L'AUGMENTATION ALARMANTE DU PHISHING EN SUISSE ROMANDE

IMPACTS SUR LES PME ET SOLUTIONS DE PRÉVENTION

TESWEB SA

PUITS GODET 10, 2000 NEUCHÂTEL, SUISSE

WWW.BEXXO.CH

Avec la contribution et l'expertise de

Introduction

Le phishing, ou hameçonnage en français, représente une menace cybernétique en croissance exponentielle en Suisse, touchant particulièrement les petites et moyennes entreprises (PME) en Suisse romande. Ce livre blanc examine l'état actuel du phishing dans la région, met en lumière les statistiques nationales et cantonales préoccupantes, identifie les cibles privilégiées au sein des PME, et présente des cas concrets d'attaques. Il analyse également la perception souvent sous-estimée du risque par les PME et leur niveau de préparation face à ces menaces. Enfin, sur la base des recommandations des autorités suisses, il propose des bonnes pratiques essentielles et introduit le logiciel **PhishTrainer** comme un outil concret et efficace pour sensibiliser et former le personnel, renforçant ainsi la première ligne de défense humaine de l'entreprise face au risque d'hameçonnage.

Table des matières

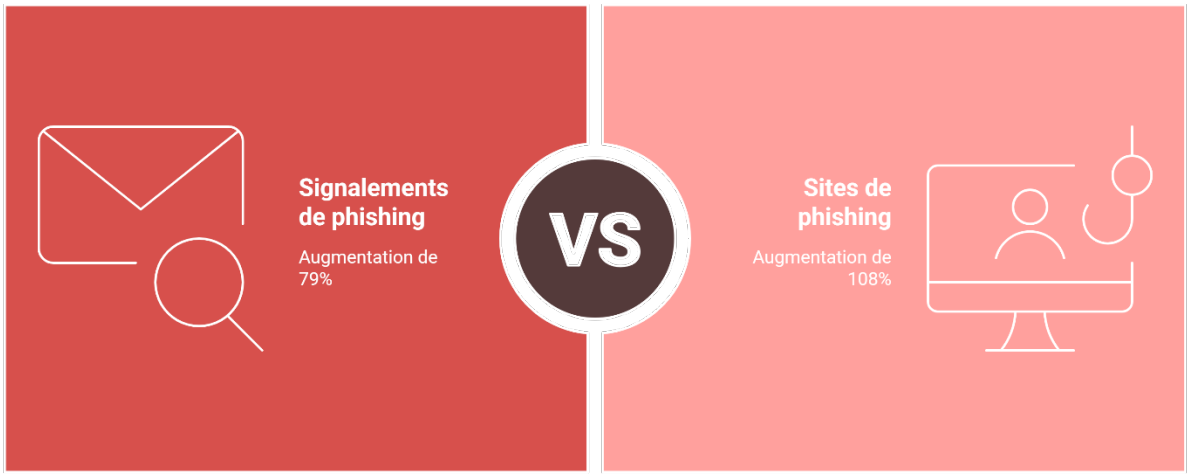
1 Vue d'ensemble et évolution des attaques de phishing en Suisse

Le phishing est une technique d'attaque par courriel, SMS ou site web frauduleux dont l'objectif est de dérober des données sensibles comme les identifiants de connexion ou les coordonnées bancaires. Ce phénomène connaît une nette progression en Suisse, et particulièrement en Suisse romande.

La plateforme nationale anti-phishing antiphishing.ch, gérée par l'Office fédéral de la cybersécurité (OFCS, ex-MELANI), centralise les signalements. Les chiffres récents démontrent une augmentation préoccupante des tentatives d'hameçonnage. En 2024, l'OFCS a reçu 975'309 signalements via antiphishing.ch, soit une hausse de +79% par rapport à 2023. Le nombre de sites de phishing distincts confirmés a également explosé, atteignant 20'872 en 2024 (+108% sur un an). À titre de comparaison, en 2023, environ 554'000 tentatives et 10'007 sites malveillants avaient été identifiés. Cette tendance s'est donc fortement accélérée.

Le tableau ci-dessous récapitule cette évolution nationale :

Augmentation préoccupante des tentatives d'hameçonnage

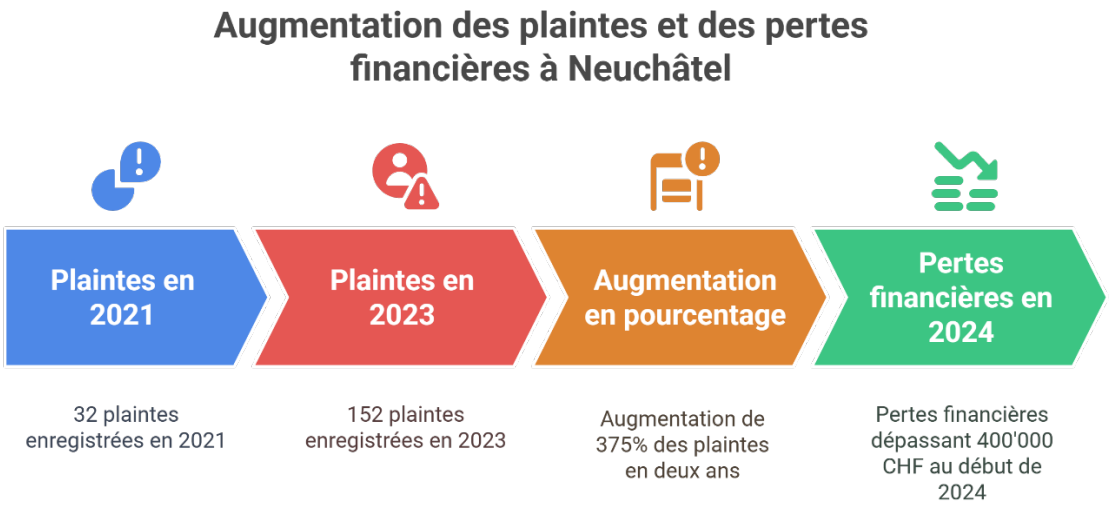


2 Situation et impacts en Suisse romande

La Suisse romande est particulièrement touchée par le phénomène. Selon la RTS, les montants escroqués via des arnaques de phishing dans la région dépassaient déjà 2 millions de CHF au cours de 2024. La police neuchâteloise a qualifié la progression des cas de phishing d'«inquiétante» en 2024, constatant que cette forme d'escroquerie est celle qui connaît la croissance la plus rapide dans le canton. À Neuchâtel, le nombre de plaintes est passé de 32 en 2021 à 152 en 2023, soit une augmentation de +375% en deux ans. Les pertes financières associées dans ce seul canton dépassaient déjà 400'000 CHF sur les premiers mois de 2024.

Ces statistiques alarmantes signifient qu'en Suisse romande, une annonce de menace est désormais faite toutes les quelques minutes aux autorités compétentes.

Ces données nationales et régionales montrent que le grand public et les PME constituent la majeure partie des victimes et des rapporteurs d'attaques, représentant 98% des signalements. La vigilance accrue est donc indispensable pour tous.



3 Cibles privilégiées : quels types de PME sont visés

Le phishing n'épargne aucune catégorie de PME. Les cybercriminels adaptent leurs stratagèmes, et toutes les entreprises, de la micro-entreprise à la PME exportatrice, peuvent être ciblées.

- **Tous les secteurs** d'activité sont touchés. Des campagnes ont usurpé l'identité de prestataires web (comme Infomaniak en 2021) pour cibler des milliers de sociétés romandes de divers secteurs, ou imité des services officiels (poste, impôts, assurance sociale AVS) dans tout le pays. Aucun domaine, qu'il s'agisse du commerce, de l'artisanat, des services ou de l'industrie, n'est à l'abri.
- **La taille de l'entreprise** n'est pas un critère d'immunité. Les petites structures sont souvent moins protégées et formées, ce qui en fait des proies faciles. Les entreprises de taille moyenne gèrent des flux financiers plus importants, les rendant potentiellement plus rentables pour les escrocs. Les PME (<250 employés) représentent 99,7% des entreprises en Suisse, offrant un vaste champ d'action aux pirates qui peuvent lancer des vagues massives de phishing dans l'espoir que certains utilisateurs mordent à l'hameçon.

- **Certains profils de** collaborateurs sont particulièrement visés. Si tous les employés peuvent recevoir des emails généraux (faux liens de connexion, pièces jointes malveillantes), ceux disposant de privilèges financiers ou d'accès sensibles sont des cibles de choix. La technique de la fraude au président (ou CEO fraud) illustre cela : l'attaquant se fait passer pour un dirigeant pour convaincre un employé (souvent en finance/comptabilité) d'exécuter un paiement urgent sur un compte frauduleux. Une recrudescence de ces fraudes ciblées a été observée en Suisse romande début 2023. Les escrocs effectuent un travail de renseignement via des sources publiques pour connaître le nom du directeur et du responsable financier, falsifient l'adresse email du dirigeant, et peuvent même renforcer la supercherie par un appel téléphonique se faisant passer pour un expert-comptable externe. Les cadres décisionnels et employés clés des PME sont ainsi des cibles privilégiées.

En résumé, les PME romandes, quel que soit leur secteur ou leur taille, doivent partir du principe qu'elles peuvent être visées par du phishing à tout moment. Les criminels adaptent leurs appâts (faux message de banque, fausse commande, faux profil RH, etc.). La surface d'attaque humaine est large et exploitée par les attaquants.

4 Cas concrets d'attaques en Suisse romande

Plusieurs incidents récents soulignent la réalité et la gravité du risque phishing pour les entreprises romandes.

- **Fraude au président en Valais (2024)** : En janvier 2024, une entreprise du Valais central a perdu près de 300'000 CHF à la suite d'une arnaque au président sophistiquée où un escroc s'est fait passer pour le CEO pour faire virer des fonds. La police valaisanne a signalé qu'il s'agissait du deuxième cas similaire en une semaine dans la région, avec des montants dérobés de plusieurs centaines de milliers de francs à chaque fois. Ces attaques éclair montrent la rapidité avec laquelle les PME peuvent subir d'énormes pertes financières.

- **Campagne Infomaniak (2021)** : Début 2021, une campagne massive a ciblé de nombreuses PME romandes en usurpant l'identité de l'hébergeur Infomaniak. Des milliers de faux courriels imitant les notifications de renouvellement de nom de domaine ont été envoyés, redirigeant les victimes vers de faux sites de paiement pour voler leurs coordonnées bancaires. Infomaniak a confirmé observer une à deux grosses vagues de phishing de ce type chaque année.
- **Attaques dans le canton de Neuchâtel (2022–2024)** : Outre l'augmentation rapide des plaintes (+375% entre 2021 et 2023), des cas spécifiques incluent de fausses factures fournisseurs, des campagnes de SMS frauduleux visant les clients d'opérateurs télécom, et de faux emails La Poste demandant des frais de douane inexistants. Ces stratagèmes ont piégé entreprises et particuliers, contribuant aux plus de 400'000 CHF de préjudices estimés dans le canton en 2024.
- **Incident Winbiz (2022)** : Bien qu'il s'agisse d'une cyberattaque plus large et non de phishing direct, l'attaque contre Winbiz (éditeur d'un logiciel de comptabilité cloud très utilisé par 45'000 PME et près de mille fiduciaires en Suisse) a paralysé l'activité de milliers de petites structures en novembre 2022. Cet événement a servi d'électrochoc, révélant la vulnérabilité de l'écosystème des PME et montrant qu'une seule attaque peut avoir des répercussions en chaîne majeures.
- **Début mai 2025** : Des fournisseurs et partenaires suisses de Prismecs ont été visés par des courriels d'hameçonnage. Ces messages, usurpant l'identité du directeur suisse, incitaient à cliquer sur un lien pour consulter un document. L'attaque a été découverte lorsqu'un antivirus a bloqué l'ouverture du lien chez un destinataire, révélant une intrusion dans le système de Prismecs. L'incident est significatif en raison de l'implication de Prismecs, sous-traitant de General Electrics, dans la centrale de réserve de Birr.

Ces exemples démontrent que le risque phishing est réel et que les conséquences (vol de liquidités, interruption d'activité, perte de confiance) peuvent être dramatiques pour les PME.

5 PME romandes : perception du risque et niveau de préparation

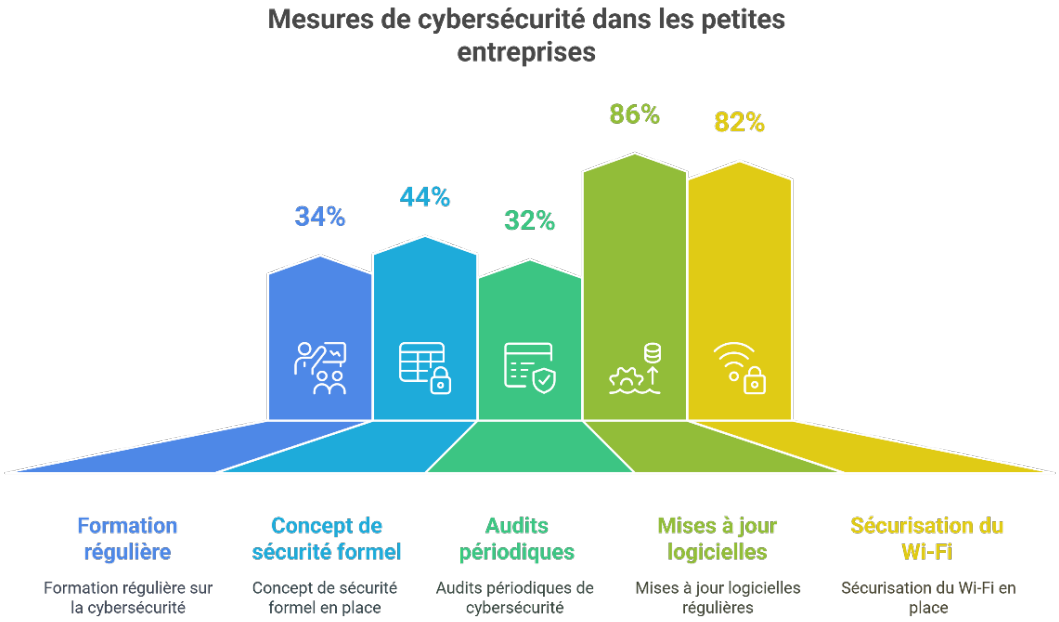
Malgré la hausse des menaces, de nombreuses PME restent insuffisamment préparées. Il existe un écart entre la gravité objective du risque et sa perception.

- **Une menace souvent sous-estimée** : Beaucoup de dirigeants de PME pensent à tort "ne pas être une cible intéressante" car ils estiment ne pas avoir de données stratégiques ou de grosses sommes en banque. Or, mettre à l'arrêt une entreprise pour exiger une rançon peut toucher n'importe quel domaine. Les statistiques contredisent cette sous-estimation : en Suisse, une PME sur trois a déjà été victime d'une cyberattaque ou fraude financière, et les attaques contre les entreprises suisses ont augmenté de 61% en 2023. Les PME romandes ne sont donc pas trop petites pour intéresser les escrocs.

- **Retard dans la formation et les mesures organisationnelles** : La sensibilisation des employés et les procédures de sécurité sont souvent insuffisantes. Selon une étude nationale, seulement 34% des petites entreprises (4-49 employés) organisent des formations régulières sur la cybersécurité, et environ 44% ont un concept de sécurité formel. Seuls 32% procèdent à des audits périodiques. En revanche, les mesures techniques de base sont mieux appliquées (86% pour les mises à jour logicielles, 82% pour la sécurisation du Wi-Fi).

Le tableau suivant résume le taux d'adoption de mesures de protection parmi les PME suisses :

Ce décalage montre que les PME privilégient les outils techniques au détriment des facteurs humains et organisationnels. Or, face au phishing, la vigilance humaine est cruciale, car un seul clic malencontreux peut contourner les barrières techniques.



- **Prise de conscience progressive** : La conscience du risque progresse lentement. La cybersécurité est désormais classée risque n°1 pour les entreprises en Suisse. De plus en plus de dirigeants réalisent l'importance du sujet, souvent après avoir été victimes. Environ 29% des patrons de petites entreprises s'attendent à devoir renforcer leurs mesures de sécurité dans les 1 à 3 ans. Cependant, seule la moitié des PME suisses disposent aujourd'hui d'un plan de sécurité, de formations régulières ou d'audits. Il reste beaucoup à faire pour sensibiliser les nombreuses petites structures romandes qui demeurent vulnérables.
- **Mettre à jour la politique de sécurité** en fonction des nouvelles menaces et des évolutions réglementaires.
- **Adapter et moderniser** l'infrastructure informatique (virtualisation, migration vers le cloud, etc.) avec des solutions de sécurité adéquates.

L'enjeu est d'intégrer la cybersécurité, et la lutte anti-phishing, dans la culture d'entreprise.

6 Recommandations et bonnes pratiques anti-phishing

Les autorités suisses et les spécialistes diffusent des conseils clés pour se prémunir contre l'hameçonnage. Le Centre national pour la cybersécurité (NCSC/OFCS) publie notamment des recommandations officielles.

- **Rester vigilant et sceptique** : Adopter une attitude méfiante face aux messages non sollicités demandant une action rapide. Ne jamais faire confiance d'emblée à un email/SMS inattendu demandant des codes ou un paiement. Aucune administration ou banque sérieuse ne demande de confirmer des identifiants par email/SMS. En cas de doute, ne cliquez pas et vérifiez par un autre canal.
- **Signaler les tentatives de phishing** : Signaler toute tentative sur la plateforme antiphishing.ch (gérée par l'OFCS) pour aider au blocage des sites frauduleux. Utiliser report.ncsc.admin.ch pour un suivi personnalisé. Signaler participe à l'effort collectif.
- **Protéger les accès sensibles** : Mettre en place l'authentification multi-facteurs (MFA) partout où possible (messagerie, cloud, e-banking). Le MFA bloque 99% des accès non-autorisés même si un mot de passe est volé. Utiliser un mot de passe unique et robuste (idéalement avec un gestionnaire de mots de passe) pour chaque compte critique.
- **Sensibiliser et former le personnel** : S'assurer que les employés connaissent les signes du phishing et les bons réflexes (vérifier l'adresse de l'expéditeur, déceler les fautes, ne pas divulguer de données sensibles par email). Valoriser le signalement d'emails douteux à l'IT plutôt que d'essayer de gérer seul. En cas de clic malencontreux, agir immédiatement (changer mots de passe, contacter banque/autorités).
- **Prudence sur les liens et pièces jointes** : Ne jamais cliquer sur un lien ou ouvrir une pièce jointe si la provenance n'est pas certaine. Même si le message semble légitime, l'identité peut être falsifiée. En cas de doute, ne pas répondre ou cliquer, mais plutôt accéder au site officiel en tapant l'adresse directement. Ouvrir une pièce jointe seulement si elle est attendue et confirmée par l'expéditeur supposé.
- **Vérifier les demandes de paiement** : Instaurer des procédures strictes pour contrer la fraude au président : vérification téléphonique auprès d'un cadre pour les virements exceptionnels, double signature pour les montants importants. Ne jamais se fier à un simple email pour déclencher un transfert de fonds. En cas de demande urgente d'un "dirigeant", vérifier l'identité de l'émetteur par un canal indépendant (numéro habituel du supérieur, pas celui fourni dans l'email). La Prévention Suisse de la Criminalité (PSC) recommande de toujours contrôler l'identité via un canal indépendant quand de l'argent est en jeu.

- **Surveiller les comptes financiers** : Contrôler régulièrement les relevés bancaires et de carte de crédit pour détecter rapidement toute transaction suspecte. Plus une fraude est détectée tôt, plus les chances de bloquer ou récupérer les fonds sont élevées.
- **Utiliser les outils de filtrage** : Activer les filtres anti-spam/anti-phishing des messageries. Utiliser les filtres SMS sur les smartphones professionnels. Maintenir les logiciels de sécurité (antivirus, etc.) à jour. Ces outils ne sont pas infaillibles mais complètent la vigilance humaine.

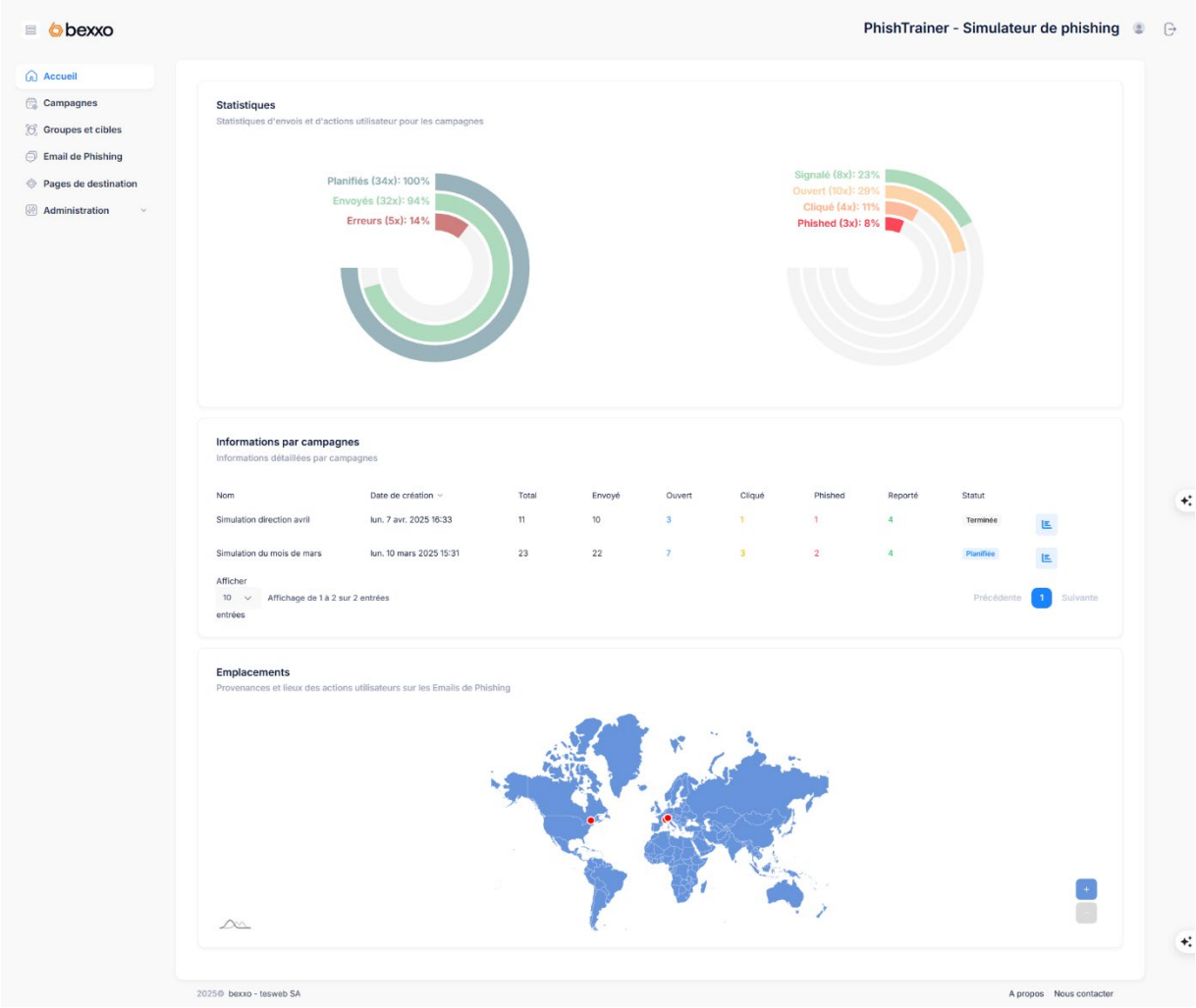
En appliquant ces recommandations, les PME peuvent réduire leur exposition au phishing. Le NCSC (OFCS) propose des ressources en français (fiches, check-lists) et relaie les alertes sur les campagnes en cours. La collaboration entre organismes publics et PME est appelée à se renforcer.

7 Renforcer la première ligne de défense humaine

Comme souligné, le facteur humain est crucial face au phishing, et le retard dans la formation et la sensibilisation du personnel constitue un point faible majeur pour de nombreuses PME romandes. C'est précisément sur cet enjeu que des outils spécialisés peuvent faire une différence significative.

PhishTrainer est un logiciel de simulation de phishing conçu en Suisse, pour répondre à la nécessité de sensibiliser les collaborateurs aux risques numériques et de renforcer leur vigilance. Développé et hébergé en Suisse, il bénéficie des standards de qualité, de sécurité et de confidentialité helvétiques.

L'objectif de **PhishTrainer** est de mesurer la vigilance des utilisateurs et de les former de manière concrète et continue à identifier les menaces d'hameçonnage. Le logiciel expose les employés à des campagnes de courriels frauduleux réalistes et adaptées à leur contexte professionnel.



En utilisant **PhishTrainer**, les entreprises peuvent :

- **Évaluer la vigilance des employés** via des simulations réalistes et adaptées.
- **Renforcer les réflexes face au phishing** en habituant les collaborateurs à identifier les signaux d'alerte et à adopter les bons comportements.
- **Former de manière continue et ciblée** grâce à un apprentissage progressif avec des scénarios variés et personnalisés.
- **Identifier les points faibles organisationnels** pour adapter les actions de sensibilisation.
- **Réduire les risques humains et financiers** en diminuant l'exposition de l'entreprise aux cyberattaques et en limitant les impacts.

Le logiciel offre une personnalisation avancée des emails de simulation et des pages de destination, permettant aux organisations d'adapter le contenu, le design et les scénarios pour refléter leur environnement de travail et les menaces réelles. Cette flexibilité renforce l'efficacité des campagnes.

Pour une mise en œuvre rapide, une bibliothèque de modèles (templates) prêts à l'emploi est disponible. Ces différents modèles s'inspirent directement de scénarios réels en lien direct avec l'écosystème suisse et couvrent différents types d'attaques courantes, utilisables tels quels ou adaptés.

La sécurité étant le cœur de PhishTrainer, les données sont chiffrées côté client, ce qui garantit une sécurité et confidentialité absolue de vos données stockées chez PhishTrainer.

Tous les détails sous : https://www.bexxo.ch/fr/phishtrainer.html

8 Conclusion

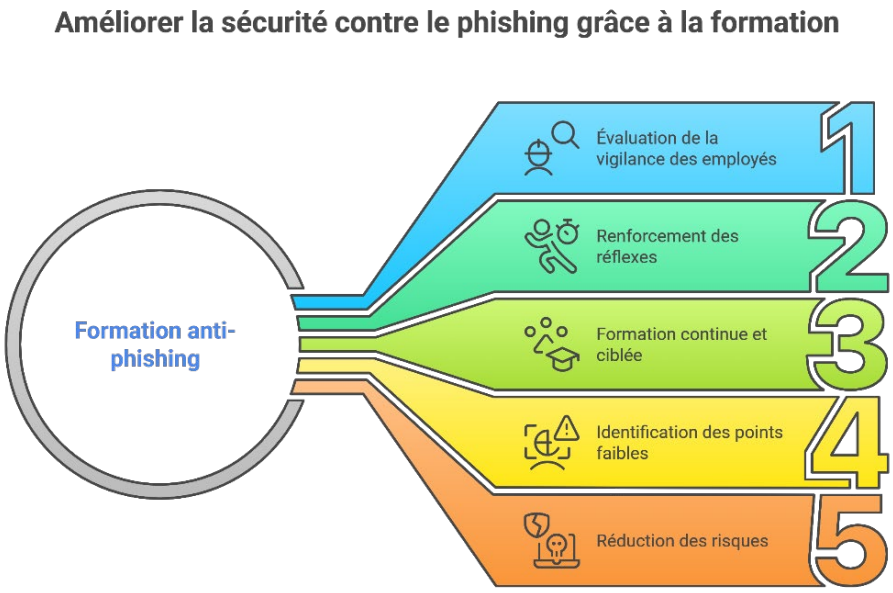
Le phishing s'est imposé comme un risque majeur pour les PME en Suisse romande, avec une croissance alarmante des attaques et des pertes financières significatives. Aucune entreprise n'est à l'abri, et la sous-estimation du risque ainsi que le retard dans la formation du personnel sont des facteurs aggravants.

Cependant, il est possible de se protéger en adoptant une attitude proactive, en intégrant la cybersécurité dans la culture d'entreprise, et en suivant les recommandations des autorités. La sensibilisation et la formation continue des employés sont des piliers essentiels de cette protection.

Des outils dédiés comme **PhishTrainer** offrent une solution concrète pour adresser le facteur humain, permettant d'évaluer la vigilance, de former le personnel aux réflexes de sécurité et d'identifier les vulnérabilités organisationnelles. En combinant des mesures techniques de base, des procédures organisationnelles solides, et une

sensibilisation continue renforcée par des simulations réalistes, les PME romandes peuvent significativement réduire leur exposition au phishing et protéger leur activité et leur réputation face à ce fléau croissant.

Rester informé des menaces et adopter les bonnes pratiques est vital pour déjouer la plupart des tentatives d'hameçonnage et éviter de devenir une statistique de plus dans les rapports sur la cybercriminalité.



9 Références

Sources : Office fédéral de la cybersécurité (NCSC/OFCS), rapports 2023-2024 ; Prévention Suisse de la Criminalité (PSC) ; études digitalswitzerland/La Mobilière (2022) ; médias romands (RTS, ArcInfo, RTN, PME Magazine, Blick) pour les cas d'actualité et statistiques régionales. Toutes les données citées proviennent de sources fiables et officielles.

PhishTrainer | Logiciel Simulation de Phishing Solutions- bexxo: https://www.bexxo.ch/fr/phishtrainer.html