Comment reconnaitre un hameçonnage (*phishing*)

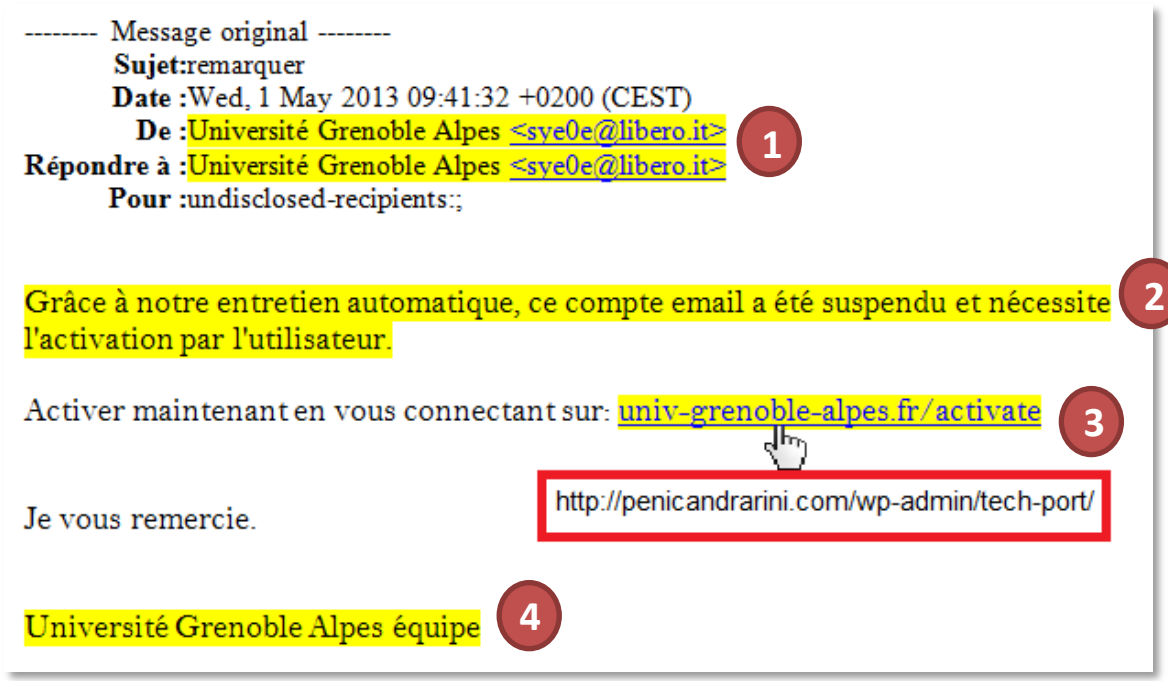
Parmi les nombreux courriels indésirables, certains sont plus pernicieux que d'autres puisqu'ils vont inciter le destinataire du message à divulguer des renseignements personnels dans le but de réaliser une usurpation d'identité. Ces messages d'hameçonnage, *phishing* en anglais, vont essayer de collecter directement ou en se faisant passer pour un tiers de confiance, des données personnelles telles qu'identifiant et mot de passe, coordonnées bancaires, etc.

Cette technique d'ingénierie sociale, quand elle est diffusée par messagerie électronique, se base sur plusieurs éléments :

- elle va profiter de la lecture souvent trop rapide du message ;
- elle va jouer sur une notion d'immédiateté de la réponse, sous peine de perdre un service ;
- elle peut jouer sur la curiosité face à une catastrophe, ou un événement très médiatisé...

Voici quelques pistes pour reconnaître de tels messages. Les exemples sont donnés sur des campagnes reçues à l'Université, et qui ont, malheureusement, conduits à des fuites d'identifiants.

Exemple de message n°1 :



Outre le fait que la DSI ne vous demandera jamais vos identifiants login/mot de passe dans un message, voici ce qui devrait vous alerter pour reconnaître ou au moins suspecter un mail d'hameçonnage (*phishing*) :

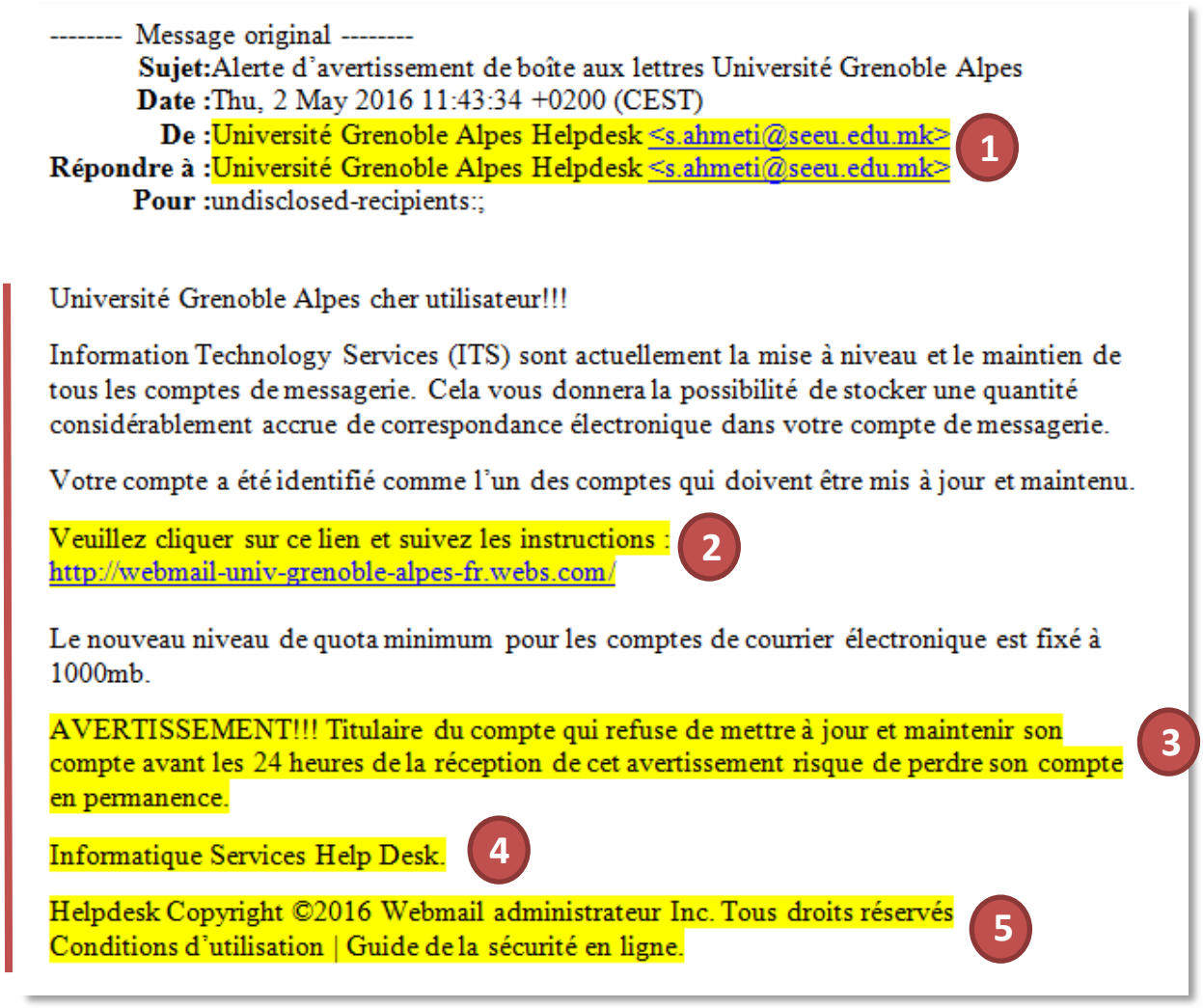
1. Bien que l'adresse d'expéditeur soit aisément falsifiable, ici le fait qu'elle appartienne à un site italien (.it) et non au domaine univ-grenoble-alpes.fr doit nous alerter.

2. Généralement, les *phishing* jouent beaucoup sur une immédiateté des décisions à prendre, pour éviter de perdre un service, et c'est le cas ici.

3. En **passant** la souris sur le lien, on voit s'afficher dans la barre de navigation (en bas de la page) la véritable adresse du lien ici http://penicandrarini.com/wp-admin/tech-port/ qui, bien sûr, n'est pas un site de l'Université Grenoble Alpes.

4. Une signature générique très vague, avec une tournure peu française, alors que les messages de la DSI sont généralement signés nominativement, avec l'adresse et le téléphone de la DSI.

Exemple de message n°2 :



-------- Message original --------
Sujet: Alerte d'avertissement de boîte aux lettres Université Grenoble Alpes
Date : Thu, 2 May 2016 11:43:34 +0200 (CEST)
De : Université Grenoble Alpes Helpdesk <s.ahmeti@seeu.edu.mk> 1
Répondre à : Université Grenoble Alpes Helpdesk <s.ahmeti@seeu.edu.mk>
Pour :undisclosed-recipients:;

Université Grenoble Alpes cher utilisateur!!!

Information Technology Services (ITS) sont actuellement la mise à niveau et le maintien de tous les comptes de messagerie. Cela vous donnera la possibilité de stocker une quantité considérablement accrue de correspondance électronique dans votre compte de messagerie.

Votre compte a été identifié comme l'un des comptes qui doivent être mis à jour et maintenu.

6 Veuillez cliquer sur ce lien et suivez les instructions : 2
http://webmail-univ-grenoble-alpes-fr.webs.com/

Le nouveau niveau de quota minimum pour les comptes de courrier électronique est fixé à 1000mb.

AVERTISSEMENT!!! Titulaire du compte qui refuse de mettre à jour et maintenir son compte avant les 24 heures de la réception de cet avertissement risque de perdre son compte en permanence. 3

Informatique Services Help Desk. 4

Helpdesk Copyright ©2016 Webmail administrateur Inc. Tous droits réservés
Conditions d'utilisation | Guide de la sécurité en ligne. 5

Outre le fait que la DSI ne vous demandera jamais vos identifiants login/mot de passe dans un message, voici ce qui devrait vous alerter pour reconnaître ou au moins suspecter un mail d'hameçonnage (*phishing*) :
1. Bien que l'adresse d'expéditeur soit aisément falsifiable (c'est le cas ici pour la première partie *Université Grenoble Alpes Helpdesk*), la seconde partie (s.ahmeti@seeu.edu.mk) renvoie à un domaine macédonien (.mk), et non au domaine univ-grenoble-alpes.fr. Cela doit nous alerter.

2. Le nom du lien doit nous alerter. Il contient bien univ-grenoble-alpes.fr, mais est suffixé par quelque-chose d'étranger (ici **.webs.com**). Il ne renverra donc pas vers l'Université Grenoble Alpes.

3. Généralement les *phishing* jouent beaucoup sur l'immédiateté d'une réponse à donner, pour éviter de perdre un service, et c'est le cas ici.

4. Une signature générique très vague, alors que les messages de la DSI sont généralement signés nominativement, avec l'adresse et le téléphone de la DSI.

5. Un copyright très étrange.

6. Le texte est en français approximatif, sûrement issu d'un traducteur automatique.