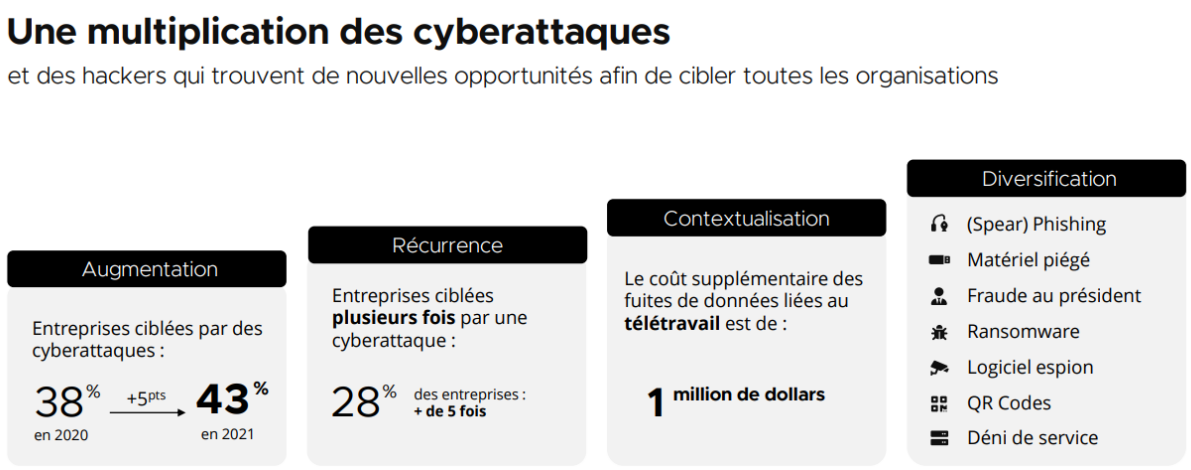
Formation de sensibilisation des collaborateurs face aux cyber risques

LE CONTEXTE :



Les couches de sécurité ne suffisent plus, puisque **90% des cyberattaques aboutissent suite à une erreur humaine**. Il faut traiter le facteur humain.

OBJECTIFS :

- Entrainer et former les collaborateurs aux cyberattaques, grâce à une méthode approuvée
- Apprendre à reconnaitre et à ne pas sous-estimer les risques des cyberattaques.
- Permettre un apprentissage par l'action de simulation d'attaques entièrement automatisé
- Réduire considérablement votre vulnérabilité

PUBLIC :

- ✓ Collaborateurs
- ✓ Responsable du traitement des données.
- ✓ DSI et RSSI.
- ✓ Chef de projet.
- ✓ Direction marketing.
- ✓ Juriste.
- ✓ Correspondant Informatique et libertés.
- ✓ Toute personne concernée par le traitement des données personnelles (RH, comptabilité…).

PEDAGOGIE

Alternance d'apports théoriques et pratiques
Simulation d'attaques
Support de cours et documents d'application remis en fin de formation
Évaluation des connaissances

LIEU

Formation en ligne

Durée : 1 an de formation en ligne

ELEMENTS DE CONTENU :

1. Le cadre légal en matière de protection de données personnelles

- ✓ Historique et contexte. Le cadre légal.
- ✓ Le rôle de l'autorité de contrôle (CNIL). Les contraintes

2. Les définitions et mots-clés

- ✓ Les définitions tels que 'phishing', 'ransomware'.
- ✓ Les participants apprendront un vocabulaire précis pour discuter des cybermenaces, en comprenant la signification des termes techniques, ce qui renforcera leur capacité à les détecter.
- ✓ Comprendre et Apprendre à se servir d'un programme de simulation d'attaques entièrement automatisé

3. Les principes fondamentaux

- ✓ La formation se concentre sur les principes fondamentaux de la sécurité informatique, offrant aux participants une base solide pour comprendre les menaces, les vulnérabilités pour protéger leur entreprise.
- ✓ Ils apprendront à ne pas sous-estimer les risques comme des pertes financières, une paralysie de l'activité, une baisse de la productivité, une dégradation de la réputation de votre structure, des vols de données.
- ✓ Cette formation fournit les bases essentielles pour développer une stratégie impactante.

4. Les acteurs

- ✓ Les acteurs internes. Les acteurs externes
- ✓ La responsabilité des acteurs

5. Les droits des personnes concernées

- ✓ Le droit à l'information
- ✓ Le droit d'accès
- ✓ Le droit de rectification
- ✓ Protéger les droits des individus touchés par les cyberattaques

6. Contribuer à la démarche de conformité de mon organisme

- ✓ Large choix de contenus basés sur de vraies cyberattaques
- ✓ Un apprentissage par l'action
- ✓ Simulation d'attaques entièrement automatisé
- ✓ Programmation des campagnes au bon moment et en illimité
- ✓ Ciblez les collaborateurs les plus vulnérables

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE

Mohatra est certifié auprès de Qualiopi. La société met tout en œuvre pour répondre aux normes et aux professionnalismes des organismes deformation.

Numéro de déclaration d'activité (NDA) : **75331204133**

SIRET : 821 596 087 00055