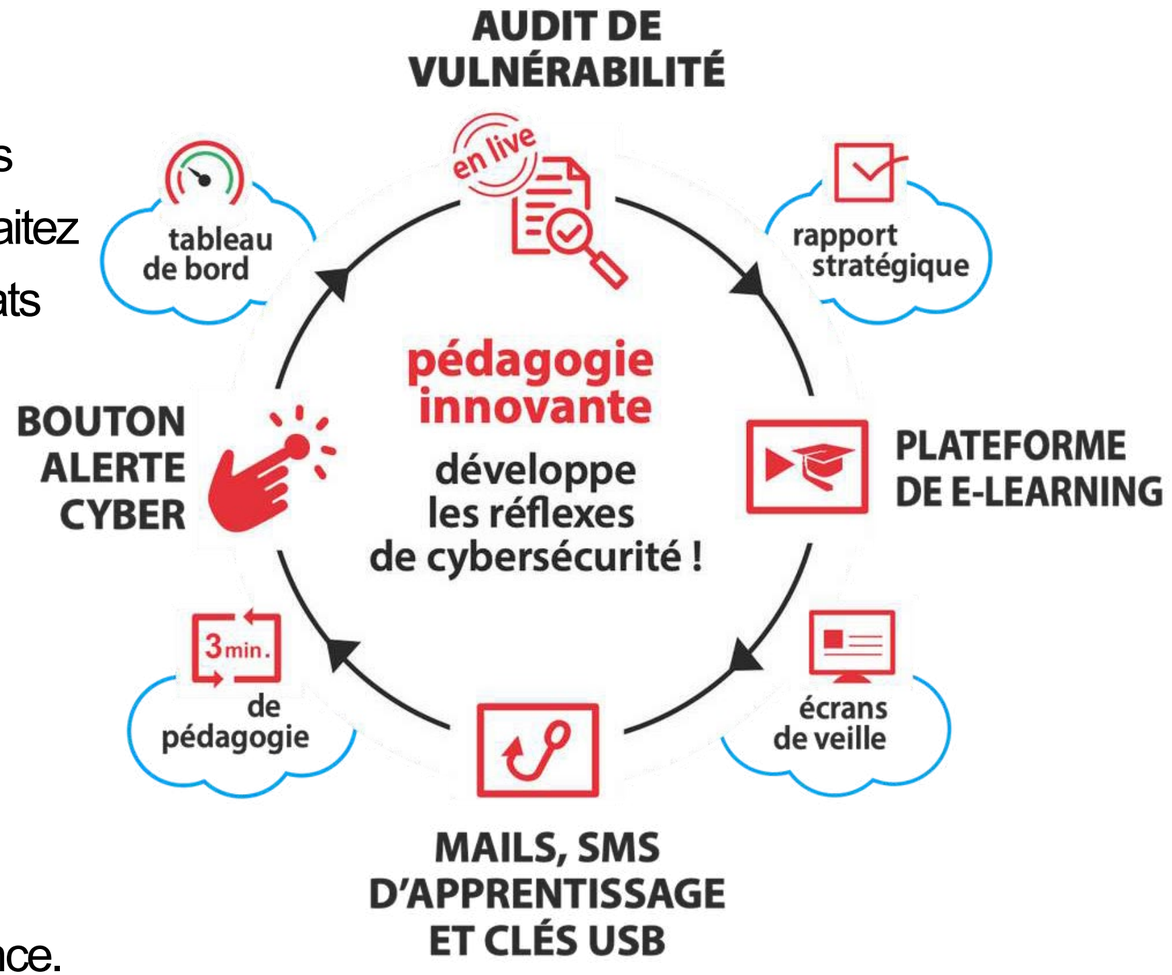
Sérénité

Utile dans la sphère privée

Sur la durée

Pour résumer AvantdeCliquer.com L'humain au cœur de la cybersécurité c'est :

- Démarrage immédiat
- Audit initial d'une semaine
- Restitution des résultats lors d'une visioconférence de 60 minutes
- Export des résultats via votre espace admin quand vous le souhaitez
- Accès à l'espace d'administration permettant de suivre les résultats individuels
- Montée en compétence de vos utilisateurs via des mises en situation réalistes en continu
- Plateforme d'e-learning
- Ecrans de veille
- Bouton de signalement d'alerte phishing (optionnel)
- Campagnes personnalisées
- Campagnes SMS et sensibilisation clé USB
- Accompagnement mensuel de 30 à 45 minutes en visioconférence.



CYBER CERCLE

CYBER SÉCURITÉ NORMANDIE

AUSY

AvantdeCliquer.com
L'humain au coeur de la cybersécurité

BANQUE des TERRITOIRES

cea

CERTitude NUMERIQUE

CYBER MALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

escrypt
SECURITY. TRUST. SUCCESS.

FORTINET

ANPP

ANSSI

APSSIS

EFCIS

APSSIS
Association Pour la Sécurité des SI de Santé

CESIN

POLICE NATIONALE
OFFICE CENTRALE DE LA POLICE JUDICIAIRE

DGA

Gendarmerie nationale

Références

AvantdeCliquer.com
L'humain au cœur de la cybersécurité

C.A.I.H.
Centrale d'Achat de l'Informatique Hospitalière

Référencé GouvTech

RÉPUBLIQUE FRANÇAISE

Éditeur référencé UGAP-SCC

UGAP

The 2022 French CYBER-SECURITY STARTUPS radar
By WAVESTONE & bpifrance Le Hub

FÉDÉRATION FRANÇAISE DE LA CYBERSÉCURITÉ
FFCYBER

FRANCE RELANCE

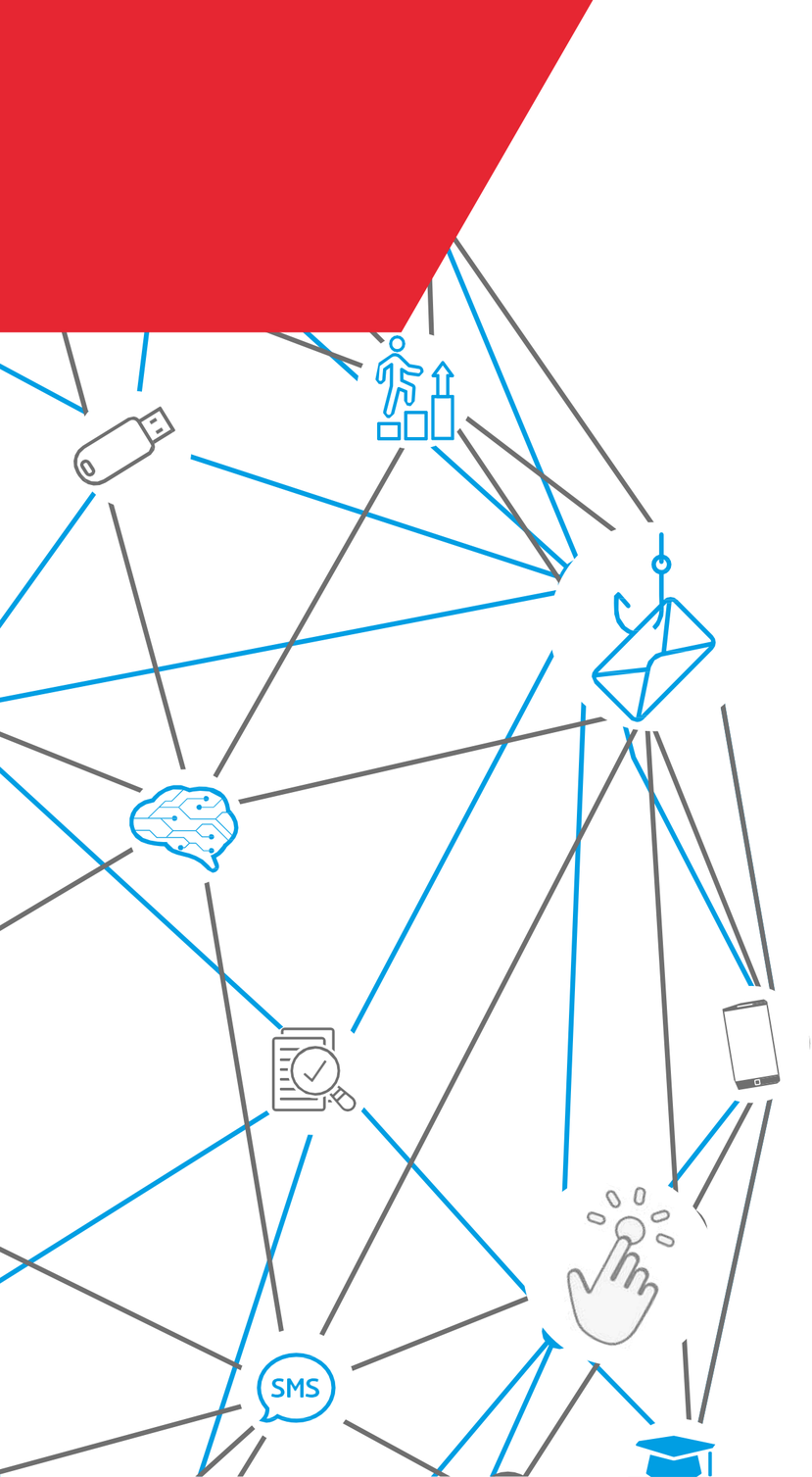
FRANCE CYBER SECURITY

Lauréat de l'intelligence économique
Trophées de l'agroalimentaire

BPI France
Solution pertinente pour sensibiliser les utilisateurs à la cybersécurité

Finaliste du prix de l'innovation du Salon des Maires et des Collectivités Locales

Lauréat de l'Innovation SANTEXPO
Transformation Digitale & Cybersécurité



AvantdeCliquer.com

L'humain au cœur de la cybersécurité

présentée au

SECURITY FORUM

Belgique 2022

Merci de votre attention