Prévenir les turbulences : cybersécurité dans le voyage connecté

Comment réduire le risque et protéger vos clients.

par Serge Houtain

Mettre en place une prévention efficace

Sécurité des données et réglementations

Assurer la conformité et la protection des informations sensibles

Sécurisation des transactions

Garantir la sécurité des paiements et des échanges en ligne

Protection des accès

Sécuriser les comptes et gérer les droits d'accès

Formation du personnel

Sensibiliser et former les équipes aux bonnes pratiques

Politique de confidentialité

Maintenir la transparence et la confiance avec la clientèle

Gestion de crise

Préparer un plan d'action et disposer d'une assurance adaptée

Amélioration continue

Assurer une veille et adapter les mesures régulièrement

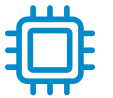
Difficultés rencontrées

Aspects réglementaires

- Complexité des exigences légales et réglementaires (**RGPD, PCI-DSS, NIS2**, ...)
- Protection et sécurisation des données

Ressources et compétences

- Manque de ressources et de compétences internes
- Gestion de la réputation et de la communication



Défis techniques

- Évolution rapide des technologies et des menaces
- Continuité de service et gestion des pics de trafic

Les 13 questions à se poser

Infrastructure & Sécurité technique

- Avez-vous une connaissance exhaustive de votre parc informatique et de vos actifs métier ?
- Appliquez-vous régulièrement les mises à jour des logiciels et des systèmes d'exploitation ?
- Utilisez-vous un antivirus ou un anti-malware ?
- Avez-vous activé un pare-feu et en connaissez-vous les règles de filtrage ?

Protection des données

- Effectuez-vous des sauvegardes régulières ?
- Avez-vous implémenté une politique d'usage de mots de passe robustes ?
- Comment sécurisez-vous votre messagerie ?
- Envisagez-vous d'utiliser des solutions cloud ?

Organisation & Gestion des risques

- Comment séparez-vous vos usages informatiques ?
- Comment maîtrisez-vous le risque numérique en situation de nomadisme ?
- Comment vous informez-vous et comment sensibilisez-vous vos collaborateurs ?
- Avez-vous fait évaluer la couverture de votre police d'assurance au risque cyber ?
- Savez-vous comment réagir en cas de cyberattaque ?

Vous êtes le premier pare-feu : soyez vigilant(e)

70%

Facteur humain

Le facteur humain représente la majorité du risque cyber

90%

Attaques par phishing

La grande majorité des attaques commencent par un e-mail malveillant

La fraude au président (Fraude CEO, FOVI, …)

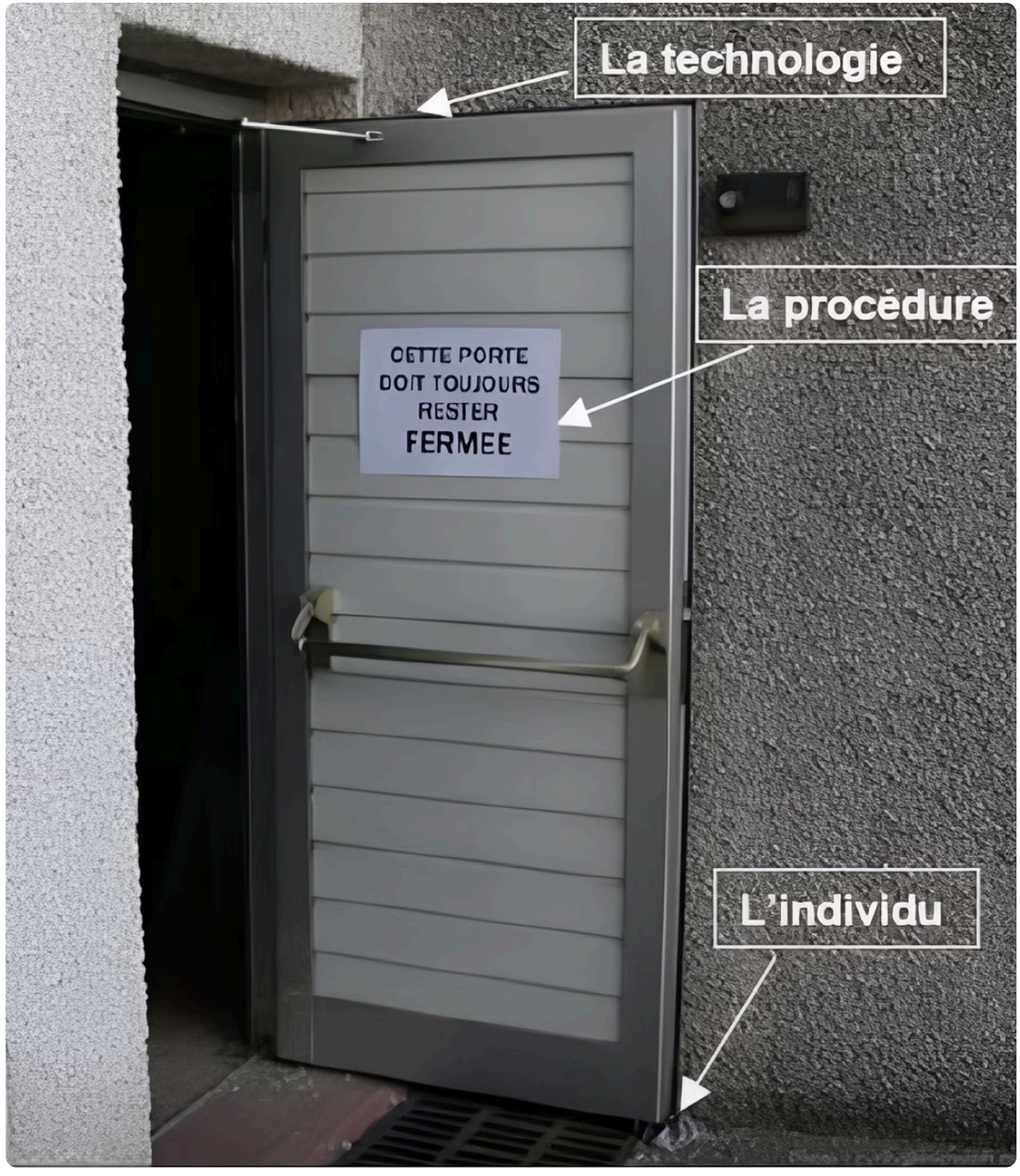
HAINAUT

160.000 euros volés à l'office du tourisme de Mons : un cybercriminel exploite le phishing et l'usurpation d'identité

06 oct. 2024 à 15:30 • 1 min

Le piège s'est refermé, dans l'atmosphère feutrée des bureaux de l'office du tourisme de Mons. Une simple demande de virement. Puis une autre. Et encore une. Par quatre fois, des virements d'une somme vertigineuse, 160.000 euros au total, ont quitté les caisses de l'office. L'expéditeur ? Natacha Vandenberghe, directrice de l'office. Enfin, c'est ce que croyait l'employée qui a obéi sans hésitation. Mais voilà, les demandes émanaient en fait d'un habile usurpateur, un maître du phishing, jouant de l'identité de la directrice pour mieux berner sa cible.

Métaphore (mais pas que…)



Sensibilisation et formation

Formation des employés

Programmes de sensibilisation dédiés pour le personnel des agences de voyages et plateformes touristiques

Collaboration partenaires

Diffusion et partage des bonnes pratiques de cybersécurité avec l'ensemble des sous-traitants et partenaires

Culture de sécurité

Développement d'initiatives pour renforcer la culture cybersécurité à travers toute la chaîne de valeur

Les **employés** et les partenaires constituent **la première ligne de défense** dans la prévention des incidents de cybersécurité.

La Région Wallonne vous aide

Aperçu du soutien

La Région wallonne propose des chèques-entreprises "cybersécurité" pour les TPE/PME.

- Des audits et diagnostics de cybersécurité
- L'accompagnement dans la mise en œuvre de politiques de sécurité
- La labellisation et l'évaluation de la sécurité informatique

Conditions de financement

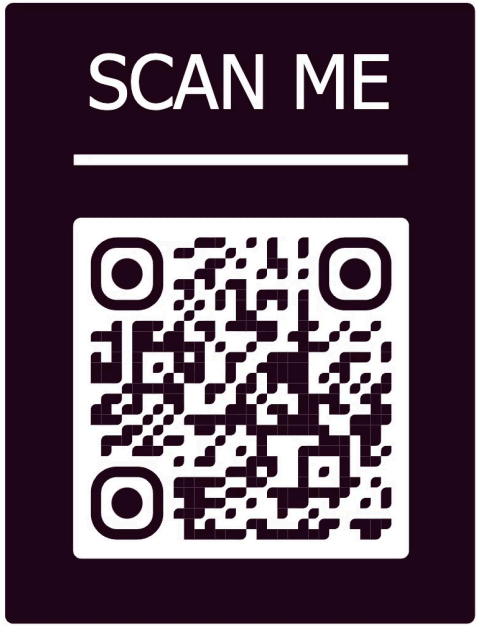
- Couverture de 75% des honoraires du consultant/prestataire (hors TVA)
- Plafond de 50 000€ par bénéficiaire sur 3 ans
- Maximum de 70 000€ pour la thématique "Numérique" sur 3 ans
- Limite globale de 100 000€ par année civile tous chèques confondus

Critères d'éligibilité

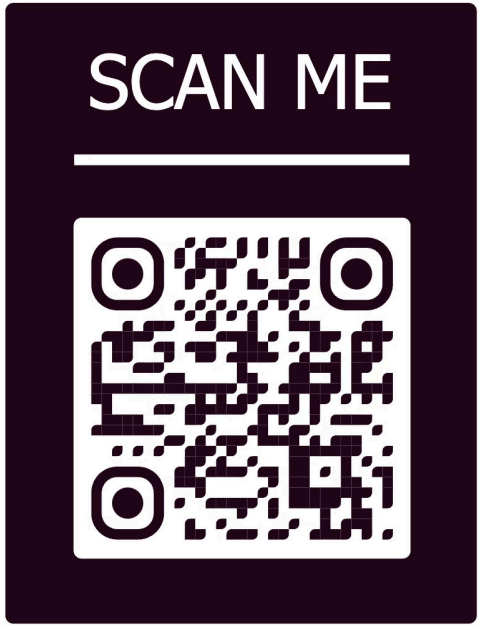
- Être une PME (moins de 250 employés et chiffre d'affaires annuel inférieur à 50M€)
- Avoir son siège d'exploitation principal en Wallonie
- Ne pas être une ASBL
- Ne pas opérer dans les secteurs exclus (pêche, agriculture, etc.)

Ressources web

Analyse gratuite de votre site web par SafeOnWeb@atwork



SafeOnWeb (Conseils, documentation)



Chèques Entreprises Région Wallonne

Merci de votre attention !