Reconnaître et déjouer le phishing (hameçonnage)

Les signes qui trahissent un email frauduleux et les réflexes à adopter avant de cliquer.

14 min de lecture · Niveau Essentiel · cyberionis.fr/ressources/phishing

Le phishing reste le vecteur d'attaque n° 1 contre les entreprises : un message se fait passer pour un tiers de confiance — banque, fournisseur, administration, collègue — afin de voler des identifiants, de faire exécuter un paiement ou d'installer un logiciel malveillant. Ce guide décortique le fonctionnement de l'attaque, ses variantes (SMS, téléphone, QR code, ciblage sur mesure), les protections techniques à mettre en place, et le plan d'urgence si le clic a déjà eu lieu.

1. Comment fonctionne une attaque de phishing

Une campagne de phishing suit presque toujours le même déroulé en trois temps :

1. La préparation

L'attaquant collecte ses cibles : adresses email achetées après des fuites de données, moissonnées sur le site web de l'entreprise, LinkedIn ou les registres publics. Pour les attaques ciblées, il étudie l'organigramme, les fournisseurs et le vocabulaire de l'entreprise afin de rendre son message crédible.

2. L'appât

Le message combine deux ingrédients : un prétexte crédible (facture, colis, alerte de sécurité, document partagé, relance administrative) et un levier émotionnel — l'urgence, la peur ou la curiosité — qui court-circuite la réflexion. L'objectif est que vous agissiez avant de réfléchir.

3. La capture

Le lien mène vers une copie parfaite de la page de connexion attendue (Microsoft 365, banque, service de livraison). Ce que vous y tapez part directement chez l'attaquant — qui parfois relaie votre saisie vers le vrai site pour que vous ne remarquiez rien. Variante : la pièce jointe installe un logiciel qui vole les mots de passe enregistrés ou ouvre un accès distant au poste.

> **CAS CONCRET**
> *Scénario réel vu en PME : un comptable reçoit un « partage de document » Microsoft 365 imitant parfaitement l'original, saisit ses identifiants, et rien ne se passe — il pense à un bug. Trois semaines plus tard, l'attaquant, qui lisait ses emails depuis, envoie aux clients de l'entreprise de fausses factures avec un RIB modifié, depuis la vraie boîte du comptable.*

2. Les signaux d'alerte

Aucun signal isolé n'est une preuve, mais deux ou trois combinés doivent déclencher la méfiance :

- Un sentiment d'urgence : « votre compte sera suspendu sous 24 h », « dernier rappel avant poursuite »
- Une adresse d'expéditeur approximative : service@paypa1.com, direction@entreprise-fr.net — vérifiez

l'adresse complète, pas le nom affiché

- Un lien dont l'adresse réelle (survolez sans cliquer, ou appui long sur mobile) ne correspond pas au texte affiché
- Une demande inhabituelle : identifiants, RIB, paiement urgent, cartes cadeaux, code reçu par SMS
- Une rupture de canal : votre banque ne demande jamais vos codes par email, un collègue ne demande pas un virement par SMS
- Une pièce jointe inattendue : .zip, .html, .iso, facture non sollicitée, « scan » d'un expéditeur inconnu
- Des fautes ou une formulation étrange — mais attention : l'IA générative produit désormais des faux sans aucune faute ; l'absence de faute ne prouve rien

3. Les variantes à connaître

Smishing (par SMS)

Faux avis de colis, fausse vignette Crit'Air, faux message de la banque ou de l'Assurance Maladie. Le SMS inspire confiance et se lit dans l'instant, souvent en situation de distraction — c'est ce qui le rend si efficace. Les liens raccourcis y masquent la destination réelle.

Vishing (par téléphone)

Un faux conseiller bancaire « anti-fraude » vous appelle : des débits suspects auraient été détectés, il faut « sécuriser le compte » en validant des opérations ou en communiquant des codes. Le numéro affiché peut être falsifié pour imiter celui de votre banque. Règle absolue : raccrochez et rappelez vous-même le numéro officiel — jamais celui qu'on vous donne.

Quishing (par QR code)

Le QR code — collé sur une borne de recharge ou un parcmètre, inséré dans un email ou un PDF « sécurisé » — échappe aux filtres anti-spam et masque totalement sa destination. Ne scannez pas de QR code pour vous « authentifier » à la demande d'un message.

Spear phishing et compromission de partenaires

Le phishing ciblé vise une personne précise avec un message sur mesure : le comptable reçoit un email « du dirigeant », l'assistante un message « du fournisseur habituel ». Le cas le plus difficile à détecter : la boîte email d'un vrai partenaire est compromise, et le message frauduleux arrive dans une conversation existante, de la vraie adresse. C'est pourquoi les procédures (vérification téléphonique des RIB, double validation des paiements) protègent là où la vigilance ne suffit plus.

4. Les bons réflexes au quotidien

Dans le doute, ne cliquez jamais depuis le message. Ouvrez votre navigateur et connectez-vous au service par son adresse habituelle, ou appelez l'interlocuteur à un numéro que vous connaissez déjà.

- Jamais d'identifiants saisis après avoir cliqué sur un lien reçu — c'est LA règle qui neutralise l'essentiel du phishing
- Vérifier l'adresse complète de l'expéditeur, pas seulement le nom affiché
- Prendre dix secondes : aucune vraie urgence ne se joue à la minute ; l'urgence est l'outil de l'attaquant
- Signaler le message douteux au référent informatique avant de le supprimer — il protège peut-être vingt collègues qui ont reçu le même
- Signaler les tentatives sur signal-spam.fr et transférer les SMS frauduleux au 33700

5. Protéger l'entreprise techniquement

La vigilance humaine est indispensable mais faillible — un jour de fatigue suffit. Les mesures techniques réduisent le nombre de messages qui arrivent et les dégâts d'un clic :

- La double authentification partout : même identifiants volés, le compte tient — c'est la mesure au meilleur rapport effort/protection
- Un filtrage anti-phishing en amont des boîtes (inclus dans Microsoft 365 / Google Workspace, à activer et régler)
- SPF, DKIM et DMARC sur votre domaine, pour que les fraudeurs ne puissent pas envoyer d'emails « de votre part » (voir notre guide dédié)
- Un navigateur et des postes à jour : les pages malveillantes exploitent des failles corrigées
- Le gestionnaire de mots de passe comme détecteur : il ne propose pas de remplir les identifiants sur un faux site, car l'adresse ne correspond pas — un remplissage qui ne se déclenche pas est un signal d'alarme

6. J'ai cliqué : le plan d'urgence

Un clic n'est pas une catastrophe si la réaction est rapide. L'ordre des opérations :

- J'ai saisi un mot de passe : le changer immédiatement sur le service concerné et partout où il est réutilisé, puis activer la MFA ; vérifier dans les paramètres de la messagerie qu'aucune règle de transfert ou de suppression automatique n'a été créée
- J'ai ouvert une pièce jointe : déconnecter le poste du réseau (câble et Wi-Fi) sans l'éteindre, et prévenir le référent IT ou votre prestataire
- J'ai saisi des coordonnées bancaires : prévenir la banque, faire opposition, surveiller les comptes
- J'ai validé une notification MFA que je n'avais pas demandée : changer le mot de passe et déconnecter toutes les sessions actives du compte
- Dans tous les cas : signaler l'incident en interne, immédiatement et sans honte

ATTENTION

Le pire scénario n'est pas le clic — c'est le clic caché. Chaque heure de silence laisse l'attaquant lire les emails, préparer une fraude au virement ou déployer un ransomware. Une culture du signalement sans blâme est la meilleure protection de l'entreprise : celui qui signale vite a le bon réflexe, jamais une faute.

7. Entraîner l'équipe

- Sensibiliser à l'embauche puis par rappels courts réguliers — le sujet s'use vite, les exemples réels reçus par l'entreprise sont les meilleurs supports
- Organiser un ou deux exercices de faux phishing par an, suivis d'un débriefing bienveillant : l'objectif est le taux de signalement, pas la chasse aux cliqueurs
- Former spécifiquement les fonctions exposées : comptabilité, direction, RH, accueil
- Afficher la règle d'or quelque part : « Un doute ? On ne clique pas, on signale. »

L'essentiel à retenir

01 Former chaque collaborateur à repérer les signaux d'alerte

02 Instaurer la règle : jamais d'identifiants saisis depuis un lien reçu

03 Activer la double authentification sur toutes les messageries

04 Configurer SPF, DKIM et DMARC sur votre domaine

05 Définir à qui signaler un email suspect, et valoriser le signalement

06 Vérifier tout changement de RIB fournisseur par téléphone

07 Organiser un exercice de faux phishing une fois par an

Questions fréquentes

Comment vérifier un lien sans cliquer dessus ?

Sur ordinateur, survolez le lien sans cliquer : l'adresse réelle s'affiche en bas du navigateur ou dans une infobulle. Sur mobile, un appui long affiche l'URL. Lisez l'adresse de droite à gauche : ce qui compte est le vrai nom de domaine juste avant le premier « / » — « microsoft.com.verification-xyz.ru » n'a rien de Microsoft.

J'ai cliqué sur le lien mais je n'ai rien saisi. Suis-je en danger ?

Le risque est faible : dans l'immense majorité des cas, le simple affichage de la page ne compromet rien, le danger est dans la saisie d'identifiants ou le téléchargement d'un fichier. Par précaution, fermez la page, ne téléchargez rien, et signalez le message. Si le poste est ancien ou pas à jour, mentionnez-le au référent IT.

Notre antispam laisse passer des phishings. C'est normal ?

Aucun filtre n'arrête tout : les attaquants testent leurs messages contre les filtres du marché avant d'envoyer. Un bon filtrage élimine l'essentiel du volume ; la vigilance humaine et la MFA couvrent le reste. Si le volume reçu est vraiment élevé, le paramétrage du filtre (et la configuration DMARC de votre domaine) mérite une revue.

Les exercices de faux phishing ne risquent-ils pas de braquer les équipes ?

Ils braquent quand ils servent à pointer du doigt. Menés correctement — annoncés dans leur principe, débriefés collectivement, sans sanction ni classement individuel — ils sont au contraire bien acceptés et font durablement progresser le taux de signalement, qui est le vrai indicateur de sécurité.

Que faire des emails de phishing reçus : supprimer ou garder ?

Signalez d'abord (référent interne, bouton « signaler » de la messagerie, signal-spam.fr), puis supprimez. Si le message a servi à une fraude réalisée, conservez-le précieusement : il devient une preuve pour la plainte et l'assurance.

Pour aller plus loin

Cybermalveillance.gouv.fr — fiche hameçonnage — www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing

Signal Spam — signaler un email frauduleux — www.signal-spam.fr

33700 — signaler un SMS frauduleux — www.33700.fr

Phishing Initiative — faire bloquer un site de phishing — phishing-initiative.eu/contrib/

Un doute, une urgence, un incident ?

Cyberionis évalue votre exposition, prépare vos défenses et vous épaule pour réagir vite en cas d'attaque.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr