# Document d'information, Boîte à outils de cybersécurité de la GCA : Protéger vos e-mails et votre réputation

Les e-mails sont largement utilisés pour amorcer une cyberattaque. Il est extrêmement rapide et peu coûteux d'envoyer des milliers d'e-mails à des destinataires peu méfiants dans l'espoir que certains d'entre eux croient qu'ils sont authentiques et cliquent sur le lien du site web malveillant ou téléchargent la pièce jointe dangereuse.

Votre système informatique pourrait être infecté par un certain type de programme malveillant ou de ransomware, permettant au criminel de voler vos données importantes ou de transférer votre argent vers des comptes frauduleux. Le criminel serait également en mesure de prendre le contrôle de vos systèmes et de trafiquer vos coordonnées bancaires, de sorte que les clients effectuent des paiements sur d'autres comptes en pensant qu'il s'agit de votre compte.

L'utilisation d'e-mails d'hameçonnage est extrêmement efficace pour les criminels : ils peuvent toucher des milliers de victimes potentielles très rapidement. Pour que leur attaque réussisse, l'apparence de l'e-mail doit cependant laisser penser qu'il provient d'une source légitime.

Les méthodes utilisées par les criminels sont multiples :

- **Spoofing par imitation du nom de l'expéditeur**
  - Nom affiché dans la zone de l'expéditeur : ***« Commerce »***
  - Adresse e-mail : <personne@yahoo.com>
    - *Survolez le nom de l'expéditeur à l'aide du curseur pour vérifier l'adresse réelle avant de continuer.*

- **Spoofing par imitation du nom de domaine**
  - Nom affiché dans la zone de l'expéditeur : ***« Commerce »***
  - Adresse e-mail : <personne@c**0rn**merce.com>
    - *Vérifiez attentivement l'adresse e-mail avant de continuer.*

- **Spoofing par usurpation du nom de domaine**
  - Nom affiché dans la zone de l'expéditeur : ***« Commerce »***
  - Adresse e-mail : <personne**@commerce.com**>
    - *Utilisez DMARC pour vous protéger contre l'usurpation de nom de domaine.*

Même après avoir vérifié et revérifié, agissez toujours avec prudence et utilisez d'autres méthodes pour garantir la légitimité de l'e-mail si vous avez un doute (appelez par exemple l'expéditeur pour lui demander s'il vous a bien envoyé l'e-mail).

Si vous vous retrouvez sans défense contre une attaque par usurpation du nom de domaine :

- Les attaquants peuvent se faire passer pour vous ou votre fournisseur/client pour demander un paiement ou passer des commandes.

- Les attaquants peuvent également se faire passer pour d'autres membres de votre organisation.

Ils peuvent commettre les délits suivants :

- **CEO Fraud (fraude au président)** : un e-mail est envoyé en se faisant passer pour le PDG ou une personne habilitée haut placée. Dans la plupart des cas, l'e-mail demande à un collègue d'effectuer un paiement immédiatement.
    - *Faites comprendre à vos employés qu'il est recommandé de procéder à une double vérification. Les entreprises familiales fonctionnent souvent sur le principe de la confiance et contrôlent peu : les attaquants en profiteront.*

- **Piratage de messagerie en entreprise (BEC, business email compromise)** : un e-mail est envoyé à partir d'un compte de messagerie dont la sécurité a été compromise. Il est envoyé « au sein de l'organisation » ou utilise un nom de domaine légitime (spoofing par usurpation du nom de domaine). Ces e-mails peuvent être destinés à des fournisseurs ou des clients et demander un paiement vers un compte dont les coordonnées bancaires ont été modifiées. Étant donné que l'attaquant se trouve « au sein de l'organisation », les e-mails paraissent plus authentiques et utilisent certaines techniques d'authentification qui permettent de valider les détails de l'expéditeur, les rendant ainsi plus difficiles à repérer. L'attaquant a pu surveiller les communications et s'être infiltré dans le système depuis un certain temps : il aura donc rassemblé beaucoup d'informations.
    - *Utilisez DMARC pour éviter que la sécurité de vos données soit compromise en premier lieu, si la technique du spoofing par usurpation du nom de domaine est utilisée.*
    - *Utilisez des mots de passe forts et des mécanismes d'authentification à plusieurs facteurs pour réduire les risques de compromettre la sécurité de vos comptes.*
    - *Vérifiez régulièrement les paramètres de votre compte de messagerie pour garantir que les e-mails ne sont pas transférés vers une adresse e-mail inconnue.*
    - *Mettez en place une politique permettant de vérifier tous les détails des nouveaux fournisseurs et clients en utilisant au moins deux méthodes différentes. Si une modification est apportée, procédez toujours à une vérification en utilisant une méthode alternative connue (p. ex., composez un numéro de téléphone que vous connaissez ou passez par un standard connu ; ne vous fiez pas uniquement au contenu de la signature, car ces informations peuvent également avoir été modifiées).*

**DMARC (Domain-Based Message Authentication, Reporting and Conformance, authentification des messages basée sur un domaine, génération de rapports et conformité)**
Une politique DMARC permet à un expéditeur d'attester que ses messages sont protégés et indique au destinataire ce qu'il doit faire si l'une des méthodes d'authentification réussit ou échoue.

DMARC :

- Empêche un imposteur de « se faire passer pour vous » dans un e-mail.
- Vous évite de recevoir un e-mail d'un imposteur.
- Fournit des renseignements sur les tentatives d'envoi de courrier indésirable, d'hameçonnage ou d'hameçonnage ciblé à l'aide du domaine de messagerie de votre organisation par le biais de rapports.
- Renforce la confiance vis-à-vis des clients et de la chaîne d'approvisionnement.

Toutefois :

- Pour que DMARC soit efficace, l'expéditeur et le destinataire doivent avoir mis en place une politique DMARC valide et une vérification DMARC.

- Si le client et le fournisseur utilisent DMARC, ils sont ***tous les deux*** PROTÉGÉS contre l'usurpation de domaine de messagerie. Si un seul d'entre eux utilise DMARC, aucun des deux n'est protégé.

- Ce qui advient de l'e-mail une fois reçu dépend de la façon dont la politique DMARC de l'expéditeur a été configurée.

**Utilisez les outils de la boîte à outils Protéger vos e-mails et votre réputation pour en savoir plus sur DMARC et pour le configurer sur votre domaine de messagerie.**

**https://gcatoolkit.org/fr/petites-entreprises/proteger-vos-emails-et-votre-reputation/**