LES DANGERS

Les arnaques

Des personnes malveillantes peuvent abuser de votre confiance pour vous voler des informations confidentielles, vous extorquer de l'argent, vous communiquer des informations inexactes.

La plupart de ces démarches malhonnêtes se font en utilisant le mail (courrier électronique).

Le "Phishing" (hameçonnage)

Le but est de s'emparer des données personnelles d'un internaute en lui faisant croire qu'un organisme, sa banque par exemple, a besoin de ces données. Il est attiré, par un mail, vers un faux site (bancaire, de commerce électronique, etc.). On va lui demander d'effectuer une opération sur son compte en ligne, par exemple, confirmer un mot de passe, ou faire une mise à jour de ses données personnelles... L'escroc a désormais tout loisir d'accéder à ses comptes puisqu'il dispose de toutes les informations confidentielles nécessaires.

Comment se protéger contre le phishing ?

- Utilisez les fonctions antiphishing de votre navigateur
  Les nouvelles versions des navigateurs (> Internet Explorer 7) proposent désormais des mécanismes capables de détecter les "faux sites".
- Effacez le mail et ne pas en tenir compte. En effet, toutes les banques sérieuses ont déclaré qu'elles ne demanderaient jamais les données confidentielles d'un client par courrier électronique. Si le consommateur doute, il peut toujours contacter directement son banquier.

Les spams

C'est un email souvent publicitaire envoyé à des milliers de personnes. Les victimes peuvent avoir leur boîte aux lettres pleine en quelques semaines.

Ces spam se classent en 4 catégories :

- les offres financières (prêts à taux réduits, cartes de crédit, arnaques liées aux lettres africaines, etc.),
- les produits de santé/physiologiques (soins par les plantes, viagra, régimes, produits minceur...),
- messages à caractère érotique ou pornographique
- une catégorie électronique (téléphones mobiles, cartouches d'encre, imprimantes, appareils photo, etc.),

© PMTIC - LabSET – ULg 2014

Tout cela bien sûr, proposé sous forme d'offres promotionnelles alléchantes.

Comment se protéger contre les spams ?

- Ne transmettez pas votre adresse électronique sur un espace public d'Internet (lors d'une visite d'un site, lors d'un forum, d'un chat, etc.).
- Si vous devez communiquer, remplacez ce symbole @ par la mention "at" votre correspondant pourra utiliser l'adresse en la réencodant manuellement. Vous éviterez ainsi que votre adresse électronique ne soit collectée par des chaînes de recherche qui détectent les adresses comprenant le symbole @.
- Ne répondez pas aux spams !
- Vous ne feriez que confirmer l'existence et l'exactitude de votre adresse. De plus, personne ne lira votre réponse, ces e-mails sont envoyés par des robots.
- Ne cliquez pas sur « **Se désinscrire** », sauf s'il s'agit d'un site que vous connaissez et auquel vous vous souvenez vous être inscrit(e). En effet, avec cette méthode, les pirates vérifient que l'adresse de messagerie est toujours valide et régulièrement consultée.
- Activez le service antispams de votre messagerie.

La plupart des messageries proposent un service en option qui arrête le spam avant que vous ne le receviez. Dans certains cas, il est nécessaire de l'activer.

Les scams

C'est un e-mail que vous n'avez jamais demandé à recevoir et qui vous propose en général un gain d'argent facile et rapide (loterie, bourse, etc) ou qui sollicite votre générosité.

Comment se protéger contre les scams ?

Supprimez immédiatement le courrier sans l'ouvrir.

Pour cela : cliquez avec le bouton droit de la souris sur le nom du courrier, faites glisser votre souris jusqu'à la commande « **Courrier indésirable** » et cliquez sur « **Ajouter l'expéditeur à la liste des expéditeurs bloqués** ».

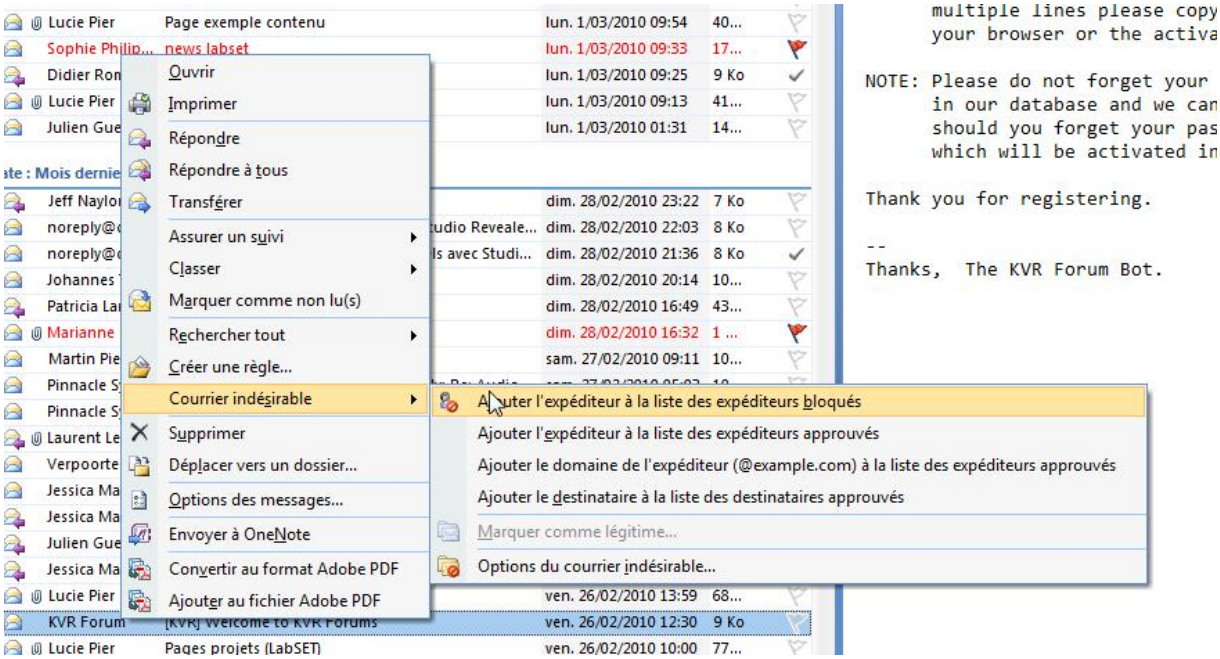
Exemples de scam

A votre Attention,

Très cher(e) Monsieur ou Madame,

Nous vous contactons par cette présente pour vous informer de votre gain a MICROSOT, à organisé une Tombola concernant toutes personnes ayant une boite électronique.
A l'issue de cette tombola, vous avez été tiré donc L'heureux(s) bénéficiaire de la somme de 250.000 €,le tirage a été fait après une campagne de mailing et d'un tri à l'aide du puissant logiciel mail fox (TOPAZ) d'une base de données de plus de 30.000.000 adresses Email tirées de tous les continents.
VEUILLEZ PRENDRE CONTACT AVEC L'AVOCAT ACCRÉDITE CI DESSOUS POUR LA PROCÉDURE DE RETRAIT DE VOTRE GAIN, afin qu'il vous fasse parvenir la procédure à suivre en vue de vous mettre en règle concernant les formalités d'usages.

« Bonjour,
Je me nomme Kevin KOUMIA. Je rentre en contact avec vous pour solliciter une assistance de grande importance. Ma soeur et moi avons decouvert que nous venons d'heriter indirectement de la somme de 10 000 000 de dollars Americains qui ont ete deposés dans une compagnie de securité par notre défunt père, cet argent beneficierai à son partenaire étranger, et nous aimerions le transférer dans un pays étranger ou nous pourrions nous exiler parce que nous avons perdue nos parents dans le conflis de BOUAKE (Côte D'ivoire). »



Source des images :
http://www.amitbhawani.com/blog/email-phishing-scams-prevention/
http://brandedsolutions.wordpress.com/

Les canulars (hoax)

Qu'est-ce qu'un hoax ?

On appelle hoax (en français canular) un courrier électronique propageant une fausse information et poussant le destinataire à diffuser la fausse nouvelle à tous ses proches ou collègues.

Ainsi, de plus en plus de personnes font suivre (anglicisé en forwardent) des informations reçues par courriel sans vérifier la véracité des propos qui y sont contenus.

Les conséquences de ces canulars sont multiples :

- L'engorgement des réseaux en provoquant une masse de données superflues circulant dans les infrastructures réseaux ;
- Une désinformation, c'est-à-dire faire admettre à de nombreuses personnes de faux concepts ou véhiculer de fausses rumeurs (on parle de légendes urbaines) ;
- L'encombrement des boîtes aux lettres électroniques déjà chargées ;
- La perte de temps, tant pour ceux qui lisent l'information, que pour ceux qui la relayent ;
- La dégradation de l'image d'une personne ou bien d'une entreprise ;
- L'incrédulité : à force de recevoir de fausses alertes, les usagers du réseau risquent de ne plus croire aux vraies.

Ainsi, il est essentiel de suivre certains principes avant de faire circuler une information sur Internet.

Comment lutter contre la désinformation ?

Afin de lutter efficacement contre la propagation de fausses informations par courrier électronique, il suffit de retenir une seule idée :

Toute information reçue par courriel non accompagnée d'un lien hypertexte vers un site précisant sa véracité doit être considérée comme non valable !
Ainsi, tout courrier contenant une information non accompagnée d'un pointeur vers un site d'information ne doit pas être transmis d'autres personnes.
Lorsque vous transmettez une information à des destinataires, cherchez un site prouvant votre propos.

Comment vérifier s'il s'agit d'un canular ?

Lorsque vous recevez un courriel insistant sur le fait qu'il est essentiel de propager l'information (et ne contenant pas de lien prouvant son intégrité), vous pouvez vérifier sur le site hoaxbuster (site en français) s'il s'agit effectivement d'un hoax.

Si l'information que vous avez reçue ne s'y trouve pas, recherchez l'information sur les principaux sites d'actualités ou bien par l'intermédiaire d'un moteur de recherche.

© PMTIC - LabSET – ULg 2014

Un exemple d'hoax :

Objet : Message d'alerte virus et de bonne année

Merci de transmettre ce message à tout votre carnet d'adresse
Et bonne année malgré tout!
Cordialement
Alain

Objet: ALERTE VIRUS PORTABLE & INTERNET

>
>Message d'Alcatel - il est important de le lire, car la source est sérieuse et le danger maximal.
>
> Objet: Alerte Pirate
> > Diffusion message d'alerte à rediffuser a tous ceux que vous connaissez et qui ne figureraient pas dans les destinataires.
> >
1. Il s'agit d'1 information provenant du Ministère de l'Interieur à l'attention de tous les détenteurs de téléphone portables : UN CORRESPONDANT LAISSE 1 MESSAGE AFIN QU'ON LE RAPPELLE AU 01 41 46 51 14.
> >
N'appelez surtout pas ce numéro ou vos factures augmenteront sans commune mesure. Cette information communiquée par l'Office Centrale de Répression du Banditisme est a diffuser le + largement possible.
> >
Depuis quelques temps, des escrocs ont trouvé 1 système pour utiliser frauduleusement vos portables. Ils vous appellent sur votre GSM, et se présentent comme le "PROVIDER" ITINERIS, SFR, BOUYGUES, auquel vous êtes abonnes. Ils demandent ensuite de composer 1 code qui est le 09 # en vous expliquant qu'il s'agit de vérifier le bon fonctionnement de votre portable.
> >
NE COMPOSEZ SURTOUT PAS CE CODE ET RACCROCHEZ IMMEDIATEMENT. Ils disposent de l'outillage permettant grâce a ce code de lire votre carte SIM. Il ne leur reste alors plus qu'a créer 1 nouvelle carte. Cette fraude se pratique a grande échelle, il est donc nécessaire de faire suivre cette information très rapidement au plus grand nombre de personnes de votre entourage, particuliers, entreprises etc ...

Source : http://www.commentcamarche.net/contents/1225-les-canulars-hoax