SHIRUDO
A CYBERSECURITY
SERIOUS GAME

LES 9 POINTS DE CONTRÔLE D'UN MAIL

#Mission 10

Une réponse négative à l'un des points ci-dessous doit vous rendre vigilant. Deux (ou plus) réponses négatives doivent vous alerter.

Si vous avez le moindre doute, n'ouvrez pas les pièces jointes et ne cliquez sur aucun lien du mail.

Avant l'ouverture du mail :

- ☐ **Origine** : Est-ce que je connais cet expéditeur ?
- ☐ **Adresse** : L'adresse email de l'expéditeur est-elle bien celle habituellement utilisée ?
- ☐ **Objet** : L'objet du mail est-il en lien avec la nature de nos relations habituelles ?

Le contenu du mail :

- ☐ **Interlocuteur** : Suis-je l'interlocuteur le plus approprié ?
- ☐ **Signature** : La signature est-elle identique aux précédentes ?
- ☐ **Contenu** : L'email comporte-t-il des fautes d'orthographe ou de syntaxe ?

Votre intuition !

- ☐ **Nature** : L'intention du mail est-elle en rapport avec notre relation habituelle ?
- ☐ **Émotion** : Puis-je affirmer que je n'éprouve aucun sentiment de crainte, d'empressement ou d'euphorie à la lecture de cet email ?
- ☐ **6ème sens !** : Puis-je affirmer que je n'ai aucun doute à la lecture de ce mail ?

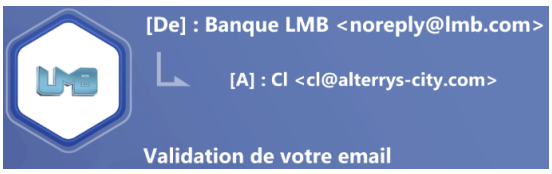
L'émotion est notre pire ennemie dans ce contexte. Le mauvais "clic" peut entraîner votre organisation dans une situation irréversible.

Un doute ? Ne prenez jamais de risque, contactez votre support informatique !

EXEMPLES CONCRETS POUR ILLUSTRER CES POINTS DE CONTROLE

Premier niveau de contrôle : Origine / Adresse / Objet

Ces trois informations sont vérifiables **AVANT** l'ouverture du mail.



- **Origine** : Est-ce que je connais cet expéditeur ?
- **Oui**, c'est bien de votre banque.

Un mail en provenance d'une autre banque serait déjà suspicieux.

- **Adresse** : L'adresse email de l'expéditeur semble-t-elle conforme ?
- **Oui**, c'est bien l'adresse email habituelle.

Une adresse comme « noreply@l-mb.com » serait l'indice d'un email à éliminer en raison du tiret inséré dans le nom de domaine.

Le nom de domaine, est le nom situé après l'@ dans l'adresse mail, ici **lmb.com.** Ce nom est généralement identique au nom du site Internet.

Pour le vérifier, effectuez une recherche de l'organisation (ici la banque LMB) via un moteur de recherche. Comparez alors l'adresse proposée par le moteur de recherche avec le nom domaine de l'email, ils doivent être identiques.

- **Objet** : L'objet est-il en lien avec la nature de nos relations usuelles ?
- **Oui**, vous venez d'obtenir un nouveau compte, de prime abord, l'objet du mail semble conforme à vos relations habituelles.

Pourtant vous aviez déjà reçu un email de validation pour l'activation de votre compte par la banque. Ce second mail est donc un premier indice qui doit vous alerter et vous pousser à éliminer l'email ou à contacter la banque.

Un objet du mail tel que « Validation de vos identifiants » serait définitivement inapproprié de la part d'un établissement de confiance tel qu'une banque.

Deuxième niveau de contrôle : Interlocuteur / Signature / Contenu

Portez votre attention sur l'aspect général du mail

- **Interlocuteur :** Suis-je l'interlocuteur le plus approprié ?
- **Oui**, sans aucun doute. Vous détenez un compte personnel dans cette banque. Il est légitime que la banque s'adresse à vous.

L'adresse email de votre compte est conforme à votre adresse.

Une adresse sous la forme « Cl@alterys-city.com » serait suspicieuse, car dans ce cas le nom de la cité est mal orthographié.

- **Signature** : Est-elle identique aux précédents emails de ce même expéditeur ?
- **Non**, vous constatez ici des erreurs qui doivent irrémédiablement vous pousser à éliminer cet email.

Si l'on compare avec le premier email reçu de la banque, on constate les trois différences encadrées ci-dessous :

- **Contenu** (orthographe et syntaxe) : L'email est-il exempt de faute d'orthographe et de syntaxe ?
- **Oui**, aucune faute n'est visible dans cet email.

Provenant d'un établissement tel qu'une banque, un email avec des fautes serait un critère suffisant pour l'éliminer.

L'analyse du lien « à cliquer » de cet email reste une opération très complexe et il est préférable de vous adresser à des spécialistes.

On notera toutefois ici la présence du « https » et d'un nom de domaine correct « lmb.com » comme des éléments de confiance. À tort, bien entendu !

Troisième niveau de contrôle : Nature / Émotion / 6ème sens

Soyez vigilant, attentif à vos sensations…

- **Nature** : L'intention de l'email est-elle douteuse ?
- **Non**, l'intention est de vous inquiéter en laissant penser qu'une information est manquante et que votre compte pourrait ne pas fonctionner.

L'astuce consiste ici à vous faire valider une information déjà en possession de la banque en vous incitant à cliquer sur un lien.

S'il s'agissait d'une réelle vérification de la part de votre banque, celle-ci vous aurait envoyé un email indiquant qu'à sa connaissance votre email est « CI@alterrys-city.com » et de la contacter si vous constatiez une erreur.

- **Émotion** : Puis-je affirmer que je n'éprouve aucun sentiment de crainte, d'empressement ou d'euphorie à la lecture de cet email ?
- **Non**, l'intention est de vous laisser penser qu'une information est manquante et que votre compte pourrait ne pas fonctionner, de vous contraindre à valider une information déjà en possession de la banque, de cliquer sur un lien.

Vous trouverez souvent des emails proposant des offres promotionnelles, des liens pour consulter des photos d'un évènement, la crainte de voir votre compte clôturé ou supprimé, des demandes charitables…

- **6ème sens :** Puis-je affirmer que je n'ai plus de doute à la lecture de ce mail ?
- **Non**, plusieurs faisceaux d'indices incitent à penser que cet email est vraisemblablement dangereux.

Si vous avez répondu Oui à toutes les questions précédentes, mais que vous hésitez sur cette dernière, même si c'est la plus subjective, **ne prenez aucun risque**. Faites appel à un spécialiste ou appelez l'émetteur de l'email, sans utiliser le numéro de téléphone de l'email douteux qui pourrait vous orienter directement sur les faussaires !

Conclusion

L'analyse et la vérification des liens présents dans un mail **ne suffisent pas** à déterminer avec certitude la présence d'un email de phishing.

Vous devez prendre le temps de contrôler les 3 points de la première thématique AVANT l'ouverture du mail et l'aspect général de celui-ci.