# Cyber Attac chez les particuliers.

## Des signes qui devraient vous alerter :

**Divers exemples de Cyber Attac chez un particulier.**

**Attaque qui vise directement des personnes peu à l'aise avec leur ordinateur ou leur tablette**

- Vous recevez un e-mail ou un appel téléphonique d'une personne déclarant travailler chez Orange.com ou bien être employé à Boursorama banque.

  Comment ils savent que vous êtes chez Orange ? Simplement en regardant l'adresse IP de votre box. Par exemples Orange utilise 80.xx.xx.xx ou 193.xx.xx.xx

  Comment ils savent dans quelle banque vous êtes ? Simplement en récoltant les identifiants de votre carte bancaire qui donnent l'identité de votre banque.

- Ils signalent qu'ils ont détecté des anomalies sur vos transactions et vous demandent si vous avez détecté quelque chose de votre côté. Bien sur vous n'avez rien constaté ni rien fait. Ils vous demandent de vérifier et ils sont prêts à vous aider pour faire cette vérification.

- Si vous acceptez leur aide ils vous envoient un Email et vous demandent d'ouvrir une pièce jointe, ou ils vous demandent de vous rendre sur le site d'un tiers et d'installer un logiciel permettant à une autre personne de visualiser votre écran et de prendre la main sur votre appareil.

- Etc..

Et c'est le climat de confiance que le Cyberattaquant construit avec sa cible qui lui permet de réussir son attaque.
Ce type d'attaque est dérivé de pratiques commerciales de prospection poussées à l'extrême.

**Tentatives de fraudes liées aux abonnements Netflix, Prime, Canal + ou autres:**

Il s'agit par exemple d'appels/textos ou e-mails inattendus qui font référence à des frais d'adhésion élevés ou à un problème lié à votre adhésion et qui vous demandent de confirmer ou d'annuler les frais. Ces fraudeurs tentent de vous convaincre de leur fournir des informations de paiement ou de compte bancaire en prétendant rétablir votre adhésion.

**Tentatives d'escroqueries liées à la confirmation d'une commande :**

Il s'agit par exemple d'appels/textes/e-mails inattendus qui font souvent référence à un prétendu achat non autorisé et qui vous demandent d'agir de toute urgence pour confirmer ou annuler l'achat. Ces fraudeurs tentent de vous convaincre de fournir des informations de

paiement ou de compte bancaire, d'installer un logiciel sur votre ordinateur/appareil ou d'acheter des cartes-cadeaux.

Actuellement, mais aussi fréquemment avant les fêtes de Noel vous recevez simplement un Email vous signalant que votre colis n'est pas livré et on vous demande de cliquer un lien pour donner des informations complémentaires pour la livraison.

Dans ce cas c'est simplement l'envoie d'Email en masse sachant que X personnes sur 100 ont des commandes Internet en attente de livraisons avant les fêtes de fin d'année.

**Tentatives d'escroqueries liées à la livraison d'une commande :**

C'est la tentative la plus fréquente actuellement. Dès qu'un colis est déposé dans votre boite aux lettre (ou livré à vous-même), dans la demi-heure qui suit vous recevez un SMS sur votre téléphone personnel vous demandant de payer quelques Euros de frais de douane car le produit que vous avez reçu vient de l'étranger. Et bien sûr vous devez cliquer sur le lien proposé par le SMS. (Votre numéro de téléphone a été donné au livreur en cas de difficulté de livraison). Ce n'est pas tant le petit montant qui intéresse les escrocs mais surtout vos coordonnées bancaires. Bien sûr, là encore, il faut une complicité interne dans l'entreprise ou bien c'est simplement le livreur qui prévient un de ses copains quand la livraison est faite.

**Autre exemple ingénierie sociale.**

Vous êtes responsable d'un service informatique qui gère des réservations de vacances.

Un client vous contacte pour vous fait part d'une inquiétude concernant son prochain séjour. Cette personne est gravement malade et est allergique à certains produits de nettoyage. Elle vous demande donc de consulter son certificat médical pour vérifier que votre établissement n'utilise aucun produit qui pourrait aggraver son état de santé. Elle vous envoie un lien permettant de télécharger ce certificat. Etc….

**Pourquoi c'est important pour vous qui serez, un jour, responsable informatique ?**

Prenons un exemple :

Vous êtes responsable informatique d'une PME qui fabrique des volets roulants.

Un client vous interpelle car il a répondu à un Email qu'il pensait venir de votre part sur une livraison de pièces détachées qu'il n'avait encore reçu. Et c'était malheureusement une arnaque et il vous met en cause car une commande était en attente chez vous.

Vous devez prouver que de votre coté toutes les procédures de sécurité internes à votre entreprise ont bien été mise en place, que les mots de passe sont bien sécurisés, que cela ne pouvait en aucun cas provenir de votre entreprise (traçabilité des appels et des Mails) etc……

Mais vous devez aussi (et surtout) vous inquiéter de la manière dont votre client a été contacté par quelqu'un qui se faisait passer pour votre entreprise. (tel , Mail, SMS ) . Qui a accès à ces informations dans votre entreprise ? Vous allez donc être obligé de vérifier tous les ordinateurs de votre entreprise …(voir le fiche suivante comment faire)…