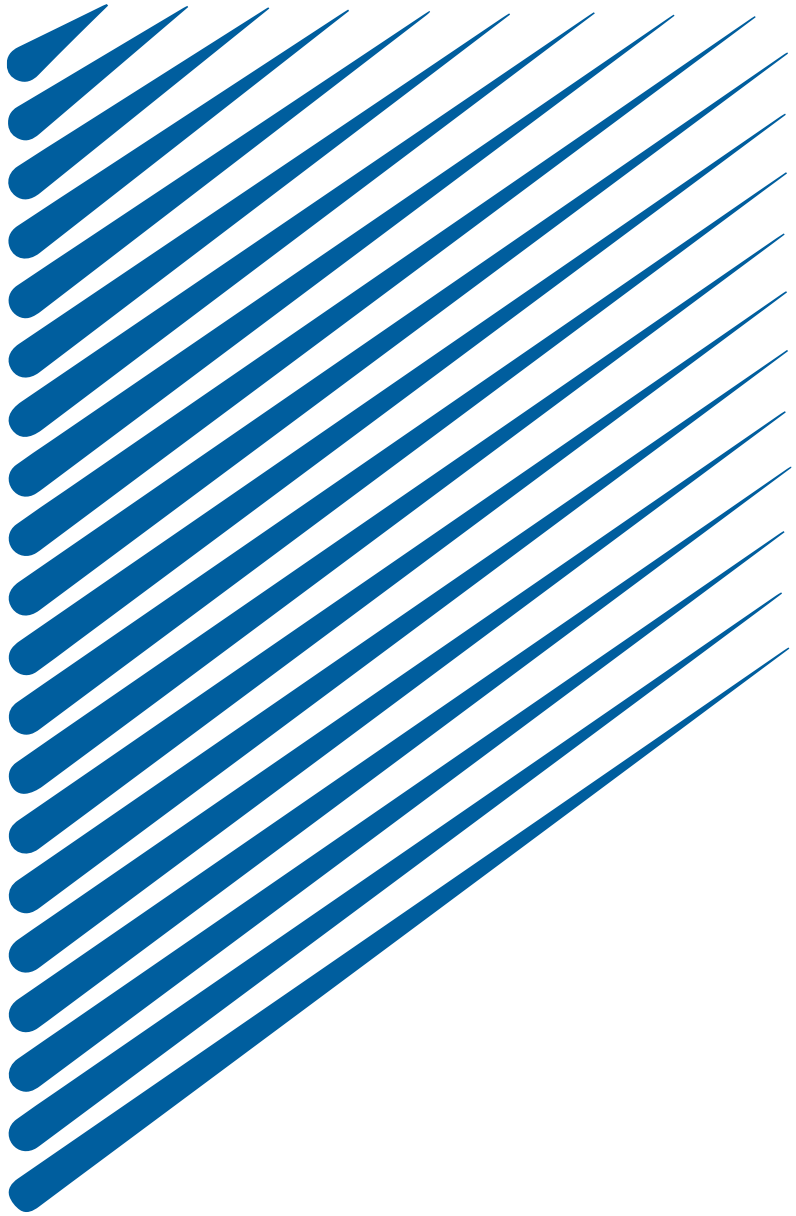


MINES PARIS | PSL

WORKSHOP SSI

Hameçonnage (Phishing)

27 & 28 Novembre 2023

SOMMAIRE

CONTEXTE

- Plus de 90% des attaques informatiques passent par la messagerie
- Augmentation très significative des campagnes d'hameçonnage depuis ces 2 dernières années.

- Les motivations principales sont :
  - Appât du gain
  - Nuisance
  - Espionnage
  - Atteinte à l'image d'une personne ou d'un établissement
  - Revendication/activisme
  - Sabotage
- Ce phénomène se développe énormément également par SMS on parle de "SMISHING"

LES CONSÉQUENCES

Prise de contrôle de votre boite mail, de votre système ou d'autres ressources

Envois de spams ou nouveaux phishings en interne

Mais aussi accès à des informations sensibles ou confidentielles, ou d'attaques plus sophistiquées

-> informations ou documents permettant l'usurpation d'identité

-> données bancaires

-> accès à d'autres ressources (cloud, réseau wifi Eduoram, accès distant, …) et applications mais aussi des attaques plus complexes, via des mécanismes d'exploitation de failles de sécurité ou d'élévation de privilèges

RECONNAITRE UN MESSAGE D'HAMMECONNAGE

L’attaquant se fait passer pour une personne ou un tiers de confiance.

Selon le niveau de sophistication et d'ingénierie sociale, il usurpe des noms, adresses mails et logo crédibles ou utilise une boite mail compromise pour envoyer les messages afin de mieux tromper ses victimes pour cliquer sur les liens ou les pièces jointes. Allant jusqu’à recopier parfaitement un message ou une newsletter d'un organisme.

•Ces messages utilisent principalement les mêmes registres dans leur contenu ou objet du message:

- Une proposition trop alléchante
- La migration d'un service ou l'accès à un nouveau service
- La peur, via la perte d'accès à un service "si vous ne cliquez pas sur le lien contenu dans un message"
- Utilisation de phrase type:
  - "Action immédiate requise,"
  - "Vous avez été piraté" ,"
  - "il y a un problème de sécurité", "vous devez revalidez vos accès" …

RECONNAITRE UN MESSAGE D'HAMMECONNAGE

- En fonction de votre logiciel de messagerie, l'adresse de l'expéditeur affichée est partielle et n'affiche que nom de la personne ou une adresse générique. Les fraudeurs utilisent souvent ce champ pour usurper le nom d'une société ou d'une personne dans l'envoi des messages malveillants.

L'attaquant peut planifier sa campagne de phishing en utilisant un timing adapté,

exemple: le phishing imitant le site de l'ENSAP en fin de mois pour coïncider avec les bulletins de paie

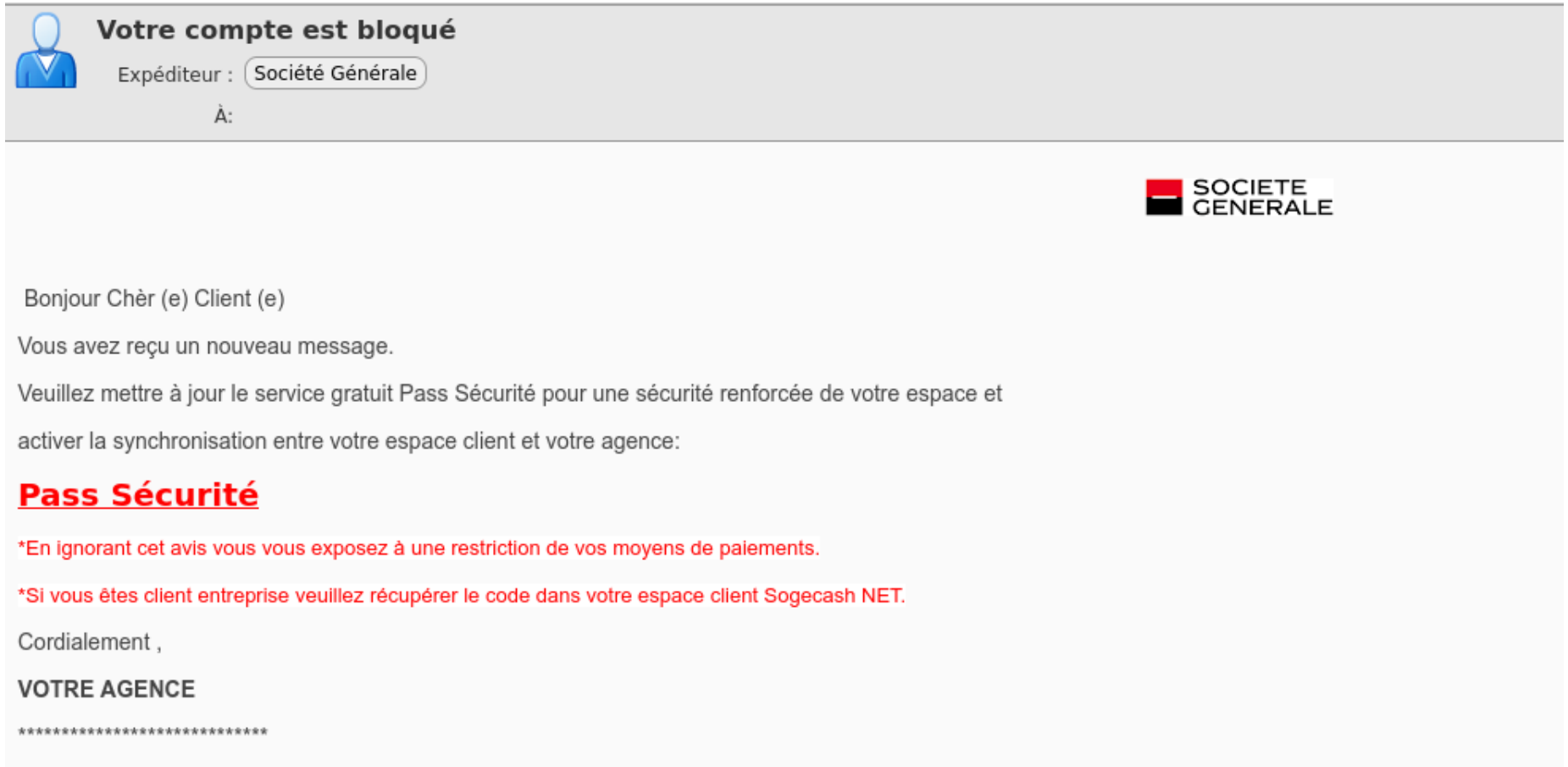
une notification pour la réception d'un colis …ou sur un projet donc l'actualité est disponible sur des sites web.

Analyser en détails l'adresse de l'expéditeur et les liens à l'aide du curseur de la souris permet de détecter une grande majorité des messages de "phishing".

Se méfier des liens utilisant des systèmes de raccourcissement d'URL, qui sont souvent utiliser pour masquer l'adresse du lien.

Le premier réflexe est de s'interroger sur l'expéditeur et la nature du message

RECONNAITRE UN MESSAGE D'HAMMECONNAGE



Votre compte est bloqué

Expéditeur : Société Générale

À:

SOCIETE GENERALE

Bonjour Chèr (e) Client (e)

Vous avez reçu un nouveau message.

Veuillez mettre à jour le service gratuit Pass Sécurité pour une sécurité renforcée de votre espace et activer la synchronisation entre votre espace client et votre agence:

Pass Sécurité

*En ignorant cet avis vous vous exposez à une restriction de vos moyens de paiements.

*Si vous êtes client entreprise veuillez récupérer le code dans votre espace client Sogecash NET.

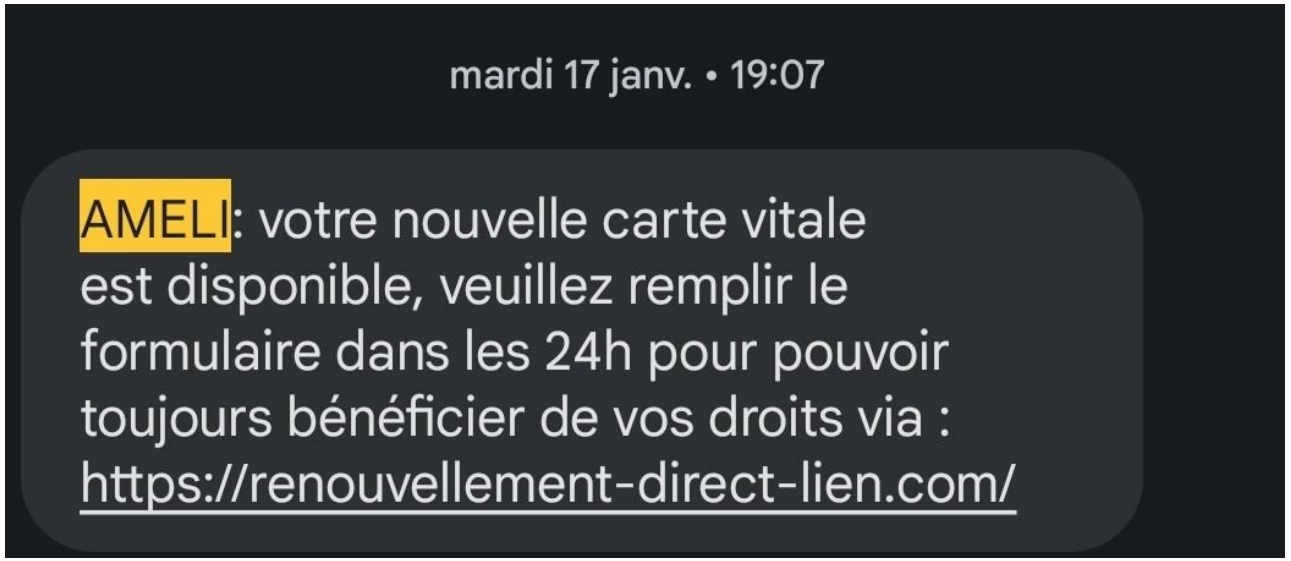
Cordialement ,

VOTRE AGENCE

****

RECONNAITRE UN MESSAGE D'HAMMECONNAGE

Les messages par SMS peuvent être plus difficile à identifier , le numéro d'envoi étant masqué par l'attaquant via un numéro abrégé ou un nom de service ou d'entité commerciale



RECONNAITRE UN MESSAGE D'HAMMECONNAGE

TR/INFRA/JUD N°250920221110

Expéditeur : Cador Maud

LOGODELIT.docx (2,2 Mo) Aperçu | Télécharger | Porte-documents | Supprimer

IMPORANT:DOCUMENT EN FICHIER JOINT.

Vous avez une réquisition JUDlClAlRE pour une infraction commise*.**

nous vous prions de répondre à l'adresse du bureau bien attendu
en stipulant vos justifications pour qu'elles soient mise en examen et vérifié afin d'évaluer
vos sanctions.

L'ADRESSE MAIL DU BUREAU: ***POLICE@ POLICEMINEURS.COM***

--
Maud CADOR COLLET
Chargée de communication

POLICE
NATIONALE

--
Maud CADOR COLLET
Conseillère Principale d'Education

Collège Alfred de MUSSET
Route du pont,
45310 PATAY

RECONNAITRE UN MESSAGE D'HAMMECONNAGE

NOTIFICATION ALERTE DE VOTRE MESSAGERIE ***ACTI0N REQUISE

Expéditeur : Darreye Camille

MESSAGERIE - REVALIDATION.

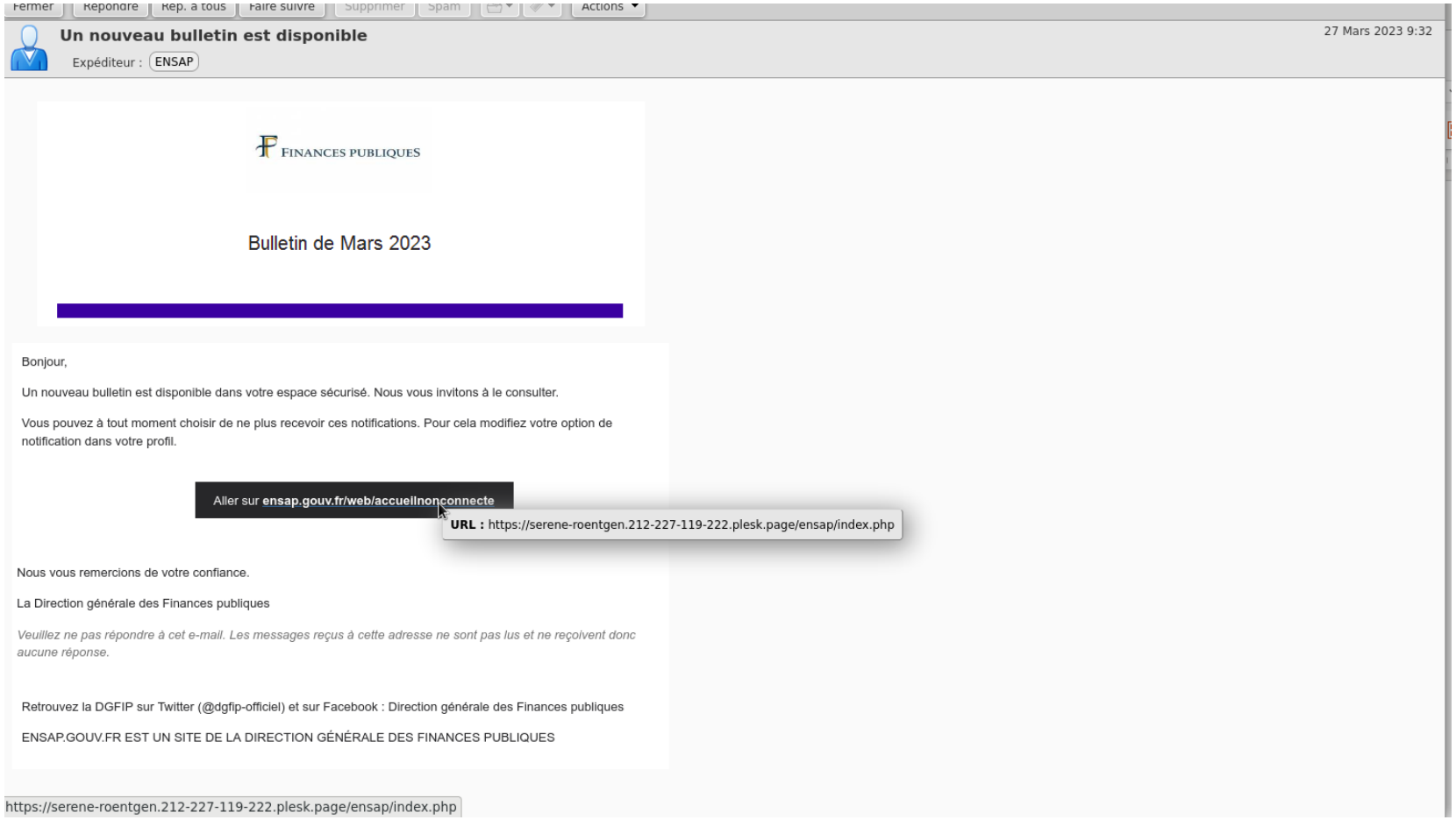
Suite à une mîse à jour de nos services, des travaux seront effectués sur le serveur de notre messagerie.

Pour éviter que votre compte soit suspendu, veuillez confirmer l'utilisation de votre adresse email.

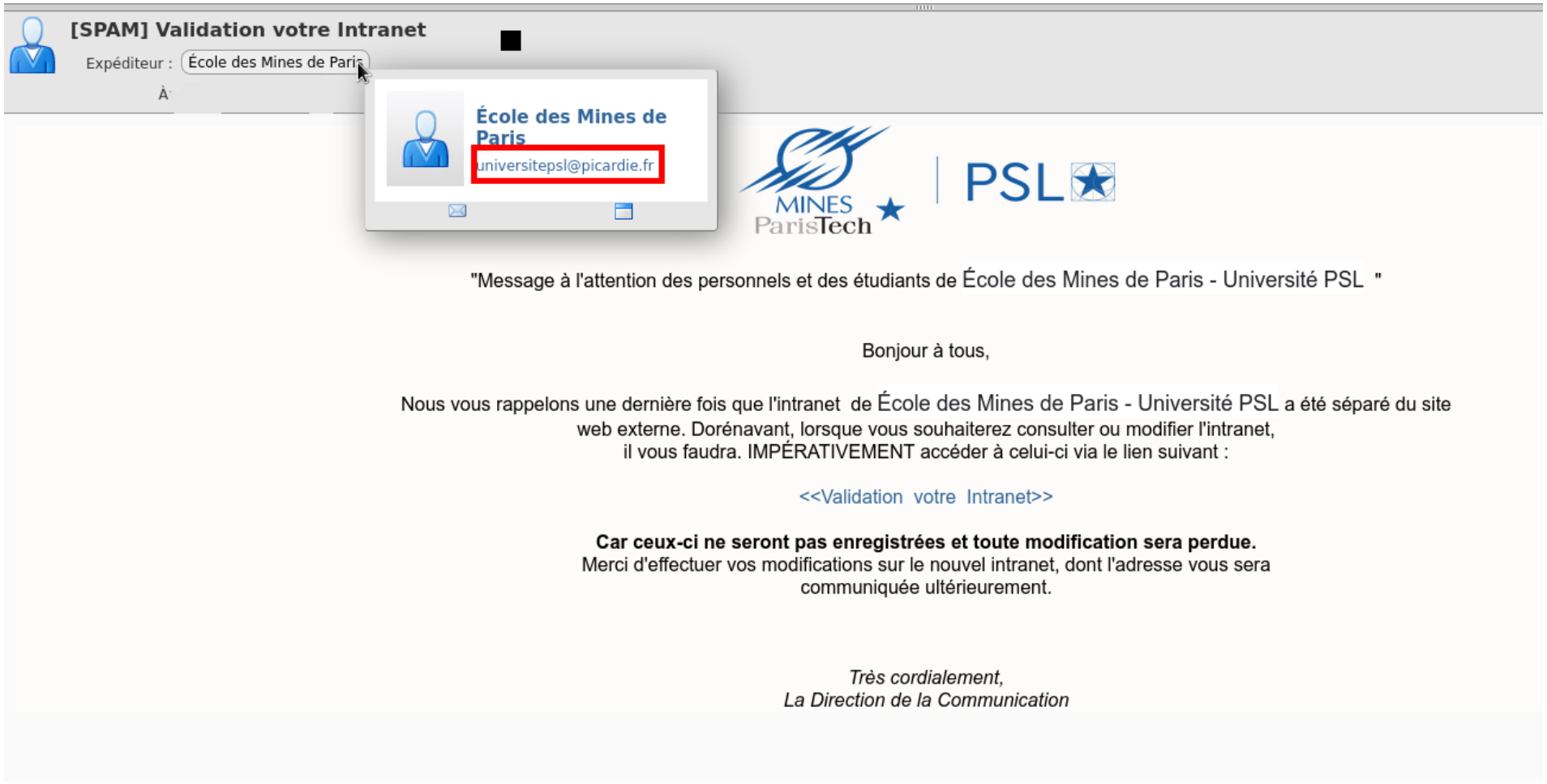
Pour cela, Cliquez sur: **AUTHENTIFICATION** pour effectuer la mise à jour. Nous nous excusons pour le désagrément.

La Direction.

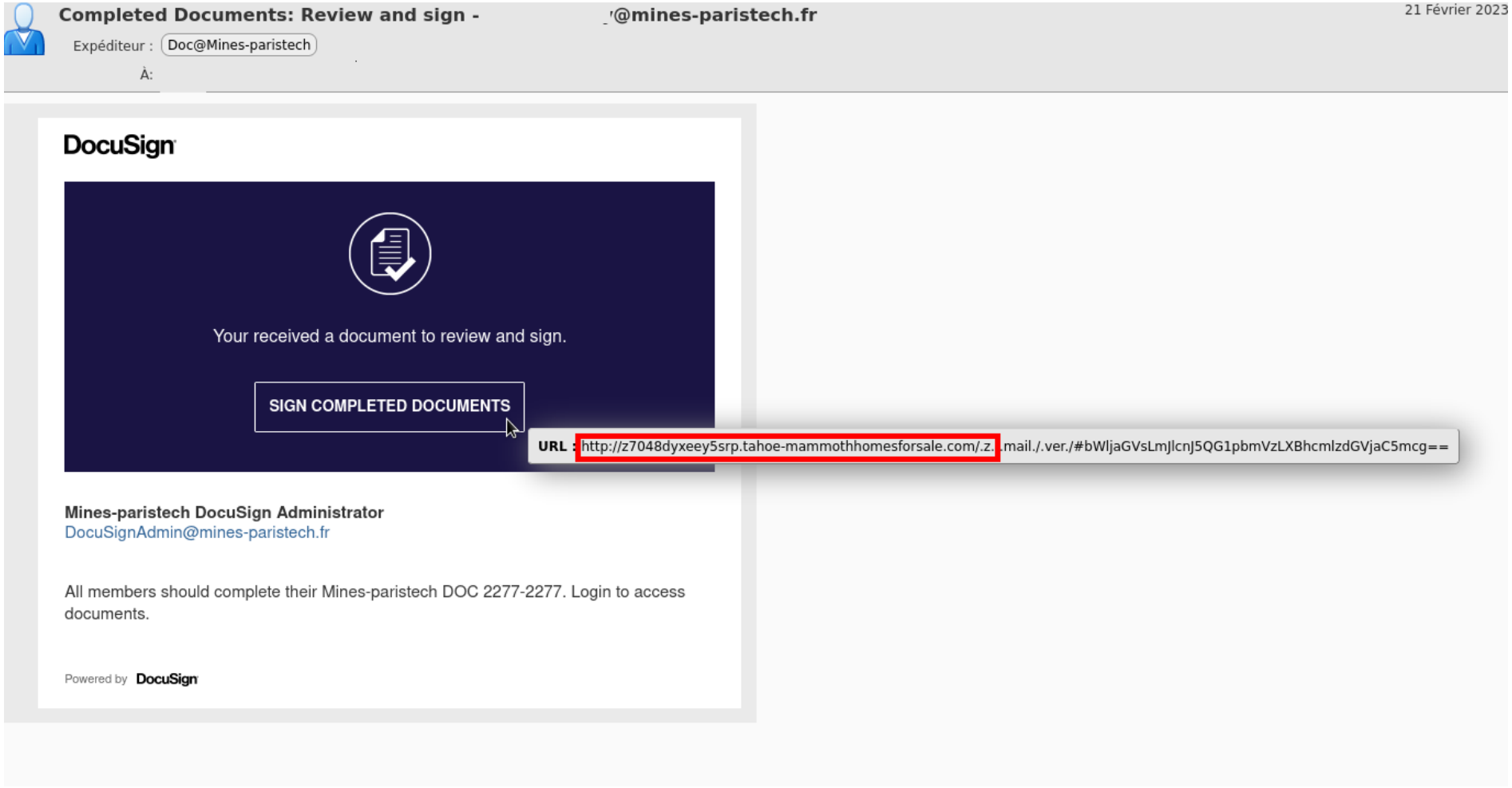
RECONNAITRE UN MESSAGE D'HAMMECONNAGE



RECONNAITRE UN MESSAGE D'HAMMECONNAGE



RECONNAITRE UN MESSAGE D'HAMMECONNAGE

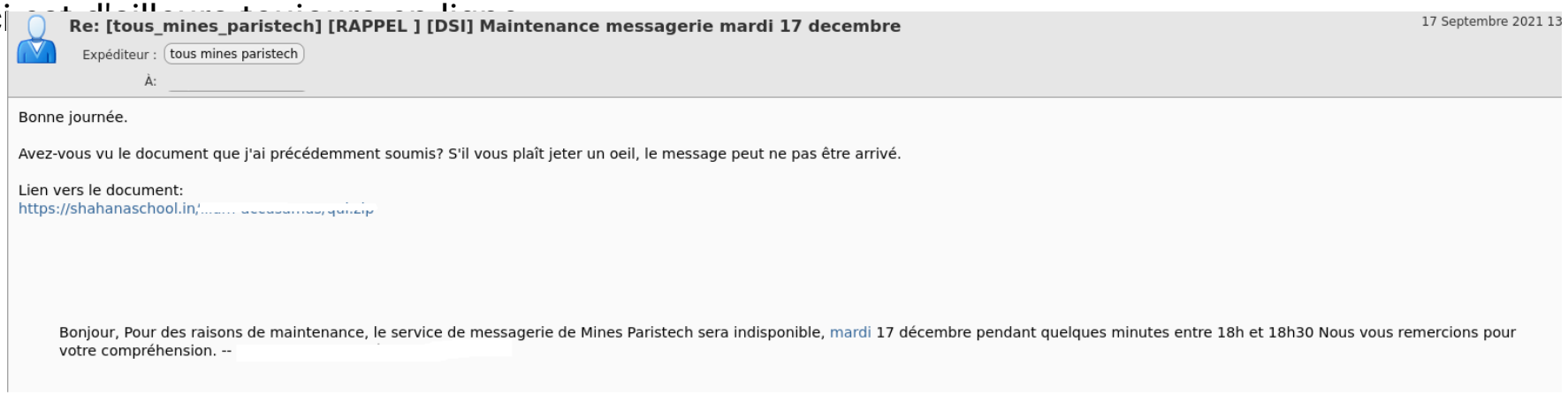


LE PHISHING, C'EST AUSSI LES PIÉCES JOINTES MALVEILLANTES

Des pièces jointes (fichiers pdf, zip , docx . Xls …) peuvent contenir des virus ou des malwares comme les "infostealers" programme malveillant qui récupèrent vos identifiants, les informations bancaires. Les infostealers sont tres mal voir pas du tout détectés par les antivirus.

Certains virus comme "Emotet" utilisent des messages existants depuis un ordinateur ou boite mail compromise pour se renvoyer à tous les contacts d'une boite mails piratée, afin de mieux tromper leur victime.

Voici un exemple d'un message de maintenance de la DSI renvoyé avec un lien pointant sur fichier .zip contenant un malware, celui-ci



COMMENT RÉAGIR ?

En cas de doute sur l'authenticité du site ou suite à la saisie de vos identifiants

1°/ Changez immédiatement votre mot de passe.

-> rappel des bonnes pratiques : 1 service = 1 mot de passe diffèrent

2°/ informer très rapidement le support de la DSI de votre site en mettant en copie rssi@minesparis.psl.eu

NE PAS se sentir coupable ou honteux -> cela arrive à tout le monde, même aux personnes les plus vigilantes
Il faut mieux agir et se signaler.

Dans le cadre personnel :

3 - Signalez l'incident sur PHAROS www.internet-signalement.gouv.fr)

4 - Portez plainte auprès des services compétents (https://www.ssi.gouv.fr/en-cas-dincident)

COMMENT SE PROTÉGER ?

Ne cliquez jamais sur un lien ou une pièce-jointe contenu dans un message qui vous semblent douteux.

Ne répondez jamais à un courriel suspect.

Au moindre doute, si vous connaissez l'expéditeur, contactez-le par un autre canal (téléphone, tchat , …)

Contacter le support de la DSI en envoyant le message d'origine au format "original" fichier en pièces jointes au format ".eml" et non pas juste en utilisant la fonction faire suivre.

Évitez l’effet boule de neige ! Disposez d’un mot de passe diffèrent pour chaque application ou service en ligne.

QUESTIONS

REFERENCES & LIENS UTILES

Recommandations CNIL

https://www.cnil.fr/fr/spam-phishing-arnaques-signaler-pour-agir

Guide de prévention des arnaques

https://www.economie.gouv.fr/files/2021-03/guide-des-arnaques-task-force.pdf?v=1691397258

Plateforme PHAROS

https://www.internet-signalement.gouv.fr/

Signal SPAM

https://www.signal-spams.fr

Ajoutez des filigranes sur vos documents avant transmission afin de prévenir les risques d'usurpation d'identité ou détournement d'usage https://filigrane.beta.gouv.fr/

Pages sécurité informatique site web de la DSI
https://www.dsi.minesparis.psl.eu/securite-phishing/