CYBER MOIS

ObjectifCyber

Appliquez nos conseils avant qu'il ne soit trop tard !

source : www.cybermalveillance.gouv.fr.

Quietic

Problèmes

Ces dernières années, les entreprises ont été les cibles de très nombreuses cyberattaques. Si une prise conscience collective commence à s'opérer, il reste encore beaucoup à faire pour atteindre un bon niveau de sécurité et démystifier ce sujet.

CYBER MOIS

Quietic

Intérêt

Obscure pour certains, anxiogène pour d'autres, **la cybersécurité est encore trop souvent perçue comme une contrainte** et comme un sujet uniquement technique. Mais si l'aspect technologique est essentiel pour assurer la cybersécurité des entreprises, la partie humaine ne doit pas être minimisée pour autant.

Connaître les bonnes pratiques

Nous le voyons chaque jour à travers les demandes d'assistance de vos collaborateurs, la plupart des attaques ciblent l'humain. Et nombre d'entre elles peuvent être évitées avec une sensibilisation efficace aux risques numériques et un apprentissage des bonnes pratiques au quotidien.

Solution

C’est pourquoi nous vous avons proposé durant toute cette année une méthodologie de sensibilisation en 4 étapes :

- ✓ **Des vidéos pour s’initier au sujet**
- ✓ **Des fiches complètes pour développer ses connaissances**
- ✓ **Des quiz pour se tester**
- ✓ **Des mémos pour retenir l’essentiel**

5 clés pour une sensibilisation réussie.

Faire face aux crises, c’est s’y préparer. Toutes les actions présentées dans ce guide sont autant de clés permettant d’augmenter l’immunité de votre entreprise face aux risques de cyberattaques. La cybersécurité est l’affaire de tous.

CYBER MOIS

Quietic

les 5 clés

01

Prendre conscience du risque cyber

L’objectif est de prendre conscience des risques, des impacts immédiats en cas de manquement aux bonnes pratiques.

02

Impliquer toute l’entreprise

Les dirigeants et les collaborateurs sont tous concernés !

03

S’appuyer sur les bonnes ressources pédagogiques

Renforcer les messages et personnaliser sa communication

04

Répéter et décliner les messages

La mémorisation passe par la répétition !

05

Vérifier l’assimiliation des messages

Testez la thérorie... et la pratique.

Clé n°1: prendre conscience du risque cyber

Comprendre les impacts d’une cyberattaque

Il suffit d’une seule intrusion dans un système informatique pour :

LA PERTURBATION DES SERVICES DE L’ENTREPRISE VOIRE L’ARRÊT TOTAL

L’INACCESSIBILITE OU LA DESTRUCTION DE FICHIERS

UN EFFET DOMINO AVEC DES DOMMAGES POUR LES CLIENTS ET FOURNISSEURS DE VOTRE ENTREPRISE

DES PERTES FINANCIERES
UNE ATTEINTE À L’IMAGE
DES RISQUES JURIDIQUES

CYBER MOIs Quietic

Reconnaître les usages à risques

En effet : un seul clic sur un lien malveillant, le téléchargement d'une pièce jointe infectée ou encore, la réutilisation d'un mot de passe tombé entre de mauvaises mains, peuvent ainsi avoir de graves conséquences.

Top 3 des attaques

Ransomware, phishing et piratage de compte constituent le top 3 des attaques auprès des entreprises. Des techniques qu'il convient de comprendre et de faire connaître à tous les collaborateurs pour mieux les appréhender et les former sur les gestes essentiels de sécurité.

Quietic

Clé n°2: impliquer toute l'entreprise

Une cyberattaque est souvent le fait d'une négligence humaine. Il suffit parfois d'une simple erreur pour rendre toute une entreprise vulnérable. Si chacun en est conscient, alors, chacun à son niveau peut être acteur et contribuer à protéger son entreprise, notamment en adaptant son comportement.

Adopter les bons réflexes

Une fois que tout le monde a pris conscience des risques cyber et des impacts encourus par l'entreprise, il devient plus légitime d'introduire les règles à suivre ou les bons réflexes à adopter. Ainsi, en cas de doute face à une situation à risque ou inhabituelle, voici quelques conseils :

- **être vigilant et ne pas prendre en main seul le problème éventuel**
- **contacter immédiatement Quietic**

CYBER MOIS Quietic

Atteindre vos collaborateurs

Afin d’optimiser la démarche de prévention au sein de votre entreprise, tous les collaborateurs (quelle que soit la taille de l’entreprise) doivent être régulièrement sensibilisés à travers :

- différents messages et relais de communication
- des témoignages de collègues pour savoir comment d’autres réagissent
- des supports et visuels originaux pour les interpeler

Quietic

Identifier votre champion.ne de la comm’

Toutes les entreprises ne bénéficient pas nécessairement d’un directeur de la communication pour les aider à conduire des campagnes de sensibilisation. L’idéal ? Identifier un collaborateur ou une collaboratrice qui se sent à l’aise pour communiquer sur le sujet !
Et qui pourra partager tous les supports directement dans votre Teams !

Quietic

Clé n°3: s’appuyer sur les bonnes ressources pédagogiques

Tous les collaborateurs ont besoin d’être “nourris” régulièrement de contenus illustrant les exemples à retenir et ce qu’il ne faut pas faire !

Personnaliser sa communication

- **Choisir les bons contenus et calibrer le ton à utiliser, des contenus toujours anxiogènes peuvent avoir pour effet de lasser vos collaborateurs...**

- **Sélectionner les bons canaux de diffusion : réunion, affichage, intranet, Teams... (et oublier l’email car c’est le principal vecteur d’attaque, donnez l’exemple !)**

CYBER MOIs Quietic

Clé n°4: décliner et répéter les messages

Le défi est de réussir à répéter sans lasser ses collaborateurs afin d'entretenir l'intérêt pour le sujet, tout en développant leur culture cyber.

Elaborer un plan d'action

Définir des actions ou des temps forts en échelonnant les communications dans le temps. Vous verrez c'est particulièrement efficace.

Donner vie à la sensibilisation

Utiliser des illustrations, qu'il s'agisse de photos ou vidéos pour mettre en avant des exemples, des initiatives ou des témoignages .
Par ailleurs, utiliser des métaphores comme le domaine médical pour expliquer l'hygiène numérique et les bons réflexes à adopter en matière de cybersécurité, ça fonctionne plutôt bien !

CYBER MOIS Quietic

Clé n°5: vérifier l’assimilation des messages

Pour s’assurer de l’efficacité de votre communication, Il est utile de vérifier régulièrement la bonne compréhension des messages et leur mise en pratique.

Confronter les retours d’expérience

Pour mesurer la compréhension des messages, des moments d’échanges peuvent être organisés sur les thématiques abordées dans la sensibilisation. L’opportunité de revenir sur des notions ou réflexes à suivre qui auraient pu être mal compris et si besoin, d’adapter des comportements pour suivre les bonnes pratiques.

CYBER MOIs

Quietic

A vous de sensibiliser !

en Octobre c’est le Cybermois !

Lancez-vous de manière concrète !

- Expliquez le contexte et les objectifs de la démarche cyber de votre entreprise à vos collaborateurs, c’est l’occasion idéale !
- Informez vos collaborateurs que vous allez communiquer régulièrement sur le sujet. Devenez le porte-voix de la cybersécurité dans votre entreprise !

Toute l’équipe Quietic est là pour vous accompagner dans votre démarche de prévention numérique !

Quietic