

# Apprendre à reconnaître un email de spear phishing

1

## Adresse de l'expéditeur

Lors d'une attaque de Spear Phishing les hackers ont recours à différentes techniques d'usurpation pour faire croire à leur victime qu'une adresse email est légitime. Ils utilisent par exemple un nom d'expéditeur imitant l'identité d'un collègue. Si vous êtes sur un appareil mobile, pensez à afficher le nom de l'expéditeur pour vérifier son adresse intégralement et valider que l'email correspond bien au nom qui s'affiche. En outre, vérifiez s'il n'y a pas de légères différences dans le nom de domaine.

2

## Objet

Les objets des emails de spear phishing sont souvent formulés de sorte à attirer l'attention de leur victime ou créer un sentiment d'urgence. Les hackers les plus doués peuvent se montrer plus subtiles, mais l'objet contiendra sans doute des termes liés à des notions financières, comme « achat », « facture », « virement », etc.

3

## Pretexting

Le pretexting est une forme d'ingénierie sociale consistant à gagner la confiance d'un utilisateur via un ou plusieurs emails. Le hacker s'appuie sur les informations dont il dispose sur sa victime pour faire la conversation et l'inciter à relâcher sa vigilance : « Comment se sont passées vos vacances ? », « Félicitations pour votre promotion ».

4

## Corps « de l'email »

Le corps de l'email est concis et contient la plupart du temps une demande d'ordre financier. Les hackers emploient souvent des formulations conçues pour que leur victime ait l'impression d'être la seule personne en mesure d'accéder à leur demande et que tout délai pourrait nuire à l'entreprise.

5

## Signature

Bien souvent, le hacker ajoute une ligne dans la signature indiquant que le message a été rédigé depuis un smartphone ou une tablette. Ce détail permet de renforcer l'urgence du message, offre une excuse justifiant l'envoi de l'email depuis une adresse personnelle et permet d'expliquer les éventuelles erreurs de grammaire ou de style.



## En cas de doute, vérifiez :

Si vous recevez un email qui vous laisse penser qu'il peut s'agir d'un spear phishing, nous vous conseillons de le transmettre à votre Administrateur IT ou à votre Partenaire MSP pour vérification.