CHECKLIST !

DIGITAL FlashUP

CHECKLIST

PHISHING – LES 7 VÉRIFICATIONS À FAIRE AVANT DE CLIQUER

Un concentré d'idées claires et utiles

Gouvernement Princier
PRINCIPAUTÉ DE MONACO
Extended Monaco Entreprise
MONACO BUSINESS OFFICE

Un email vous semble inhabituel ? Prenez 30 secondes avant de cliquer.

Le phishing (ou hameçonnage) consiste à se faire passer pour une personne ou une organisation de confiance afin de vous pousser à **cliquer, ouvrir un fichier, communiquer une information ou effectuer une action**.

Les messages frauduleux sont de plus en plus crédibles. **Une belle mise en page, un logo ou l'absence de fautes d'orthographe ne garantissent pas qu'un message est authentique.**

DIGITAL FlashUP

☐ 1. Regardez l'adresse réelle de l'expéditeur

Ne vous contentez pas du nom affiché.

Exemple

Nom affiché : Banque ABC
Adresse réelle : service-client@banque-abc-securite.com

Le nom semble crédible, mais le domaine utilisé peut ne pas être celui de la banque.

Le réflexe →

Regardez l'adresse complète et, au moindre doute, vérifiez-la par un autre moyen.

☐ 2. Méfiez-vous de l'urgence

> **« Votre compte sera bloqué dans 2 heures. »**
> **« Paiement urgent à effectuer aujourd'hui. »**
> **« J'ai besoin de ces documents immédiatement. »**

Créer de l'urgence ou de la pression vise souvent à vous faire agir **avant de réfléchir**.

Le réflexe → Plus la demande vous presse, plus vous devez prendre le temps de la vérifier.

☐ 3. Vérifiez le lien AVANT de cliquer

Sur ordinateur, **survolez le lien avec votre souris sans cliquer** : l'adresse réelle vers laquelle il mène doit apparaître.

Sur mobile, soyez particulièrement prudent avec les liens dont vous ne pouvez pas facilement vérifier la destination.

Exemple

Texte affiché : Accéder à mon compte

Destination réelle : https://mon-espace-securise.xyz/...

Le réflexe →

En cas de doute, ne passez pas par le lien reçu. Ouvrez vous-même le site ou l'application officielle que vous utilisez habituellement.

☐ 4. Une pièce jointe était-elle vraiment attendue ?

Facture, bon de commande, CV, document partagé, fichier PDF...

Une pièce jointe peut sembler parfaitement professionnelle tout en étant malveillante.

Exemple

Vous recevez une facture d'un fournisseur connu, mais **vous n'attendiez aucune facture**.

Le réflexe →

N'ouvrez pas la pièce jointe avant d'avoir vérifié la demande.

☐ 5. La demande est-elle habituelle ?

L'adresse de l'expéditeur peut être réelle si son compte a été compromis.

Soyez particulièrement vigilant face à :

- un changement de RIB ;
- un virement inhabituel ;
- une demande de mot de passe ou de code d'authentification ;
- l'envoi de données confidentielles ;
- un achat urgent ou inhabituel ;
- une modification soudaine d'une procédure.

Le réflexe → Ne vous demandez pas seulement *« Est-ce vraiment son adresse ? »*, mais aussi **« Est-ce normal qu'il me demande cela ? »**

☐ 6. En cas de doute, vérifiez par un autre canal

Vous recevez un email de votre dirigeant demandant un virement inhabituel ?

Ne répondez pas simplement au message pour demander confirmation.

Si la messagerie a été compromise, vous pourriez toujours communiquer avec l'attaquant.

Le réflexe → Appelez la personne avec un numéro que vous connaissez déjà ou contactez-la par un autre canal habituel.

☐ 7. Signalez plutôt que supprimer

Un email suspect reçu par une personne peut avoir été envoyé à toute l'entreprise.

Le réflexe → Utilisez le bouton de signalement de votre messagerie s'il existe ou transférez le message selon la procédure définie par votre entreprise.

Dans notre entreprise, je signale un message suspect à :

Téléphone / email : _____

Le test des 30 secondes

Avant de cliquer, demandez-vous :

- Je connais l'expéditeur ?
- J'attendais ce message ?
- La demande est habituelle ?
- Le lien mène au bon endroit ?
- La pièce jointe était attendue ?

Un doute ?

Ne cliquez pas. Vérifiez par un autre canal.

DIGITAL FlashUP

Vous avez déjà cliqué ?

N'attendez pas pour agir.

Vous avez seulement ouvert le lien

- Ne saisissez aucune information.
- Fermez la page.
- Signalez l'incident selon la procédure de votre entreprise.

Vous avez saisi votre mot de passe

- Prévenez immédiatement votre responsable informatique ou votre prestataire.
- Changez rapidement le mot de passe compromis depuis un équipement de confiance.
- Si vous utilisez ce même mot de passe ailleurs, changez-le également.
- Vérifiez les connexions et sessions actives lorsque le service le permet.

Vous avez communiqué des informations bancaires

- Contactez immédiatement votre banque ou établissement financier.
- Prévenez votre entreprise.

Vous avez ouvert ou exécuté une pièce jointe suspecte

- Cessez d'utiliser le poste.
- Isolez-le du réseau si une compromission est suspectée.
- Contactez immédiatement votre service ou prestataire informatique.

⚠ **Plus vous signalez rapidement l'incident, plus votre entreprise peut réagir rapidement.**

DIGITAL FlashUP

Le réflexe à retenir

STOP

Quelque chose vous paraît inhabituel ? Ne cliquez pas.

VÉRIFIER

Contrôlez l'expéditeur, le lien et surtout la demande. En cas de doute, utilisez un autre canal.

AGIR

Le message est légitime ? Continuez. Il est suspect ? Signalez-le.

DIGITAL FlashUP

RESTEZ CONNECTÉS

& Boostez vos compétences numériques sur

MONENTREPRISE.GOUV.MC/EME

Gouvernement Princier
PRINCIPAUTÉ DE MONACO

Extended Monaco Entreprise

MONACO BUSINESS OFFICE