

1. L'Expéditeur : Ne vous fiez pas au nom

Les pirates usurpent l'identité de personnes que vous connaissez (votre patron, un collègue, Microsoft, votre banque).

- Le piège : Le nom affiche "Jean Dupont", mais l'adresse réelle est jean.dupont.ceo@gmail.com ou support@microsoft-security.com.
- Le réflexe : Cliquez sur le nom de l'expéditeur pour afficher l'adresse email complète. Si le domaine (après le @) semble étrange ou ne correspond pas à l'entreprise officielle, stoppez tout.

2. Le Sentiment d'Urgence ou de Menace

Le phishing joue sur vos émotions pour vous faire agir sans réfléchir.

- Le piège : "Votre compte sera bloqué sous 2h", "Facture impayée : risque de poursuites", ou "Urgent : virement à effectuer pour une commande confidentielle".
- Le réflexe : Plus le message est alarmant, plus vous devez ralentir. L'urgence est l'alliée du pirate.

3. La Technique du "Survol" (L'astuce n°1)

Les pirates cachent souvent la destination réelle d'un lien derrière un bouton ou un texte bleu.

- Le piège : Un bouton "Cliquez ici pour vous connecter" qui renvoie vers un site malveillant.
- Le réflexe : Laissez votre souris survoler le lien (SANS CLIQUER). L'adresse de destination s'affichera en bas à gauche de votre écran ou dans une bulle. Si l'adresse paraît complexe ou suspecte (ex: bit.ly/3xYz1 au lieu de votre-entreprise.com), n'ouvrez rien.

4. Les Pièces Jointes Suspectes

Un simple clic sur un fichier peut installer un virus (Ransomware) qui cryptera tous les fichiers de l'entreprise.

- Le piège : Des fichiers nommés [Facture.zip](#), [Paiement.html](#), ou un document Word qui demande d'"Activer les macros".
- Le réflexe : Ne jamais ouvrir une pièce jointe inattendue. En cas de doute, appelez l'expéditeur sur son téléphone professionnel pour confirmer l'envoi.

5. Demandes de Coordonnées Bancaires ou Identifiants

Aucune institution sérieuse (Banque, Impôts, Microsoft, votre service IT) ne vous demandera votre mot de passe ou vos numéros de carte par email.

- Le piège : Une page de connexion qui ressemble exactement à celle de Microsoft 365 ou de votre banque.
- Le réflexe : Ne saisissez jamais vos identifiants via un lien reçu par email. Allez directement sur le site officiel en tapant l'adresse dans votre navigateur.

5. Demandes de Coordonnées Bancaires ou Identifiants

Aucune institution sérieuse (Banque, Impôts, Microsoft, votre service IT) ne vous demandera votre mot de passe ou vos numéros de carte par email.

- Le piège : Une page de connexion qui ressemble exactement à celle de Microsoft 365 ou de votre banque.
- Le réflexe : Ne saisissez jamais vos identifiants via un lien reçu par email. Allez directement sur le site officiel en tapant l'adresse dans votre navigateur.

Votre Check-list "Zéro Risque"

Avant de cliquer, posez-vous ces 3 questions :

1. Est-ce que j'attendais cet email ? (Si non = Danger)
2. L'adresse de l'expéditeur est-elle correcte à 100% ? (Vérifiez chaque lettre)
3. Le lien de destination correspond-il au site officiel ? (Survol de la souris)

Que faire si vous avez cliqué ?

Pas de panique, mais agissez vite :

1. Déconnectez immédiatement votre ordinateur du réseau (coupez le Wi-Fi ou débranchez le câble).
2. Prévenez l'équipe IT (ou votre responsable) tout de suite.
3. Changez vos mots de passe depuis un autre appareil (votre smartphone par exemple).

Pourquoi cette fiche est indispensable ?

Le phishing est responsable de plus de 80% des cyberattaques réussies. Transformer vos employés en "pare-feu humains" est l'investissement le plus rentable pour votre sécurité.