AvantdeCliquer.com
L'humain au cœur de la cybersécurité

DPO FORUM

80% DES CYBERATTAQUES ONT POUR ORIGINE UN E-MAIL FRAUDULEUX

La France est le 3ième pays le plus touché dans l'UE, d'après le baromètre du ransomware publié en janvier 2023.

En 2022, moins d'une entreprise sur 2 a subi une cyberattaque réussie cette année, une proportion en baisse par rapport à 2021 (- 9pts)

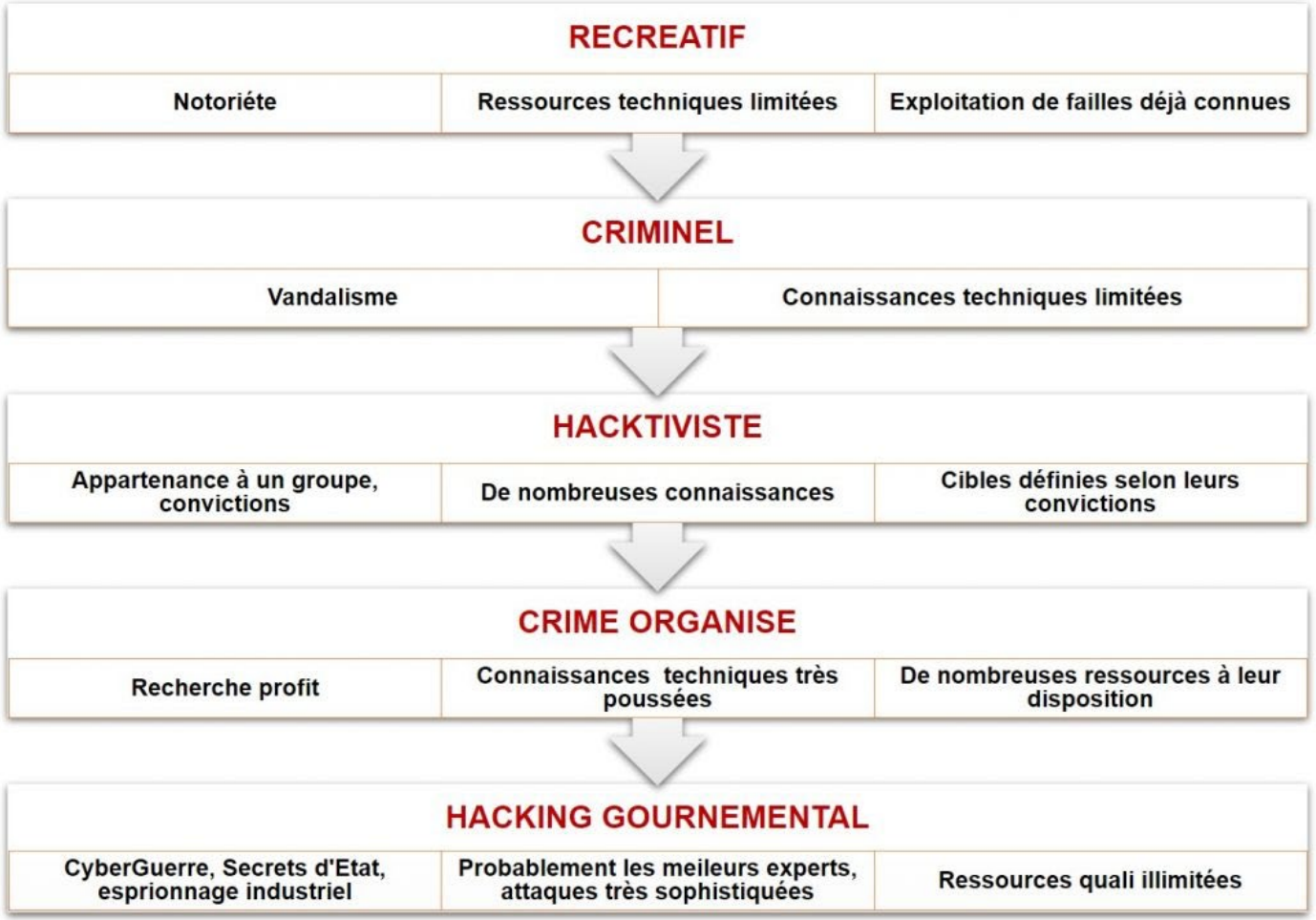
MENU Le Parisien S'ABONNER

High-tech

Vol de données : des hackers tentent de faire chanter Conforama

Le réseau de hackers ALPHV, aussi connu sous le nom de BlackCat, a annoncé avoir dérobé plus d'un térabit de données à Conforama. Le groupe français spécialiste de l'ameublement, qui a lancé une enquête en interne, affirme qu'il s'agit de documents anciens volés aux filiales espagnole et portugaise uniquement.

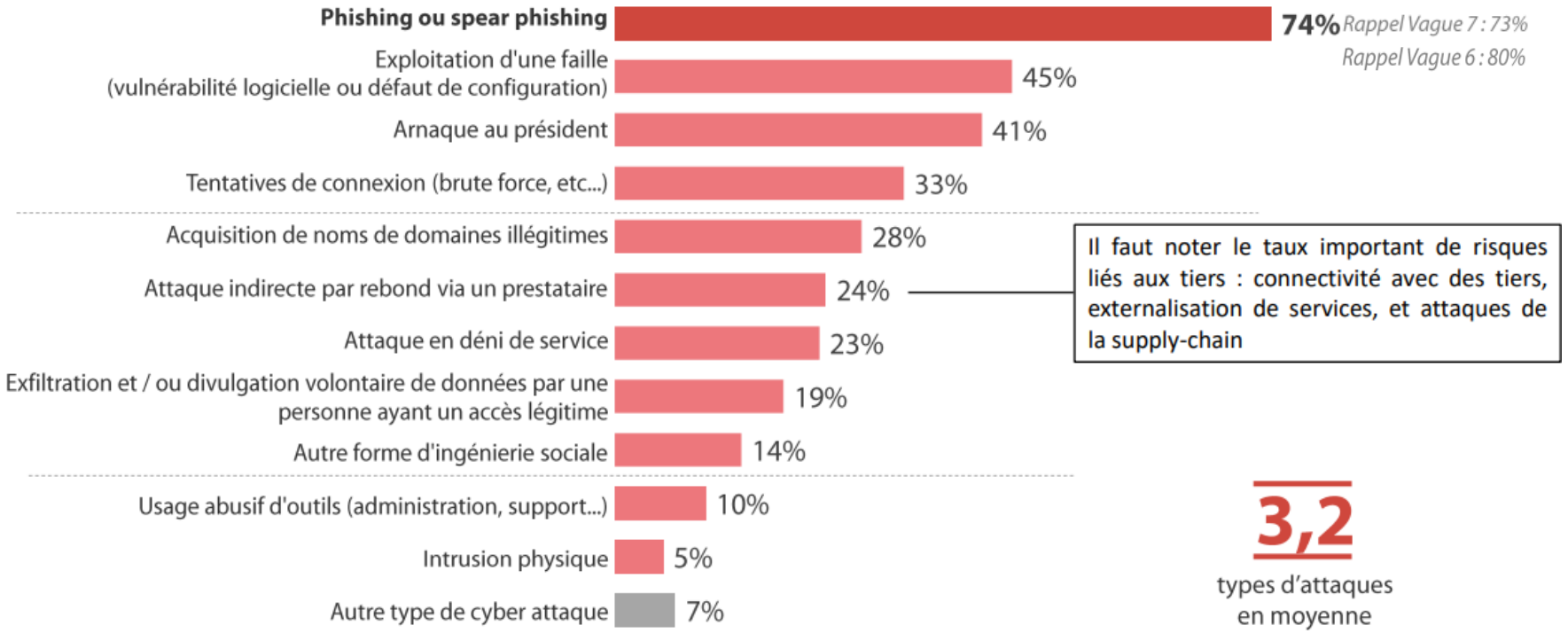
Qui sont les fraudeurs & pourquoi agissent-ils ?



Comment agissent-ils ?

Les entreprises ayant constatées au moins une attaque, en ont subi 3 en moyenne, le phishing ou spear phishing demeurant très nettement le principal vecteur

45% des entreprises ont subi au moins une cyberattaque en 2022



Il faut noter le taux important de risques liés aux tiers : connectivité avec des tiers, externalisation de services, et attaques de la supply-chain

3,2
types d'attaques en moyenne
parmi ceux ayant subi au moins une attaque

opinionway pour CESIN

Qu'est-ce que le Phishing ?

L'origine du mot Phishing : contraction de 2 mots anglais « phreaking » (piratage téléphonique) et de « fishing » (pêche).

Pratique en ligne malveillante et illégal utilisée par des fraudeurs :

- obtenir des renseignement et informations personnels ou professionnels
- but principal usurper une identité.

La technique consiste à :

- faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. —
- lui faire faire une action sur son poste de travail,
- soutirer des renseignements : mot de passe, numéro CB, numéro ou photocopie de la carte d'identité, informations sur l'entreprise, etc.
- soutirer de l'argent.

Comment reconnaître un e-mail de Phishing ?

Contexte de l'email

Vérifier si :

- E-mail personnel
- Quelque chose d'inhabituel
- Met mal à l'aise ou est à l'origine d'une montée d'adrénaline

Aspect général

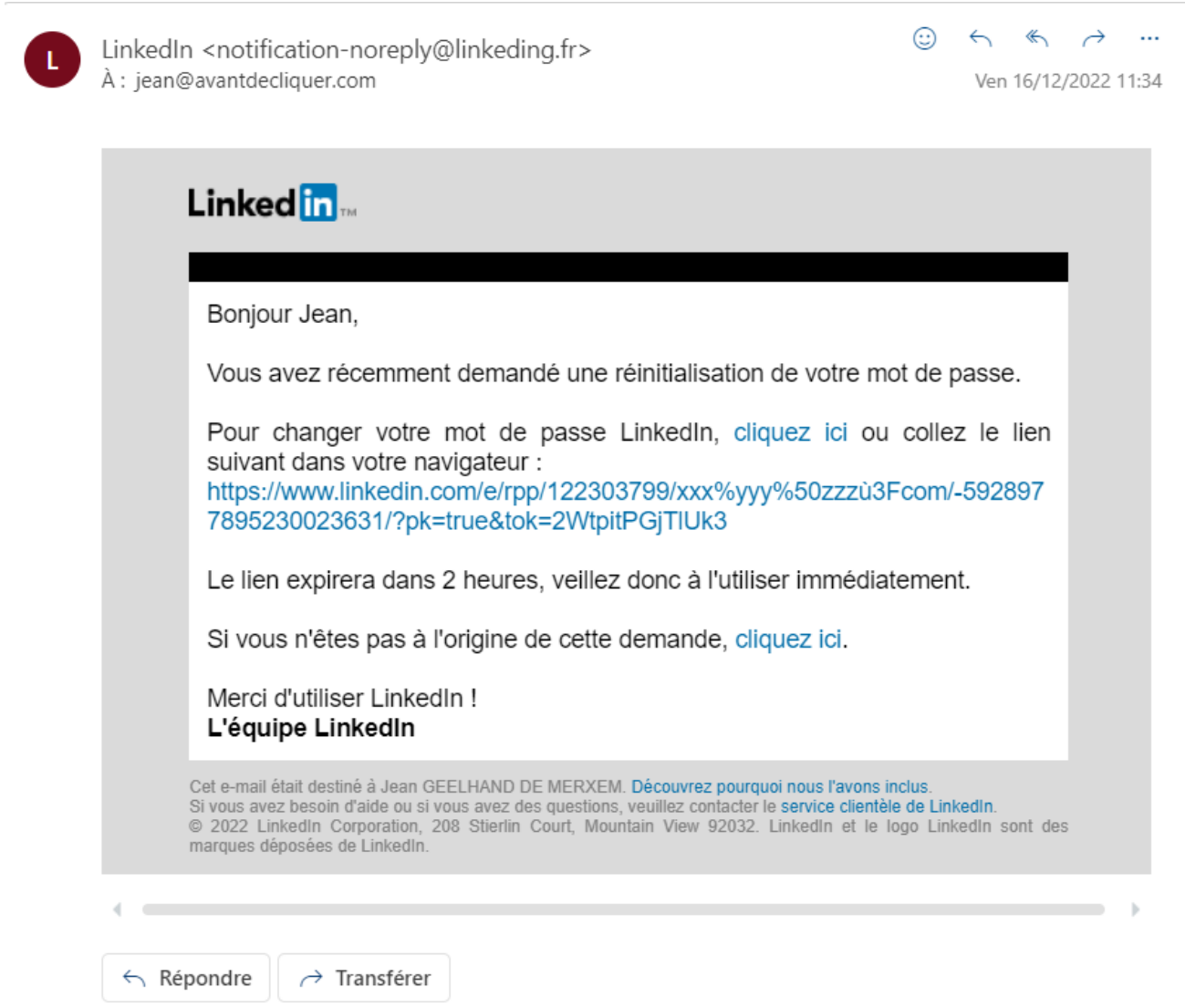
Vérifier si :

- Fautes d'orthographes
- Tournure d'une phrase qui fait pensé à de la traduction
- Pixélisation du logo pixelisé
- Adresse URL
- Expédition (nom de domaine)

ATTENTION les e-mails sont de mieux en mieux fait. Les fraudeurs ne manquent pas d'imagination pour vous faire cliquer

Exemple de phishing de masse :

Exemple de spear-phishing



LinkedIn <notification-noreply@linkeding.fr>
À : jean@avantdecliquer.com
Ven 16/12/2022 11:34

LinkedIn

Bonjour Jean,

Vous avez récemment demandé une réinitialisation de votre mot de passe.

Pour changer votre mot de passe LinkedIn, cliquez ici ou collez le lien suivant dans votre navigateur :
https://www.linkedin.com/e/rpp/122303799/xxx%yyy%50zzzù3Fcom/-5928977895230023631/?pk=true&tok=2WtpitPGjTlUk3

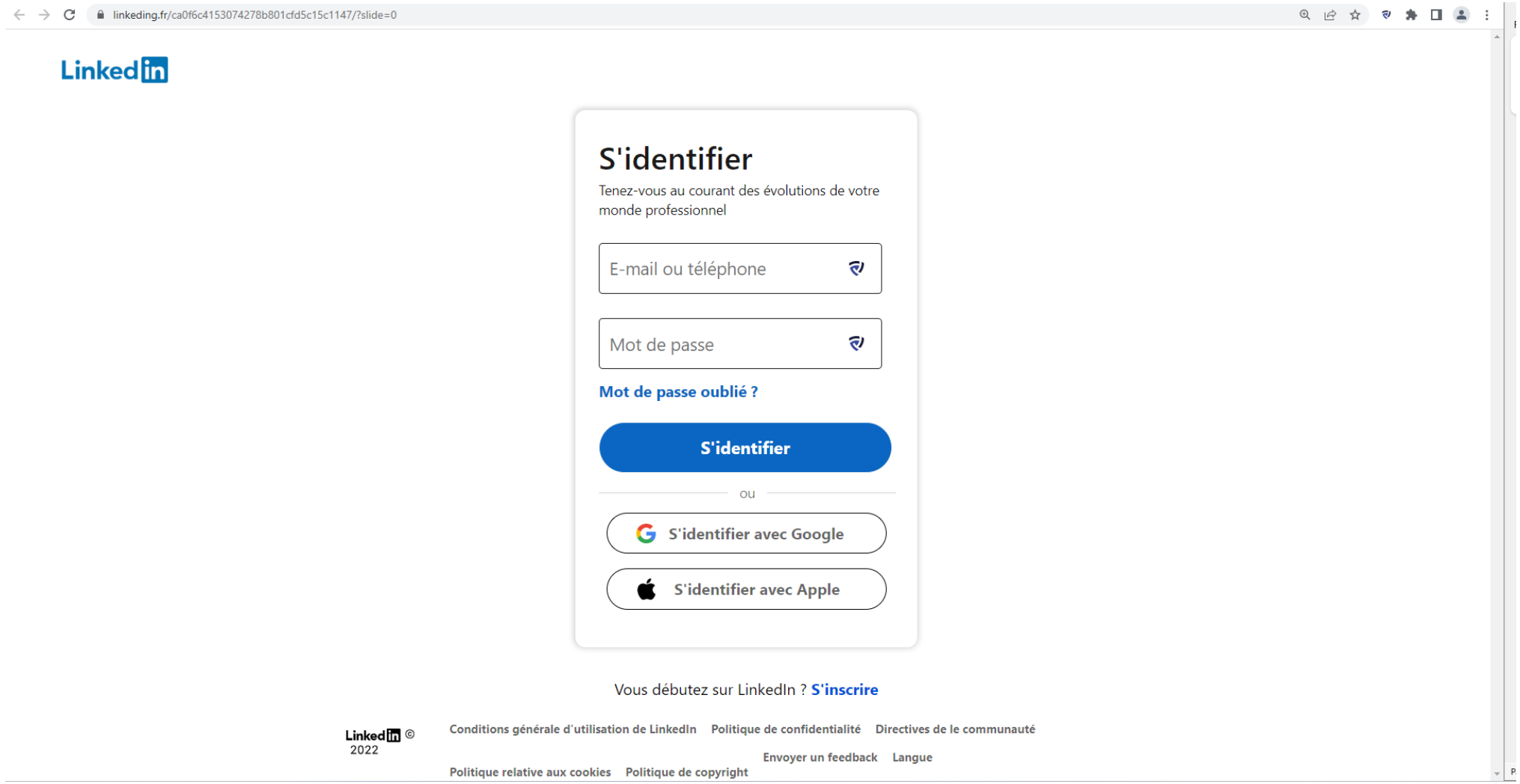
Le lien expirera dans 2 heures, veillez donc à l'utiliser immédiatement.

Si vous n'êtes pas à l'origine de cette demande, cliquez ici.

Merci d'utiliser LinkedIn !
L'équipe LinkedIn

Cet e-mail était destiné à Jean GEELHAND DE MERXEM. Découvrez pourquoi nous l'avons inclus.
Si vous avez besoin d'aide ou si vous avez des questions, veuillez contacter le service clientèle de LinkedIn.
© 2022 LinkedIn Corporation, 208 Stierlin Court, Mountain View 92032. LinkedIn et le logo LinkedIn sont des marques déposées de LinkedIn.

Répondre Transférer


linkeding.fr/ca0f6c4153074278b801cfd5c15c1147/?slide=0
LinkedIn
S'identifier
Tenez-vous au courant des évolutions de votre monde professionnel
E-mail ou téléphone
Mot de passe
Mot de passe oublié ?
S'identifier
ou
S'identifier avec Google
S'identifier avec Apple
Vous débutez sur LinkedIn ? S'inscrire
LinkedIn © 2022
Conditions générale d'utilisation de LinkedIn
Politique de confidentialité
Directives de le communauté
Envoyer un feedback
Langue
Politique relative aux cookies
Politique de copyright

Quelles sont les conséquences d'une cyberattaque ?

Rançongiciels
En France, le coût moyen d'une rançon avoisine les 130 000€.
En 2021, 25% des entreprises attaquées choisissent de payer.

Perte de confiance
des administrés, des partenaires, des équipes, des fournisseurs

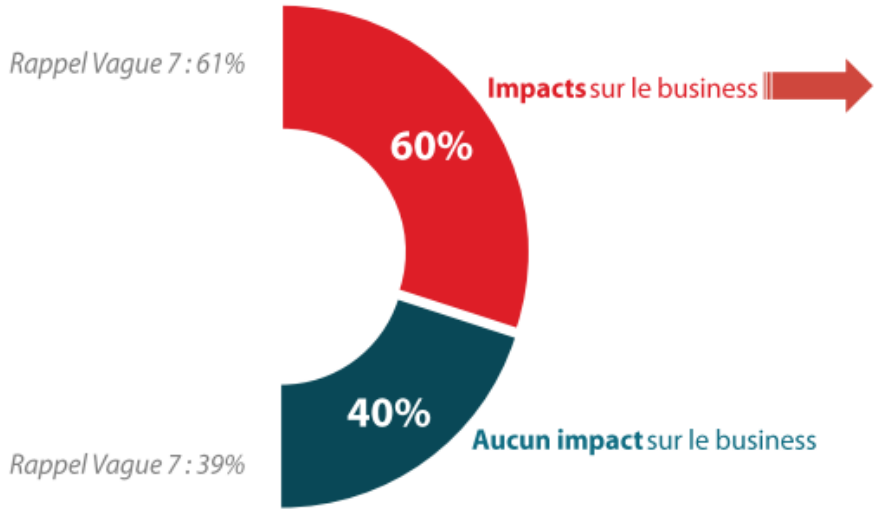
Fraude au président
Détournement de fonds

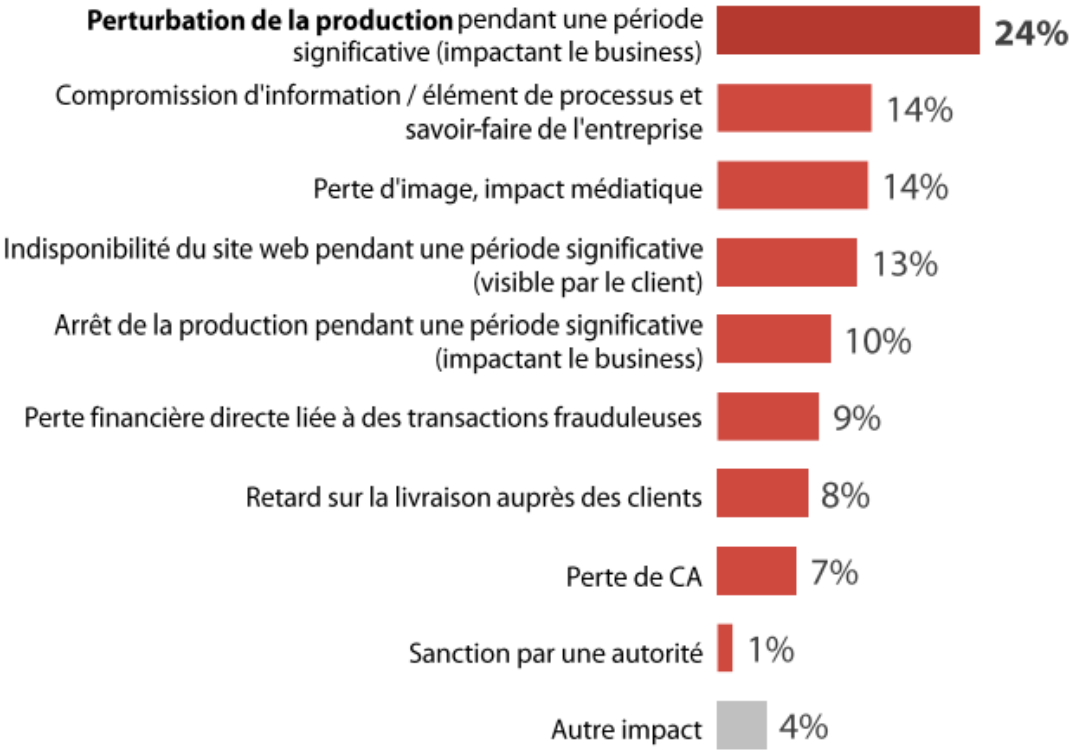
Patrimoine immatériel
Vol de méthodes, de brevets, d'informations confidentielles

Dégradation de l'image perte notoriété dans les médias de manière durable /

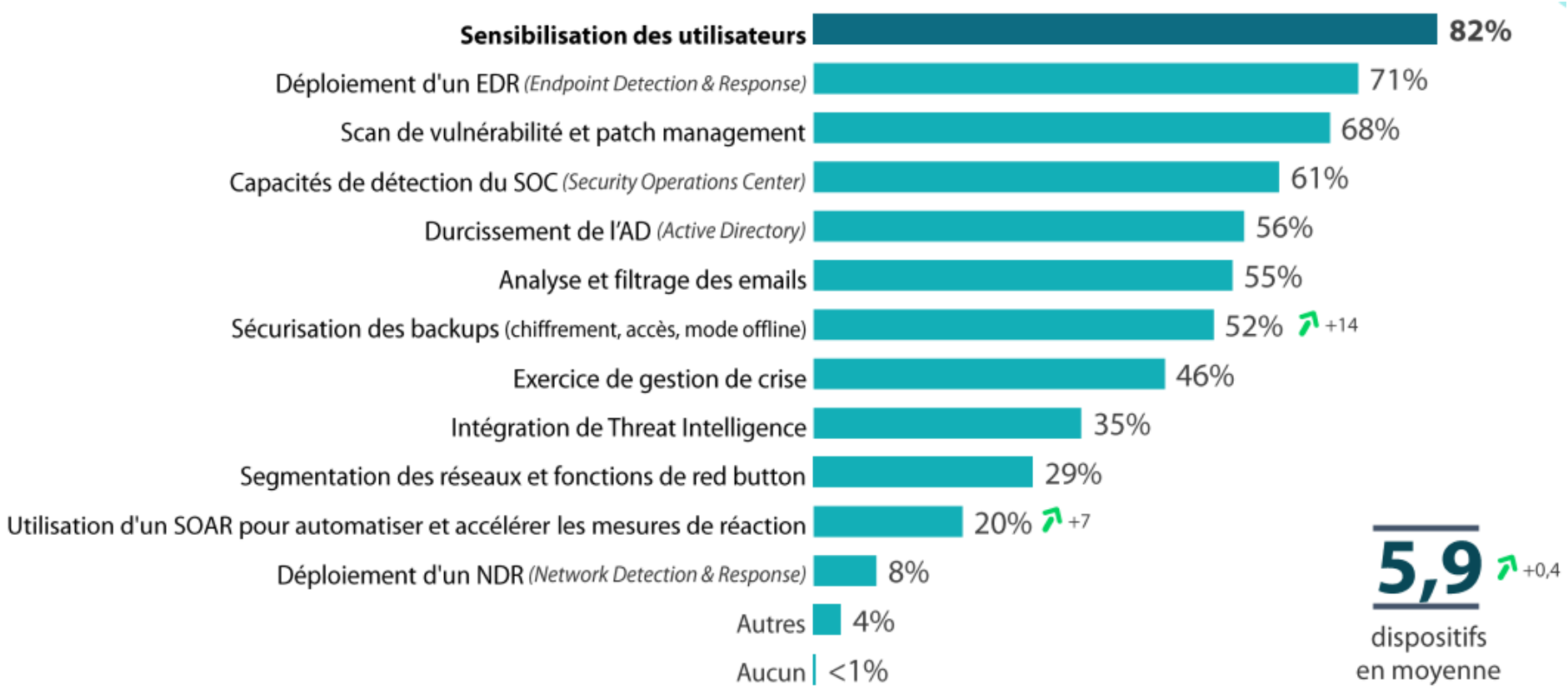
Déni de service
de la production, des expéditions, de la comptabilité, des paies...

Quelles sont les conséquences sur la production ?





Face au cyberattaque dominée par le ransomware, voici les dispositifs qui ont été renforcés :



Quel constat ? Quels impacts humains et financier ?

Attaques plus nombreuses, plus sophistiquées, plus redoutables. Les formes de Phishing évolue avec les avancés de la technologie.

Différentes méthodes d'ingénierie sociale : en plus du Phishing et Spear-Phishing

Le Vishing : appel téléphonique pour inciter transmettre des informations sensibles. Objectif : créer un sentiment d'urgence, ou de se faire passer pour une personne ayant autorité afin de donner à l'utilisateur l'impression qu'il n'a d'autres choix que de transmettre des informations

Le Smishing : incite les victimes sans méfiance à transmettre des informations sensibles via des messages SMS frauduleux. 2 attaques : Incitation à ouvrir une URL amenant à une page d'enregistrement d'informations d'identification frauduleuses ou à une page de téléchargement qui installe des logiciels malveillants / Incitation à appeler un numéro spécifié, en fonction du contenu du message. Conséquence : facture de téléphone surtaxée et élevée.

Pharming : Le pharming redirige simplement le trafic d'un site Web authentique vers une page usurpée apparemment identique, afin de voler les informations des visiteurs.

AvantdeCliquer
L'humain au cœur de la cybersécurité .com

DPO FORUM

Quel constat ?
Quels impacts humains et financier ?

Faillites de PME après une cyberattaque : ce n'est pas une légende

LISE CHARMEL

En France, l'exemple du fabriquant de lingerie Lise Charmel

Le 27 février 2020, la société Lise Charmel était mise en redressement judiciaire, à sa demande. La raison ? Une situation commerciale et financière très compliquée liée à une attaque par rançongiciel (ransomware) en novembre dernier. Le 8 novembre 2019 très précisément, tous les postes de travail et tous les fichiers de la société se sont en effet retrouvés bloqués, cryptés, par un pirate demandant une rançon en échange de la clé de déchiffrement. Cette « prise d'otage », comme le dit son dirigeant Olivier Piquet, a touché les 1 150 salariés du groupe, en France comme à l'étranger.

Cyberattaque : cet assureur français dit non au remboursement des victimes

Une décision qui devrait dissuader les victimes à payer les rançons.

Seine-Saint-Denis. Victime d'une cyberattaque, Bondy estime les dommages à 1,5 million d'euros

En novembre 2020, Bondy (Seine-Saint-Denis) avait été victime d'une cyberattaque. Depuis, la ville, qui a dû investir 1,5 million d'euros dans les réparations, n'est pas encore complètement remise de cette situation, comme le raconte son maire dans les colonnes d…

12/07

Une banque en ligne piratée, les données personnelles de 50 000 clients exposées

L'entreprise Revolut avait fait sa publicité sur ses systèmes de sécurité « primés », censés protéger l'argent de ses clients. Dimanche 11 septembre 2022, l'entreprise lettonne a dû admettre avoir été la cible d'une cyberattaque, exposant les données personnelles de 50…

22/09

Un hôpital d'Essonne victime de chantage aux données après une cyberattaque

Victime d'une cyberattaque en août, le Centre hospitalier Sud Francilien (CHSF) de Corbeil-Essonnes subit toujours un chantage aux données.

13/09

Comment se protéger ? 6 actes réflexes à pérenniser au sein d'une organisation.

1. SENSIBILISER VOS COLLABORATEURS
Actions de sensibilisation, acculturer et formez vos collaborateurs avec un code de bonnes pratiques et conduites.

2. GÉRER VOS MOTS DE PASSE
Individuel et confidentiel, mdp différent pour chaque usage, utilisation de coffre-fort ou gestionnaire de mdp, changé régulièrement de mdp tous les 3 mois par exemple.

3. METTRE À JOUR VOS APPAREILS, LOGICIELS ET VOS ANTIVIRUS
Activez et installez uniquement les MàJ automatique proposées par l'éditeur ou fournisseur, privilégiez 2 éditeurs d'antivirus différents pour les serveurs et postes de travail.

4. ÉVITER LES COMPORTEMENTS À RISQUE.
Ne jamais se connecter à un réseau public, séparez usage pro et perso. Ne pas ouvrir de pièces jointes, ne pas brancher de clés usb, ne pas cliquer sur un lien piégé.

5. SAUVEGARDER
Planifiez, déconnectez les supports, protégez et testez les sauvegardes.

6. METTRE EN PLACE DES GARDE-FOUS.
Restreindre l'accès à internet et sécurisez accès wifi et utilisez un VPN, bloquez les ports USB, mettez en place une authentification forte à multi facteurs.

Vous êtes décideur…

AvantdeCliquer.com permet aux DSI, RSSI, DPO et dirigeants de **réduire le risque** de cyberattaques de manière drastique. Au delà du développement d'une culture globale à la cybersécurité, la solution intègre un **accompagnement personnalisé pour les DSI, RSI et dirigeants**.

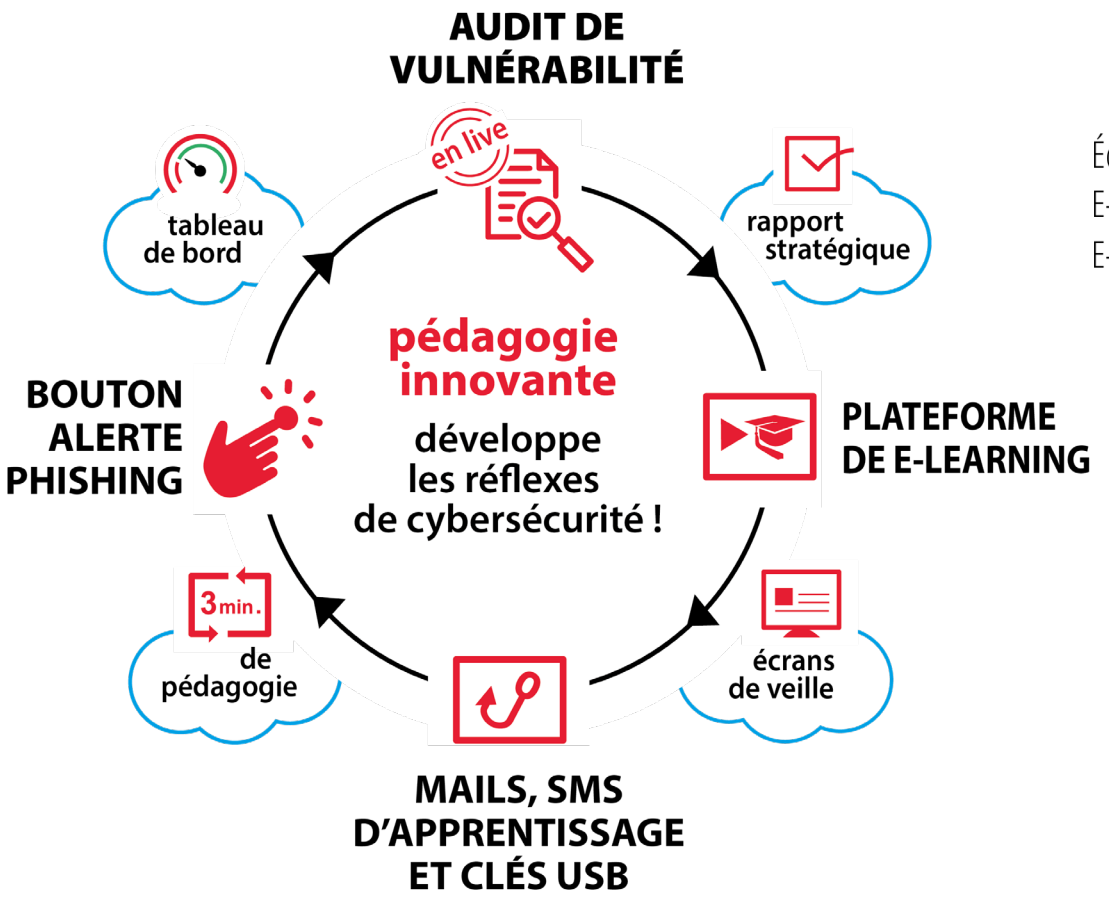
« Résultat : diviser /10 le risque de cyberattaques. »

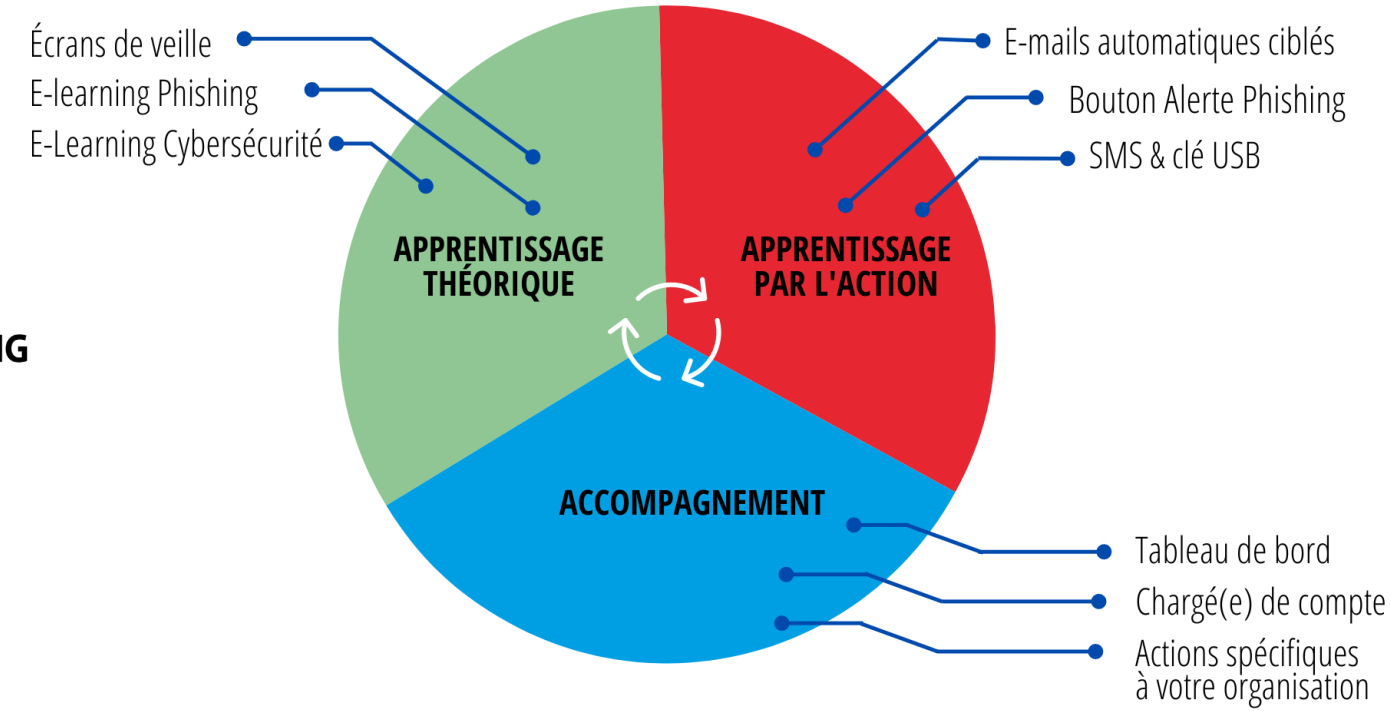
Le service informatique se dégage de la **tâche chronophage** que constitue la **sensibilisation au phishing.**

Les organisations respectent leurs obligations de mise en p de mesures organisationnelles **de protection des données personnelles du RGPD.**

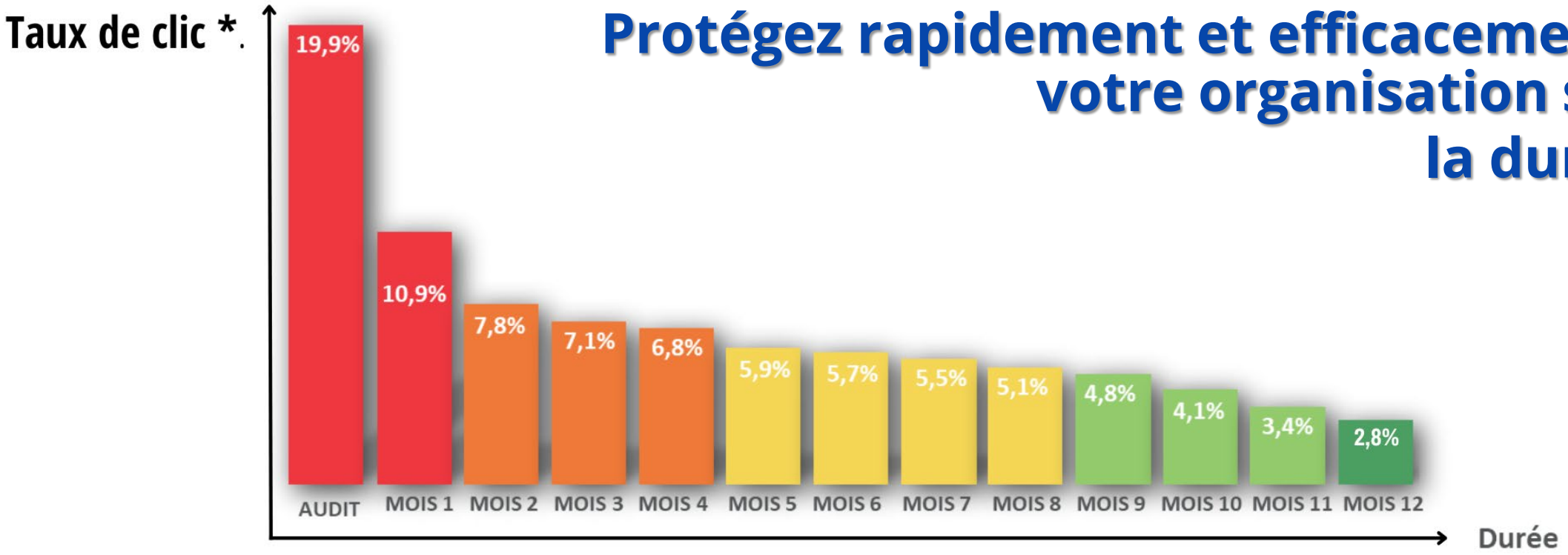
LA SENSIBILISATION À LA CYBERSÉCURITÉ RÉINVENTÉE QUI RÉDUIT DE MANIÈRE DRASTIQUE LE RISQUE DE CYBERATTAQUE

80% DES CYBERATTAQUES ONT POUR ORIGINE UN E-MAIL FRAUDULEUX


AUDIT DE VULNÉRABILITÉ
en live
tableau de bord
rapport stratégique
pédagogie innovante
développe les réflexes de cybersécurité !
BOUTON ALERTE PHISHING
PLATEFORME DE E-LEARNING
3 min.
de pédagogie
écrans de veille
MAILS, SMS D'APPRENTISSAGE ET CLÉS USB


Écrans de veille
E-learning Phishing
E-Learning Cybersécurité
APPRENTISSAGE THÉORIQUE
E-mails automatiques ciblés
Bouton Alerte Phishing
SMS & clé USB
APPRENTISSAGE PAR L'ACTION
ACCOMPAGNEMENT
Tableau de bord
Chargé(e) de compte
Actions spécifiques à votre organisation

Protégez rapidement et efficacement votre organisation sur la durée



* Moyenne réalisée en 2021 sur un ensemble de 500 000 utilisateurs tous secteurs confondus (privés ou publics) .

AvantdeCliquer
L'humain au cœur de la cybersécurité .com

Référencé GouvTech | RÉPUBLIQUE FRANÇAISE

DPO FORUM

Merci à tous pour votre attention

conçu / hébergé / développé en FRANCE

Mention Spéciale Expoprotection
Sureté-Sécurité et Cyberprévention

FÉDÉRATION FRANÇAISE DE LA CYBERSÉCURITÉ
FFCYBER

Lauréat de l'intelligence économique
Trophées de l'agroalimentaire

FRANCE RELANCE

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

FRANCE CYBER SECURITY

Lauréat de l'Innovation SANTEXPO
Transformation Digitale & Cybersécurité