Vade Secure
Predictive Email Defense

Apprendre à reconnaître **un email de spear phishing**

1 Adresse de l'expéditeur

Les hackers ont recours à diverses techniques d'usurpation pour faire croire à leurs victimes qu'une adresse email est légitime. Étudiez avec soin l'adresse des emails que vous recevez pour détecter d'éventuelles différences subtiles avec le nom de domaine attendu. Si vous utilisez un appareil mobile, pensez à développer le nom de l'expéditeur pour voir l'intégralité de l'adresse.

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

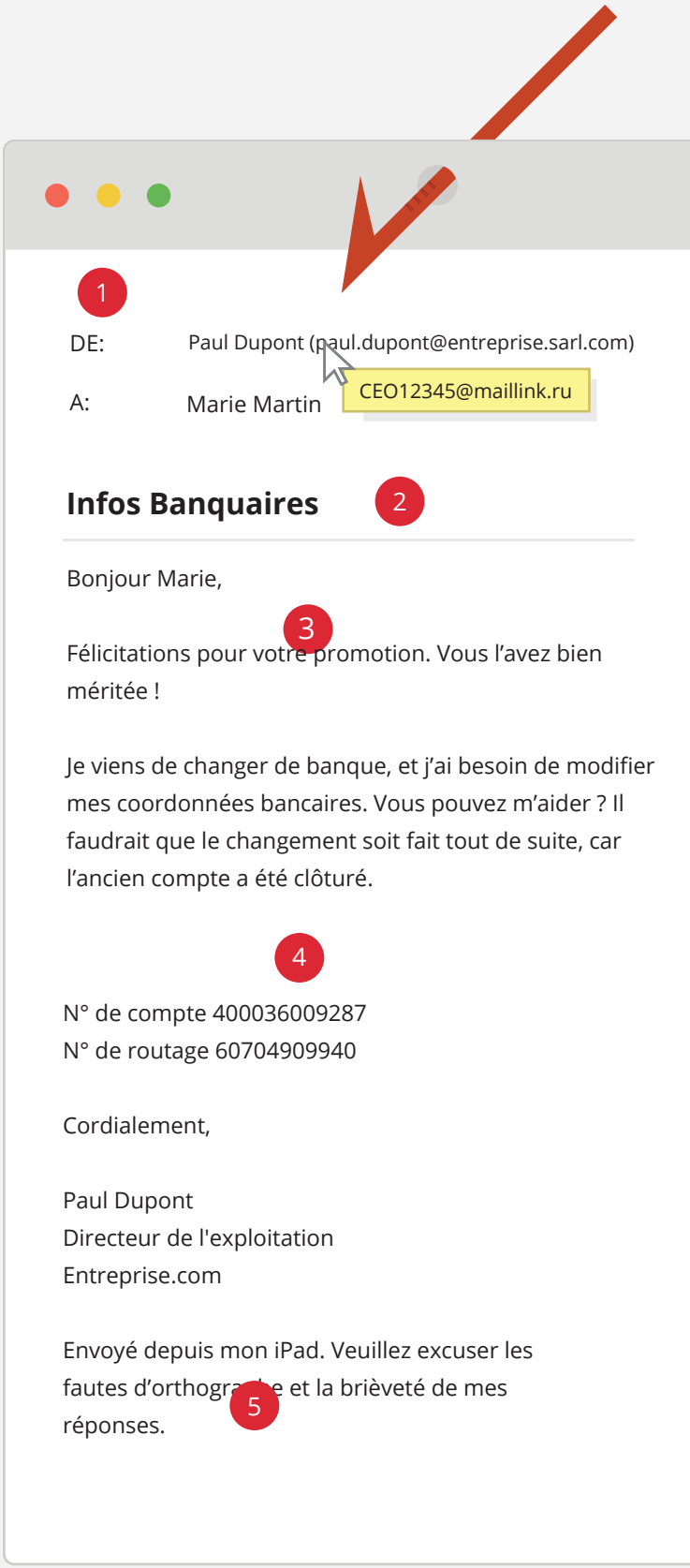
Le pretexting est une forme d'ingénierie sociale consistant à gagner la confiance d'un utilisateur en un ou plusieurs emails. Le hacker s'appuie sur les informations dont il dispose sur sa victime pour faire la conversation et l'inciter à relâcher sa vigilance : « Comment se sont passées vos vacances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

4 Corps

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 message qui, à votre avis, est du spear phishing, nous vous recommandons de le transférer à votre MSP ou à votre administrateur informatique pour complément d'enquête.

© Vade Secure