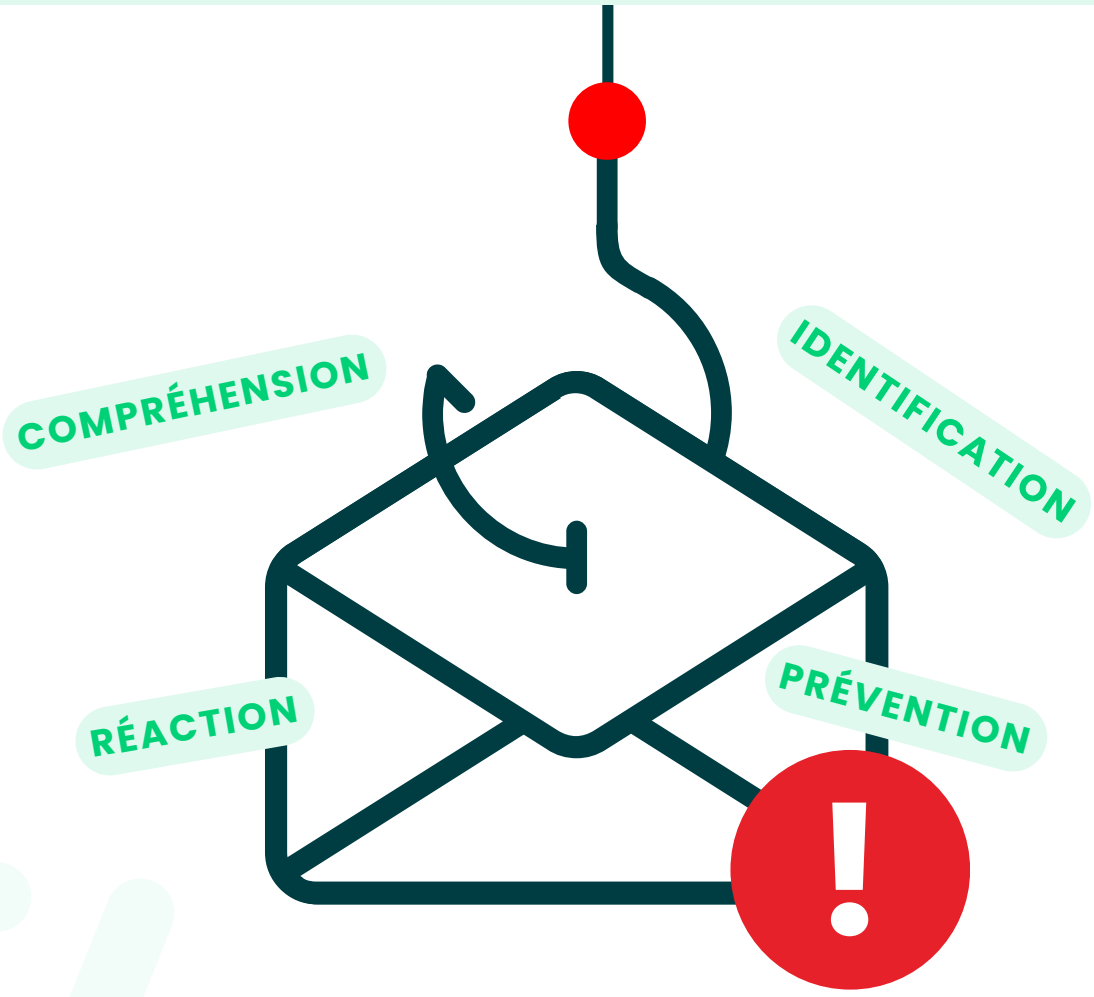
Reconnaître et éviter le phishing en 4 étapes



Ne laissez pas vos employés prendre à l'hameçon

Anderson

Le phishing en bref

Le phishing (ou hameçonnage) est un message frauduleux qui imite un contact ou un service de confiance pour **vous pousser à cliquer sur un lien, ouvrir une pièce jointe ou communiquer un mot de passe.** C'est la première porte d'entrée des attaques informatiques.

Pourquoi cela concerne mon entreprise ?

Les messages ne viennent pas toujours d'inconnus. Nous constatons régulièrement des attaques envoyées depuis la boîte mail réelle d'un partenaire, d'un fournisseur ou d'un client que vous connaissez, parce que son compte a été piraté. Le message arrive alors de la bonne adresse, avec parfois le bon ton et le bon historique.

La conséquence est simple : l'expéditeur, même connu, ne prouve jamais qu'un message est légitime. Ce qui compte, c'est de savoir si la demande est attendue et normale.

Vos employés au coeur du problème

Le phishing n'exploite pas une faille de vos logiciels, mais un réflexe humain : la confiance, la routine, la peur de mal faire. Un message bien construit court-circuite la vigilance en jouant sur l'émotion et l'urgence, c'est pourquoi aucun antivirus ne remplace un œil attentif. Les attaquants soignent d'ailleurs de plus en plus leurs messages, avec l'aide de l'intelligence artificielle : la présence de fautes est un indice, mais leur absence ne prouve rien.

Ce que cherche le hacker

- **Vos identifiants :** mots de passe, codes, accès à vos comptes et outils
- **Votre argent :** virements détournés, fausses factures, coordonnées bancaires modifiées
- **Un point d'entrée :** installer un logiciel malveillant pour rebondir sur tout le réseau de l'entreprise.

En chiffres

Le phishing n'est pas une menace théorique : c'est la technique d'attaque la plus courante, et elle vise d'abord les personnes, pas les machines.

Environ

60%

des intrusions informatiques en Europe commencent par du phishing (e-mail, appel ou SMS).

Source : ENISA, Threat Landscape 2024

68%

des violations de données impliquent une erreur ou une manipulation humaine.

Source : Verizon, Data Breach Investigations Report 2024

<60s

temps médian pour se faire piéger : 21s pour cliquer, 28 s pour saisir ses données.

Source : Verizon DBIR 2024

9 millions

de messages suspects signalés par les Belges à suspect@safeonweb.be en 2024, soit ~25 900 par jour.

Source : Centre pour la Cybersécurité Belgique (CCB / Safeonweb)

4 151 %

c'est l'explosion du volume de phishing (hameçonnage) depuis l'essor des outils d'intelligence artificielle.

Les attaques sont plus rapides, mieux ciblées et sans aucune faute d'orthographe. Ce flou artistique rend les pièges beaucoup plus difficiles à repérer.

Source : Dashlane

L'attaque en 3 étapes

Comment se déroule une attaque ?

Presque toutes les attaques suivent le même scénario en trois temps. Le reconnaître aide à l'interrompre car, à chaque étape, un doute suffit à tout arrêter.

1

L'appât

Un message crédible imite un contact ou un service de confiance et **installe l'urgence** : "facture impayée", "colis bloqué", "une connexion suspecte". Il joue sur l'émotion pour désactiver votre réflexe de prudence.

2

L'hameçon

Vous cliquez sur le lien, ouvrez la pièce jointe ou répondez à la demande. Vous saisissez un mot de passe sur un faux site, ou vous lancez sans le savoir un logiciel malveillant.

3

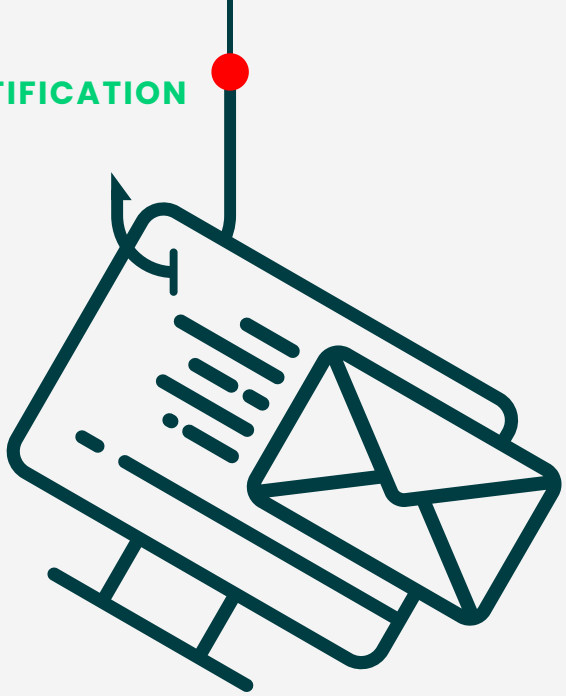
L'exploitation

L'attaquant utilise ce qu'il a obtenu : vol d'identifiants, virement détourné, données revendues, ou installation d'un rançongiciel qui se propage dans le réseau.

La bonne nouvelle

La chaîne se brise dès la première étape. Reconnaître l'appât, c'est ne jamais mordre à l'hameçon.

Anderson



Les différents types de phishing

Le phishing ne se limite pas à l'e-mail. Le canal change, la logique reste la même : créer la confiance, puis l'urgence.

E-mail de masse

Le plus courant. Un même message envoyé à des milliers de personnes en misant sur le volume : il suffit qu'une petite part clique.

Spear phishing

Ciblé et personnalisé à partir d'infos réelles (poste, collègues, projets) diffusées sur les réseaux sociaux. Beaucoup plus crédible.

Whaling

Vise les dirigeants et la direction financière. Ton corporate soigné, enjeux et pertes potentielles élevés.

Vishing

Par téléphone, souvent avec un numéro usurpé. Un faux "conseiller" ou "technicien" crée l'urgence pour obtenir codes ou accès.

Smishing

Par SMS ou messagerie : colis à suivre, amende, code à confirmer, avec un lien piégé et un appel à réagir immédiatement.

Quishing

Un QR code redirige vers un faux site. En forte hausse, car l'image échappe souvent aux filtres de messagerie.

Clone phishing

Un e-mail légitime déjà reçu est recopié à l'identique, mais son lien ou sa pièce jointe sont remplacés par une version malveillante.

Double authentification

Activez la double authentification (2FA) partout où c'est possible. Même volé, un mot de passe ne suffit alors plus à ouvrir votre compte.

5 vérifications rapides

Au-delà du ressenti, quelques vérifications simples sur le message lui-même trahissent souvent un faux.

1) Un lien qui ne mène pas où il prétend

Survolez le lien sans cliquer : l'adresse réelle apparaît. Lisez le nom juste avant le premier « / » — c'est le vrai domaine. « fournisseur-connu.be.secure-paiement24.ru » n'est pas votre fournisseur, mais le site « secure-paiement24.ru ».

2) Une demande d'informations confidentielles

Mot de passe, code PIN, question de sécurité, coordonnées bancaires : une organisation sérieuse ne les demande jamais par e-mail. Une telle demande est à elle seule un signal d'alerte.

3) Une formulation qui cloche

Salutation impersonnelle (« Cher client »), fautes, tournures maladroites, logo pixelisé. Attention toutefois : les faux sont de mieux en mieux rédigés, parfois via l'IA.

4) Le cadenas et « https » ne prouvent rien

De plus en plus de faux sites affichent le cadenas et le « https ». Ils indiquent que la connexion est chiffrée, pas que le site est honnête. Ne vous y fiez pas seul.

5) Une pièce jointe inattendue

Ne l'ouvrez pas, surtout s'il s'agit d'un programme à exécuter (fichiers terminant par .exe, .zip…) ou d'un document Office qui vous demande "d'activer le contenu" ou "les macros" pour s'afficher : c'est un moyen classique d'installer un logiciel malveillant.

Cas pratique

URGENT – Facture impayée à régulariser aujourd'hui 1

Service Comptabilité
SC comptabilite@fournisseur-connu.be 09:14
2

À : vous

Bonjour,

Notre système indique qu'une facture reste impayée. **Le compte sera suspendu sous 24 h sans régularisation.**
3

Merci de confirmer vos coordonnées de paiement via le lien sécurisé ci-dessous :

Consulter et régulariser ma facture

`http://fournisseur-connu.be.secure-paiement24.ru/login`
4

Cordialement,
Le service de facturation

1) L'urgence et la menace

Objet et texte qui pressent : «aujourd'hui», «sous 24 h», «compte suspendu». On veut vous faire agir vite, sans réfléchir.

2) Un expéditeur connu ne suffit pas

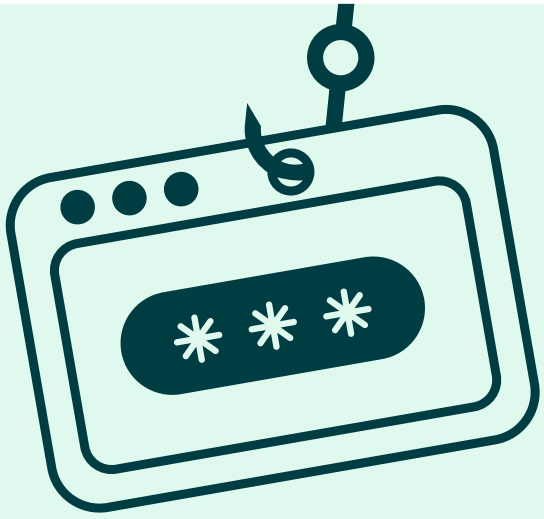
L'adresse peut être exacte et pourtant piratée. La vraie question : cette demande est-elle attendue et normale ?

3) Une demande inhabituelle

Confirmer des coordonnées de paiement, «vérifier» un compte : un partenaire légitime ne procède pas ainsi par mail.

4) Le lien ne mène pas où il dit

En survolant le lien (sans cliquer), l'adresse réelle apparaît. Ici le vrai domaine est «secure-paiement24.ru », pas votre fournisseur.



Ce que le phishing peut vous coûter

Un seul clic peut suffire. Les conséquences d'une attaque réussie touchent aussi bien vos finances que vos données et votre réputation.

Vol d'identifiants

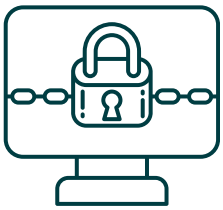
Vol de fonds

Vol de données sensibles

Revente de données

Atteinte à la réputation

Fraude au virement



Rançongiciel

Vol de propriété intellectuelle

Coûts de remédiation

Le plus long à réparer n'est pas technique.

Au-delà du coût direct, une fuite de données entame durablement la confiance des clients et des partenaires. C'est souvent ce qui prend le plus de temps à reconstruire.

Vérifier et réagir

Vérifier un message en 30 secondes

1. Cette demande est-elle attendue ? Si non, c'est déjà un signal fort.
2. Survolez le lien sans cliquer : l'adresse réelle s'affiche. Le nom juste avant le premier « / » correspond-il vraiment à l'organisation attendue ?
3. N'ouvrez jamais une pièce jointe inattendue, surtout un fichier à activer ou un document qui demande « d'activer les macros ».
4. Dans le doute sur un expéditeur connu, confirmez par un autre canal (un appel, un message séparé), jamais en répondant au mail suspect.

En cas de doute : le bon réflexe

Ne cliquez pas, ne répondez pas, ne transmettez aucune information. Signalez le message à votre support IT, qui vérifiera pour vous. Mieux vaut un signalement inutile qu'un clic de trop.

Déjà cliqué ou saisi un mot de passe ? Ne restez pas seul.

Déconnectez l'appareil du réseau si possible, changez le mot de passe concerné depuis un autre appareil, et prévenez immédiatement votre support IT. Plus l'alerte est rapide, plus les dégâts sont limités — signaler une erreur tôt n'est jamais un problème.

Phishing : les bons réflexes

Dans le doute, ne cliquez pas. Signalez.

1

Est-ce attendu ?

Facture, colis, lien, demande de mot de passe : si je ne l'attendais pas, je me méfie.

2

L'urgence est un piège

«Sous 24 h», «compte bloqué», «aujourd'hui» : on veut me faire agir sans réfléchir.

3

Je survole le lien

Sans cliquer. Le vrai domaine (avant le premier « / ») correspond-il à l'expéditeur ?

4

Expéditeur connu ≠ sûr

Une adresse connue peut être piratée. Je ne me fie jamais au seul nom.

5

Aucune pièce jointe surprise

Je n'ouvre pas un fichier inattendu, jamais « activer les macros ».

6

Je vérifie autrement

Un doute ? J'appelle la personne sur un numéro connu. Jamais en répondant au mail.

Anderson

Découpez et affichez.

Anderson

Faisons connaissance !

ASSESS
On fait le point

Un audit IT et de sécurité Microsoft 365, sans langue de bois, pour voir où vous en êtes et par où commencer.

BUILD
On pose des bases solides

Cloud Azure, réseau, infrastructure et sauvegardes : du costaud, pensé pour durer et grandir avec vous.

ENABLE
On vous simplifie le quotidien

Microsoft 365, Teams, SharePoint, Copilot… les bons outils, bien configurés, pour une équipe qui avance sans friction.

MAINTAIN
On garde l'oeil

Support réactif, maintenance et monitoring : votre IT tourne, et quand vous appelez, quelqu'un décroche.

SECURE
On veille à votre place

Protection Microsoft 365, Defender EDR, sensibilisation et SOC 24/7 : votre sécurité, à tous les niveaux.

On en discute autour d'un café ?

Commençons par un audit gratuit : 30 minutes pour repérer vos points faibles et y voir plus clair.

Simon Missaghi

simon.missaghi@anderson.be
010 87 20 90