Le mot de passe est …

Parmi les enseignements que l'on peut retenir de cette attaque et de tout ce qui a été dit à son sujet et sans vouloir m'étendre sur la nécessaire approche globale de la sécurité où il y aurait beaucoup à dire, je me contenterai dans un premier temps de rappeler quelques règles sur les mots de passe :

· un mot de passe doit rester secret et ne jamais être affiché,

· un mot de passe doit être complexe et difficile à deviner,

· il ne faut pas utiliser le même mot de passe pour des services différents,

· l'utilisation d'un gestionnaire de mots de passe comme KeePass est très vivement conseillé.

L'ANSSI a publié des recommandationshttp://www.ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf sur les mots de passe.

FAUX COURRIELS - HAMECONNAGE

Quelques exemples de faux courriers en circulation dans l'Ecole.
Cf: définition de hameçonnage

Quelques règles de base:

- Ne jamais communiquer ses identifiants (mot de passe, code de carte bleue, …) dans un email
- Vérifier toujours l'adresse du lien sur lequel on vous demande de cliquer (tous les messages "ECOLE" doivent vous renvoyer sur un lien commençant par https://www.emse.fr, https://intranet.emse.fr, https://cas.emse.fr ou https://vpnssl.emse.fr)
- Vérifier si le message reçu n'est pas un "canular" déjà répertorié sur le site HoaxBuster

Hameçonnage du 27.05.2014

Courriel frauduleux reçu ce jour

Vous noterez:

- les liens pour le moins "farfelus" sur lequels on vous demande de vous rendre qui ne finissent par **emse.fr** ou **mines-stetienne.fr**.
- les adresses utilisées pour l'emetteur
- la qualité du "français dans le texte"…

```
Expediteur: asosaceh@sct.gob.mx
Sujet: DGTFX de virus webmail

En ce moment, nous mettons à jour notre webmail à augmenter
notre limite de stockage et d'éviter notre DGTFX de virus
webmail passe. S'il vous plaît ne pas répondre à tous les
courriels demandant votre mot de passe et d'autres informations.
Pour mettre à jour bon clic lien ci-dessous et remplissez les
informations nécessaires.

http://account-web-fradmin.dudaone.com/

Webmail équipe


_____
Sent via the WebMail system at webmail.sct.gob.mx
```

Hameçonnage du 02.08.2013

Encore un courriel frauduleux à destination des élèves et du personnel:

```
Sujet: Votre quota de webmail a dépassé

Votre quota de webmail a dépassé le quota fixé qui est de 2 Go. vous êtes
en cours d'exécution sur 2.3GB.To réactiver et d'augmenter votre quota de
webmail
s'il vous plaît vérifier et mettre à jour votre compte webmail
Afin de réactiver et d'augmenter votre quota de webmail, cliquez sur le lien
ci-dessous.

http://fd10.formdesk.com/unk/uzu/

Ne pas le faire peut entraîner l'annulation de votre compte webmail.
Merci, et désolé pour le désagrément
Administrateur / Webmaster / hôte local
```

Vous noterez:

- le lien pour le moins “farfelu” sur lequel on vous demande de vous rendre
- la qualité du “français dans le texte”…

Attention, une personne s'est faite piéger en se rendant sur ce site. Son compte a été immédiatement utilisé pour ré-envoyer massivement ce même courriel en se présentant comme “webmaster@emse.fr”. Je vous laisse imaginer les conséquences pour l'image de l'école. Nous avons immédiatement procédé au blocage du compte compromis…

Hameçonnage du 13.06.2013

Depuis jeudi 13 juin 2013, le courriel suivant est parvenu en masse aux personnels et élèves de l'école:

```
From: Gitau John Ng'ang'a <John.Gitau@kemu.ac.ke>
Sujet: Compte_Avertissement-0987

En raison de la récente menace pour tous les utilisateurs de messagerie,
Microsoft se déplace vers la nouvelle version de Microsoft Internet Explorer
9 2013/Internet accès pour plus de raisons de sécurité. Service de soutien
administratif Microsoft nécessite que vous re-valider les informations de
votre webmail en cliquant ci-dessous.

Cliquez ici

Ce message est de Helpdesk. Grâce aux dernières mises à jour de sécurité IP,
nous avons nos raisons de croire que votre
compte webmail a été consulté par un tiers. Protéger la sécurité de votre
compte webmail est notre principale
inquiétude, vous avez un accès limité aux fonctions du compte webmail. Le
non sensible pour revalider, votre e-mail ne sera
être bloqués dans les 24 heures.

Merci pour votre coopération.
Help Desk
(@) 2013. L'équipe de support technique de Microsoft

--
This message has been scanned for viruses and
dangerous content by MailScanner, and is
believed to be clean.
```

Ce mail est une tentative d'hameçonnage et il ne faut pas y répondre...

On peut en effet noter:

- L'adresse du lien proposé “cliquez ici” n'est pas un site Microsoft
- nous ne vous demanderons jamais de communiquer vos identifiants par mail. Pour cela nous tenons une application unique à votre disposition :

https://intranet.emse.fr/mdp (vous noterez l'adresse officielle en emse.fr qui est la seule valable...)

Hameçonnage du 06.02.2012

```
Votre boîte aux lettres a dépassé la limite de 2 Go fixé par notre
webmaster,
```

```
vous êtes runing à 2.30GB vous ne pouvez pas envoyer ou recevoir de nouveaux
messages jusqu'à ce que vous confirmiez votre boîte de réception.
Remplissez le formulaire ci-dessous pour valider votre compte.

Remplissez les informations demandées et envoyer des e-mail à ce qui suit:

(1) E-mail:
(2) Nom d'utilisateur:
(3) Mot de passe:
(4) Confirmer mot de passe:

merci
administrateur du système.
```

Ce mail est évidemment une tentative d'hameçonnage et il ne faut pas y répondre...

On peut en effet noter:

- l'adresse “fantasque” de l'émetteur pour une telle demande
- le vocabulaire employé: *“...vous êtes runing à 2.30GB...”*

Nous ne vous demanderons jamais de communiquer vos identifiants par mail.
Pour cela nous tenons des applications à votre disposition :

- Changement du mot de passe depuis l'école
- Remise à zéro du mot de passe en cas de perte (voir la fiche associée)

*vous noterez l'adresse officielle en **emse.fr** de nos applications qui est la seule valable...*

Hameçonnage du 17.09.2012

Depuis lundi 17 septembre 2012, un grand nombre d'entre nous a reçu le courriel suivant:

```
De: École Nationale Supérieure des Mines de Saint-Étienne <webmail@emse.fr>
Sujet: Confirmer e-mail mise à jour
Ce message a été envoyé automatiquement par un programme qui Webmail
vérifie périodiquement la taille des boîtes aux lettres, où de nouveaux
messages sont
reçue. Le programme est exécuté chaque semaine pour s'assurer boîte de
réception ne se
développe trop grand. Si votre boîte de réception devient trop grand, il
vous sera
impossible d' recevoir e-mail. Juste avant que ce message a été envoyé,
comptait 18
Mégaoctets (Mo) ou plus de messages stockés dans votre boîte de réception
sur votre
Webmail Pour nous aider à re-configurer votre espace sur notre base de
données avant
```

```
maintenir votre boîte de réception, vous devez répondre à cet e-mail et
entrez votre:

Nom d'utilisateur {..........}

et mot de passe {..........}

Vous continuez à recevoir ce message d'avertissement périodiquement, Si la
taille de
votre boîte de réception augmente de 20 Mo, un programme sur Bates Webmail
déplacera votre ancien e-mail à un dossier dans votre répertoire d'accueil
pour
veiller à ce que vous allez continuer à être en mesure de recevoir par
courrier
électronique à venir. Vous serez avisé par courriel que cela a eu lieu. Si
votre
boîte de réception augmente de 25 Mo, vous ne pourrez pas recevoir de
courriels de nouveau
il sera retourné à l'expéditeur. Après avoir lu un message, il est
mieux pour répondre et enregistrer une copie.

Nous vous remercions de votre collaboration
École Nationale Supérieure des Mines de St-Étienne


-- Este mensaje ha sido analizado por MailScanner en busca de virus y otros
contenidos
peligrosos, y se considera que está limpio.
For all your IT requirements visit: http://www.transtec.co.uk
```

Ce mail est évidemment une tentative d'hameçonnage et il ne faut pas y répondre...

On peut en effet noter:

- l'orthographe
- nous ne vous demanderons jamais de communiquer vos identifiants par mail. Pour cela nous tenons une application unique à votre disposition :

https://intranet.emse.fr/mdp (vous noterez l'adresse officielle en emse.fr qui est la seule valable...)

Par contre: la tentative d'escroquerie est plus “perverse” que les autres fois car l'expéditeur se fait passer pour webmail@emse.fr

Hameçonnage du 16.07.2012

Depuis lundi 16 juillet 2012, un grand nombre d'entre nous a reçu le courriel suivant:

```
Dernier avertissement
```

```
Je vous dis que votre compte de messagerie a dépassé son limite de stockage.
Vous ne serez pas en mesure d'envoyer et recevoir des e-mails compte de
messagerie seront supprimées de notre serveur. Pour éviter ce problème, vous
recommandons de mettre à jour votre boîte aux lettres pour plus d'espace.
Cliquez sur le lien ci-dessous pour mettre à jour et compléter l'information
du cliquez sur Envoyer

http://tiny.cc/69ykhw

Si nous n'avons pas reçu une mise à jour de votre part, nous allons détruire
votre boîte aux lettres

Merci.
WEBMAIL d'administration système


--------------------------------------------------------------------------
"O usuario e integralmente responsavel por todo conteudo enviado de sua
conta de e-mail. Sua senha e pessoal e intransferivel."
```

Ce mail est évidemment une tentative d'hameçonnage et il ne faut pas y répondre...

On peut en effet noter:

- l'adresse de l'émetteur en provenance du Brésil (nous n'avons pas encore délocalisée la DSI...)
- le site sur lequel on vous demande de vous rendre, tiny.cc, qui n'est pas un site emse.fr (règle de base)
- nous ne vous demanderons jamais de communiquer vos identifiants par mail. Pour cela nous tenons une application unique à votre disposition :

https://intranet.emse.fr/mdp (vous noterez l'adresse officielle en emse.fr qui est la seule valable...)

Hameçonnage du 27.04.2012

Depuis ce matin, nous recevons massivement des courriels de ce type:

```
Votre quota de webmail a dépassé le quota, ce qui est de 2 Go. actuellement
à 2,3 Go.
Afin de relancer et d'accroître leur part de webmail s'il vous plaît cliquer
sur le lien
suivant ou copiez le lien et mettez à jour votre compte de messagerie Web
Afin de réactiver.

https://docs.google.com/spreadsheet/viewform?formkey=dDFsYzdIS3J2WFVtVDA2M3A
0WURkekE6MQ

Si non, peut entraîner l'annulation de votre compte de webmail.
```

```
Merci et désolé pour le désagrément
Admin / Webmaster / localhost
```

Encore une fois, ce mail qui provient d'ordinateurs infectés par un virus et disséminés sur toute la planète est difficile à stopper.

Néanmoins on peut noter:

- orthographe, syntaxe, conjugaison, ...
- le lien sur lequel on vous demande de cliquer qui n'est pas une adresse de l'Ecole (emse.fr)

Ne prenez surtout pas ce mail en compte et, plus que jamais, rappelez vous que la vigilance est la règle de base avec tous les courriels reçus.

Hameçonnage du 03.12.2011

```
-----
from Help Desk Webmail webmail@emse.fr
reply-to support-webmail@ml.lt
to
date Thu, Dec 1, 2011 at 9:09 PM
subject Confirmer alerte email
signed-by emse.fr

9:09 PM (11 hours ago)

Subject Confirmer alerte email



Ce message a été envoyé automatiquement par un programme sur le Webmail, qui
vérifie périodiquement la taille des boîtes de réception, où les nouveaux
messages sont reçues. Le programme est dirigé par semaine pour assurer la
boîte de réception ne se développe trop grand. Si votre boîte de réception
devient trop grand, vous serez incapable de recevez de nouveaux emails.
Juste avant ce message a été envoyé, vous aviez 18 Mégaoctets (Mo) ou plus
de messages stockés dans votre boîte de réception sur votre Webmail Pour
nous aider à re-configurer votre espace sur notre base de données avant
maintenir votre INBOX, vous devez répondre à cet e-mail et entrez votre:

Nom d utilisateur: {...........}

et Mot de passe: {.............}

Vous continuerez à recevoir ce message d avertissement périodiquement,
Si la taille de votre boîte de réception augmente de 20 Mo, alors un
programme sur Bates Webmail va déplacer votre ancienne e-mail à un dossier
dans votre répertoire home assurer que vous continuerez à être capable de
recevoir à venir par courriel. Vous serez averti par email que cela a eu
```

```
lieu. Si votre inbox pousse à 25 Mo, il vous sera impossible de recevoir
des emails nouvelles il sera renvoyé à l expéditeur. Après avoir lu un
message, il est mieux pour répondre et enregistrer une copie.

Nous vous remercions de votre coopération.
Help Desk Webmail
```

A noter

- orthographe, syntaxe, conjugaison, ...
- nous ne vous demanderons jamais de nous communiquer votre mot de passe “en clair” (que ce soit dans un mail ou sur un site)
- Fourberie avancée de l'emetteur qui tente de se faire passer pour webmail@emse.fr

Hameçonnage du 25.10.2011

```
webmail d'alerte d'équipe

La boîte aux lettres est presque pleine.
100Go 100 Go

Votre boîte aux lettres a dépassé la limite de stockage de 100 Go
vous de votre travail, 100 Go, définit
peut ne pas être en mesure d'envoyer ou de recevoir des messages jusqu'à ce
que vous rafraîchir la
Boîte de réception. Pour valider votre boîte de réception, cliquez sur le
lien
ci-dessous et de confirmer
leurs données pour la mise à jour:

http://buzurl.com/bz67

Remplissez les informations dans le lien ci-dessus et cliquez sur Soumettre
Envoyer un fichier

merci
L'administrateur du système de webmail
```

A noter

- orthographe, syntaxe, conjugaison, ...
- Le lien vous renvoyant vers un site inconnu “buzurl.com” plutôt que vers un de nos sites

Hameçonnage du 30.09.2011

```
vous avez dépassé la limite de stockage sur votre boîte aux lettres.

Vous ne serez pas en mesure d'envoyer ou de recevoir de nouveaux messages
jusqu'à ce que vous mettez à niveau votre
e-mail de quotas.

Copiez le lien ci-dessous et remplissez le formulaire pour mettre à niveau
votre compte.

http://www.weinfassrollen.ch/phpForms/use/samform/form1.html

Administrateur système
192.168.0.1
```

A noter

- orthographe, syntaxe, conjugaison, ...
- Le lien vous renvoyant vers un site inconnu www.weinfassrollen.ch plutôt que vers un de nos sites

Hameçonnage du 27.09.2011

```
Votre boîte aux lettres a dépassé, il quota / limite fixé par votre
administrateur et que vous ne pourrez pas recevoir ou envoyer de nouveaux
mails jusqu'ŕ ce que vous re-valider.
Pour re-valider CLIQUEZ ICI
https://docs.google.com/spreadsheet/viewform?formkey=dDI2VVRvSDVNMVQwQVZpNnB
wZncxNlE6MQ
Je vous remercie.
Directeur des Services d'information
```

A noter

- Les fautes d'orthographe inhabituelles
- Le lien vous renvoyant vers docs.google.com plutôt que vers un de nos sites