Sécurité des SI | Kit de sensibilisation

Le Phishing / Hameçonnage

Le 17 janvier 2020

QUESACO ?

- **Le Phishing (ou Hameçonnage) est une technique d'escroquerie** sur Internet consistant à vous piéger en usurpant l'identité d'un tiers de confiance (collègue, famille, ami, banque, opérateur, réseaux sociaux…)
- La méthode repose le plus souvent sur la **contrefaçon de sites internet, d'e-mails voire de sms**
- Le but est de **voler des données** personnelles ou professionnelles (identifiant, mot de passe, numéro de compte bancaire…) pour en faire un usage frauduleux. Ce peut être aussi le moyen de **pirater vos équipements** en y installant des logiciels malveillants

TENDANCE

- **Forte progression** (+65% 2017; +28% 2018)
- Sur **100** personnes, 3**0** vont suivre le lien frauduleux, **10** vont fournir leurs identifiants
- ~1 500 000 nouveaux sites de phishing par mois
- Porte d'entrée de la **moitié des virus** en entreprise
- Responsable d'**un tier des vols de données** d'entreprise

- De plus en plus **sophistiqué** (Ex: Empoisonnement du moteur de recherche Google)
- De plus en plus **ciblé: spearphishing** (Collecte d'informations préalable sur les réseaux sociaux)
- De plus en plus **stratégique** (Espionnage industriel, sabotage)

COMMENT LES DETECTER?

Vous avez appris à vos enfants à ne pas accepter de friandise de la part d'inconnus, c'est un peu la même chose avec les e-mails!

- **Connotation alarmiste** (« Votre compte va expirer », « Vous venez d'effectuer un achat », « Votre patron veut partager ces documents avec vous », etc.) ou alléguant un prétendu remboursement. L'objectif est d'inhiber toute réflexion.
- **Invitation à se rendre sur une page** de formulaire sur laquelle sont demandées des informations de connexion ou bancaire. Le but est clairement de voler vos identifiants.
- **Généralement accompagné d'une pièce jointe**, souvent présentée comme une facture ou tout autre document attractif (ex: Photo, liste des salaires, carte d'anniversaire). Ce fichier est un virus ou un programme intermédiaire qui téléchargera sournoisement, après-coup, un virus afin de leurrer votre anti-virus.

COMMENT LES DETECTER? …Suite

« Urgent: Veuillez nourrir votre mot de passe pour accéder à Figeak-äero »

- Le message est rempli de **fautes d'orthographe** ou tournures de phrase erronées
- Penser à vérifier la vraisemblance des adresses en **survolant les liens avec le pointeur** de votre souris
- Le message est très générique « Cher Client », « Madame, Monsieur » (de - en - vrai)
- **Souvenez-vous qu'aucun organisme ne vous demandera d'informations confidentielles à distance**
- Pour confirmer l'origine, n'hésitez pas à **contacter votre interlocuteur par un autre moyen**: téléphone, physique, courrier…
- Si le doute persiste, **demander conseil à votre support informatique**

DANS LA PRATIQUE

- Réception d'un e-mail non sollicité en provenance soi-disant de l'équipe Microsoft
- *Oulala* notre compte va être bloqué si nous ne nous connectons pas!
- En fait, nous nous apercevons rapidement que l'émetteur « cyh11241 » provient du domaine « @lausd.net » et non « @microsoft.com », c'est du phishing!

From: Microsoft office365 Team [mailto:cyh11241@lausd.net]
Sent: Monday, September 25, 2017 1:39 PM
To:
Subject: Your Mailbox Will Shutdown Verify Your Account

PHISHING!

L'adresse de messagerie devrait se terminer par @microsoft.com

Office 365

Detected spam messages from your <EMAIL APPEARED HERE> account will be blocked.

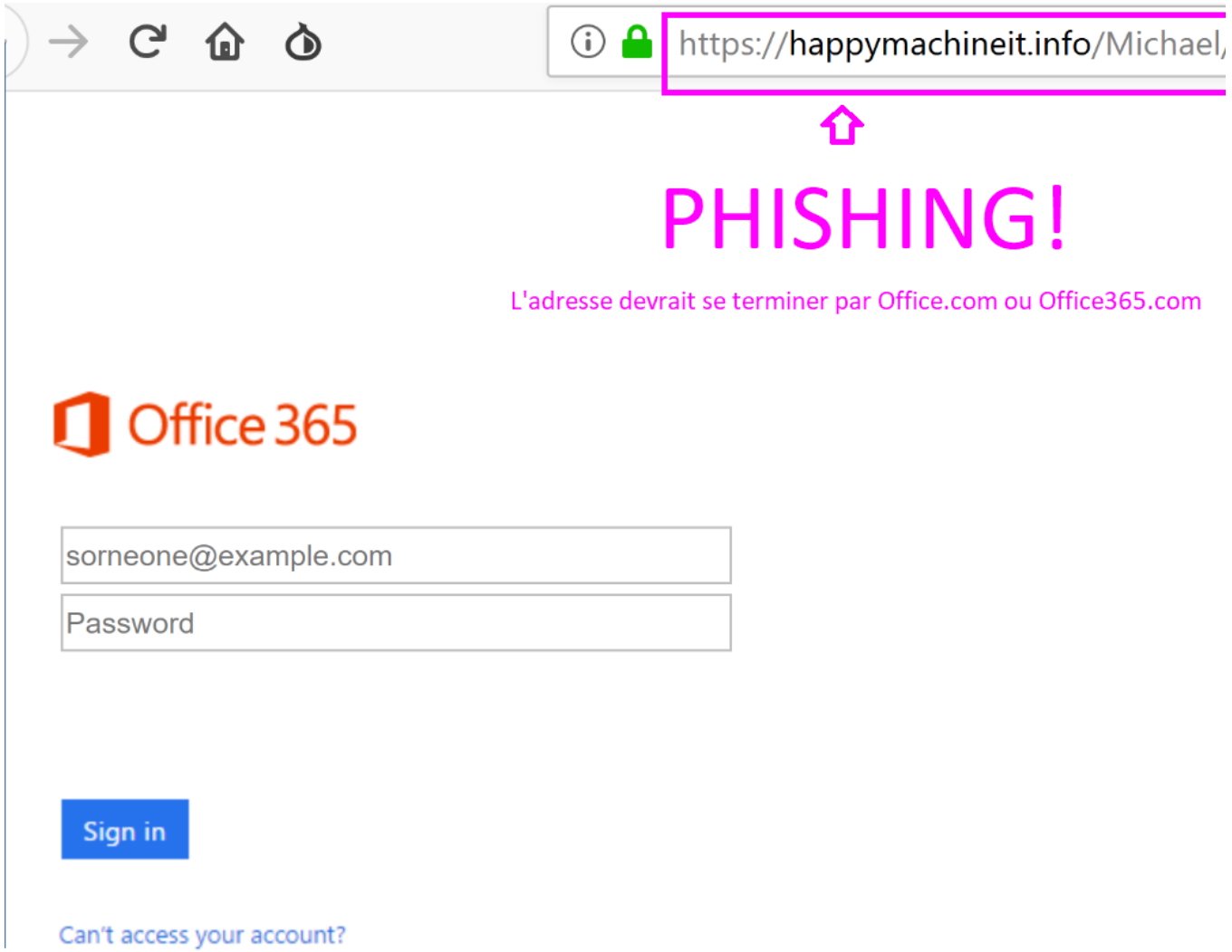
If you do not verify your mailbox, we will be force to block your account. If you want to continue using your email account please verify.

Verify Now

Microsoft Security Assistant
Microsoft office365 Team! ©2017 All Rights Reserved

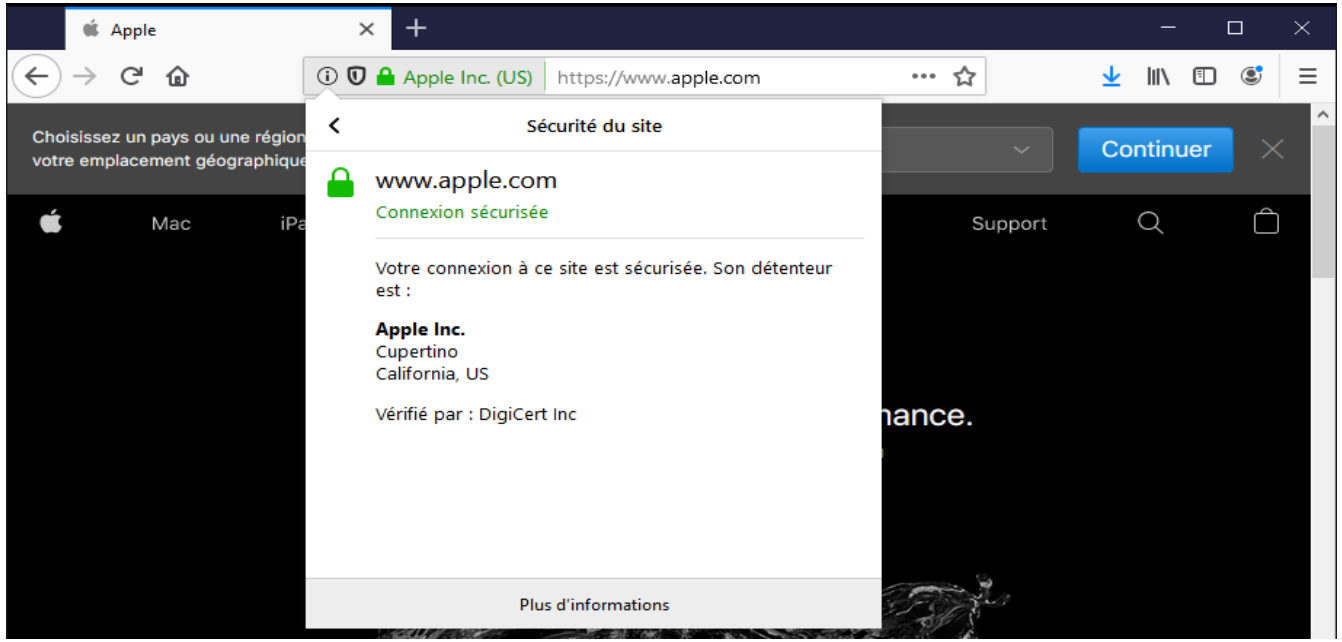
DANS LA PRATIQUE

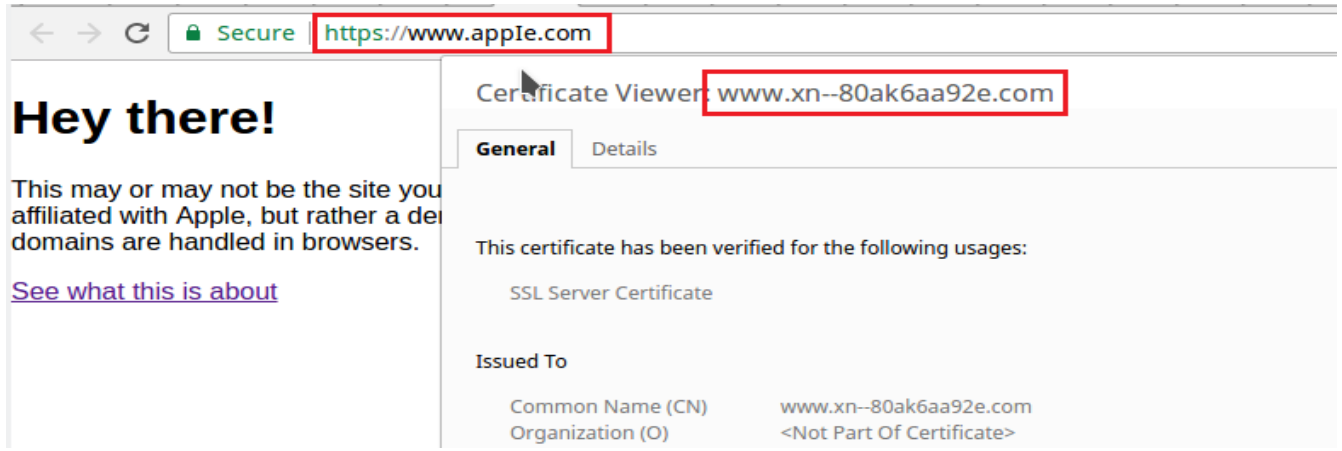
- Si l'on suit le lien malgré tout, nous sommes invités à renseigner nos identifiants de connexions office 365
- Là encore, l'adresse du site web ne fait pas partie du domaine « office.com » mais « happymachineit.info » , c'est du phishing!
- Il s'agit d'une contrefaçon visant à voler votre mot de passe



DANS LA PRATIQUE

- Certains sites d'hameçonnage utilisent des attaques par imitation (homographie)
- Pouvez-vous remarquer la différence entre les 2 adresses des sites ci-joint?
- « apple.com » avec un L et « apple.com » avec un i majuscule
- Cliquer sur le cadenas pour vérifier l'incohérence du certificat de sécurité et confirmer le phishing





Merci!