Phishing (hameçonnage)

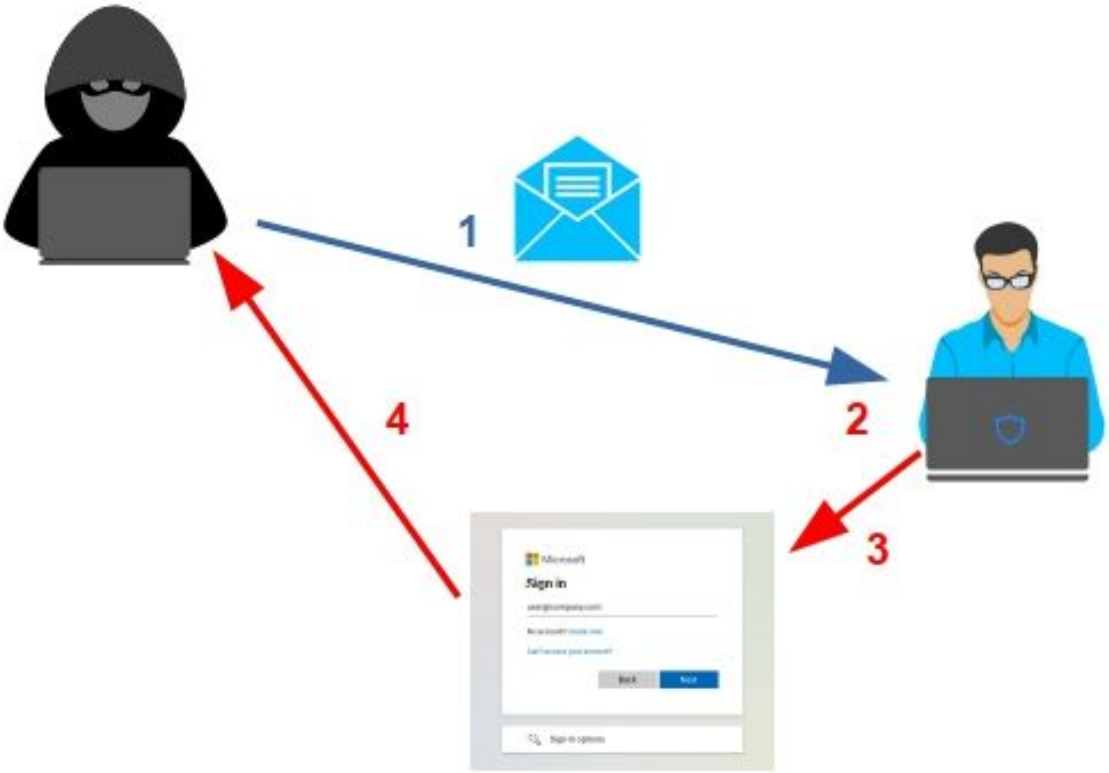
L'hameçonnage ou phishing est actuellement le moyen le plus courant d'introduire un rançongiciel (ransomware) dans votre ordinateur ou votre réseau, ou de vous faire voler vos données. Selon un rapport de Guardian Digital, 91 % des cyberattaques réussies commencent par un e-mail de phishing.

Malgré le nombre important de solutions technologiques conçues pour contrer les attaques de phishing, des logiciels antimalware à l'authentification multifacteur, la meilleure défense contre le phishing est la sensibilisation de l'utilisateur. En effet, une attaque de phishing réussie nécessite toujours que l'utilisateur effectue une action, comme saisir ses identifiants dans un formulaire ou cliquer sur un lien dangereux.

Lisez la suite pour voir comment vous pouvez détecter et agir sur le phishing de base.

Comment fonctionne le phishing

1. L'attaquant envoie un email de phishing comprenant un lien vers un site frauduleux.
2. L'utilisateur reçoit l'email et clique sur le lien.
3. L'utilisateur est redirigé vers un site contrôlé par l'attaquant, imitant un site légitime, et saisit son nom d'utilisateur et son mot de passe.
4. Le site malveillant envoie le nom d'utilisateur et le mot de passe à l'attaquant.

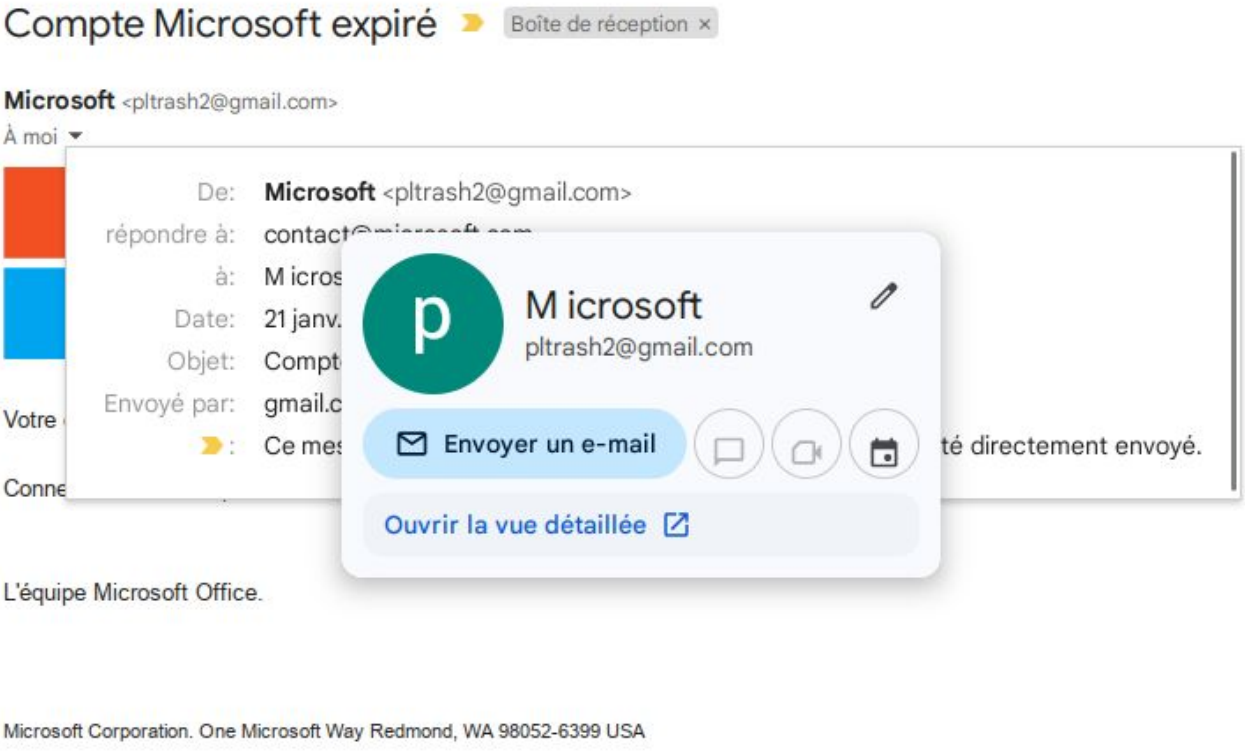


Comment éviter le phishing en tant qu'utilisateur

Plusieurs éléments peuvent vous alerter sur la légitimité de l'email.

Vérifiez l'adresse de l'expéditeur

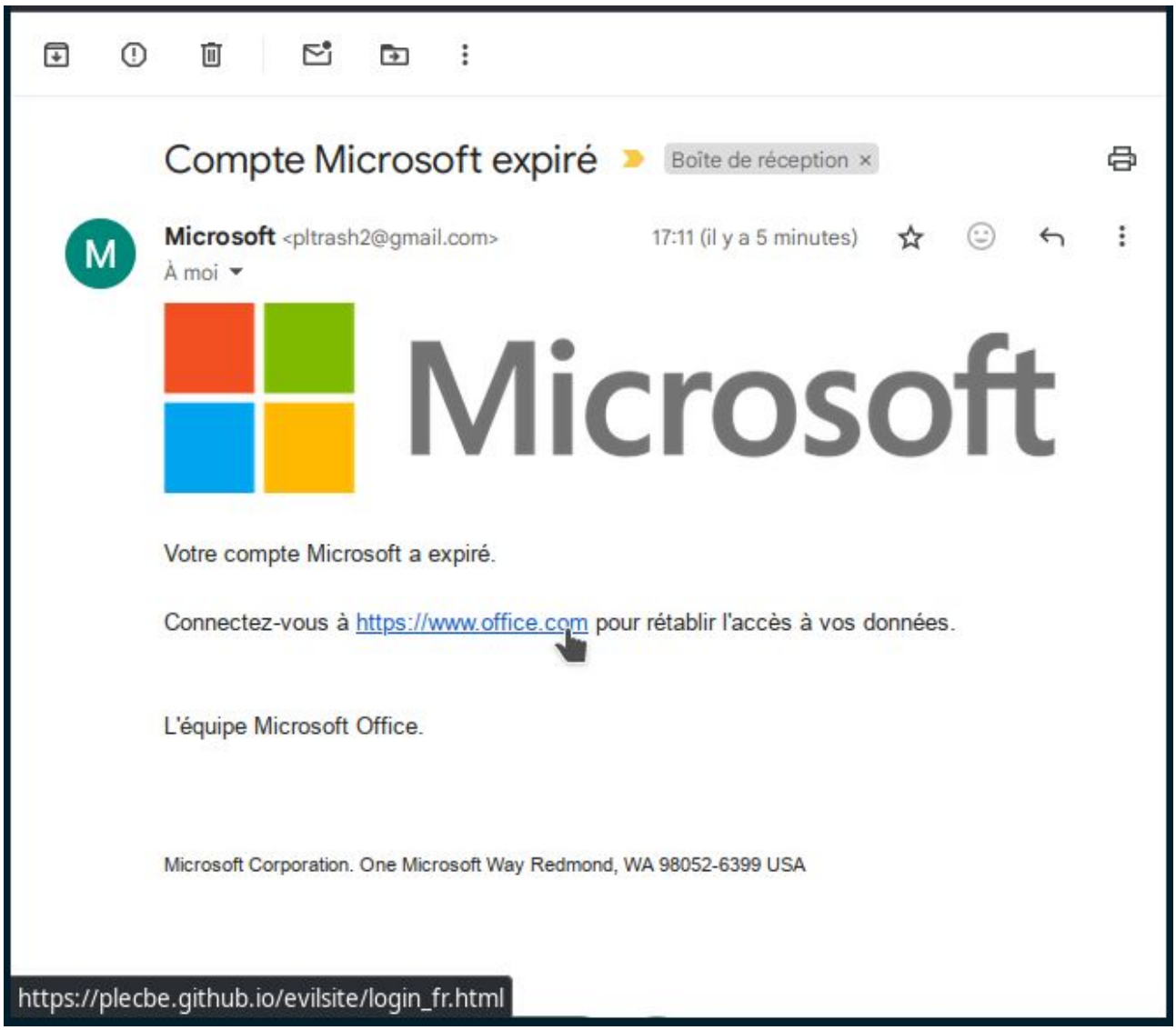
Un courriel peut contenir 2 adresses pour l'expéditeur : la « vraie » adresse, utilisée pour se connecter à son système de messagerie, et une autre, appelée nom d'affichage, qui peut généralement être définie librement. Dans Gmail, elle peut être affichée par défaut, ou un clic sur la flèche vers le bas à côté du nom du destinataire révèle l'adresse réelle de l'expéditeur, écrite entre crochets (<>).



Dans cet exemple, le vrai nom de l'expéditeur est *pltrash2@gmail.com*, mais j'ai modifié le nom d'affichage pour qu'il ressemble à un nom légitime. Si les 2 noms sont différents et que le « vrai » nom de l'expéditeur ne correspond pas à une personne ou une entreprise connue, méfiez-vous !

Vérifiez le lien

Les liens ne sont pas toujours ce qu'ils semblent être. Le texte qu'ils présentent n'est pas toujours la véritable destination vers laquelle ils renvoient. Si vous passez la souris sur le lien, il révélera sa véritable destination. Regardez dans le coin inférieur gauche.



Dans cet exemple, le lien semble vous diriger vers un site Microsoft (*www.office.com*), alors qu'il redirige vers un site malveillant, imitant potentiellement le véritable écran de connexion Microsoft et capturant vos identifiants.

Comment lutter contre le phishing en tant qu'utilisateur averti

- Utilisez un logiciel antiphishing.
- Ajoutez les domaines frauduleux à vos filtres de messagerie, proxys, DNS, pare-feu.
- Formez vos utilisateurs.
- Signalez les emails de phishing aux autorités.
- Signalez les emails de phishing aux propriétaires de domaines.
- Signalez les sites de phishing aux éditeurs de navigateurs.
- Signalez les sites de phishing au bureau d'enregistrement de noms de domaines ou à l'hébergeur.

Toutes ces actions seront expliquées dans les prochains articles du blog.