PHISHING : QUELQUES CONSEILS POUR NE PAS SE FAIRE PIEGER

5

Université de Lille

Pourquoi ce guide ?

À destination des personnels et étudiants de l'université
Ce guide vise à sensibiliser à la technique du phishing (hameçonnage) . Le but n'est pas de devenir soi-même un bon « pirate », mais d'être capable de détecter les mails frauduleux et de les éliminer plutôt que de suivre aveuglement leurs consignes.

Définition :

Le phishing est une techniques d'ingénierie sociale incitant un utilisateur à fournir « en toute bonne foi » des données sensibles ou d'autres ressources (argent, par exemple) à des personnes mal intentionnées, ou amenant l'utilisateur à installer à son insu des logiciels malveillants sur son poste de travail.
Le média utilisé pour effectuer ce phishing est généralement la messagerie électronique, mais le téléphone, le fax ou l'écrit peuvent également être mis à contribution.

••• Phishing : quelques conseils pour ne pas se faire piéger

Exemples de phishings

Phishing assez facile à détecter :

De : webmaster@universite.fr [mailto:albert.duchmoll@univ-ville.fr]

Envoyé : mardi 16 octobre 2018 08:21

Objet : Alerte

Votre limite de stockage de boîte aux lettres a été dépassé en raison du taux élevé de Spam / ordure de tous les messages entrants sont rejetés.

Pour re-valider votre email. Cliquez sur le lien ci-dessous et envoyer

le formulaire de revalider leur e-mail.

CLIQUEZ ICI: http://upgrade-001-dept-akd12389754.tropid.com

C 2,018 équipe de support technique.

Phishing moins facile à détecter :

Votre espace client

Chère cliente, cher client

Suite au refus de votre banque lors d'un prélèvement de facture , Votre paiement a été malheureusement refusé.

A fin de résoudre ce dernier nous avons mis au point en accord avec votre banque une nouvelle tentative avec des vérifications plus approfondis. Veillez cher client suivre la procédure ci-dessous , toutes nos excuses pour ce désagrèment.

Résoudre ce problème maintenant

Cordialement

Votre conseiller ENGIE

Retrouvez tous nos services sur votre espace client

Ce mesage vous est adressé automatiquement. Nous vous remercions de ne pas répondre, ni d'utiliser cette adresse email. ATTENTION : Ce message est strictement confidentiel. Son intégrité n'est pas assurée sur internet. Si vous n'êtes pas destinataire du message, merci de le détruire.

ENGIE SA au capital de 832 987 567 €. RCS Paris n° 552 730 285.

••• Phishing : quelques conseils pour ne pas se faire piéger

Précautions à prendre

Les phishings étant de plus en plus sophistiqués (ex : courriel personnalisé, avec une bonne syntaxe et sans fautes d'orthographe), il est nécessaire de prendre un certain nombre de précautions pour éviter d'en être victime. Voici une liste, non exhaustive, de précautions :

- ne jamais croire que l'expéditeur d'un courriel est bien celui dont le nom apparaît dans le courriel (sauf cas particulier de courriel authentifié par un «certificat électronique»),
- en cas de doute sur l'expéditeur, ne pas hésiter à se faire confirmer l'identité de celui-ci, de préférence en demandant une information connue seulement de cette personne, ou en la contactant par une autre moyen (téléphone, SMS, de visu),
- être extrêmement vigilant avant de cliquer sur une adresse WEB proposée dans un courriel : comparer minutieusement le texte affiché et l'adresse sous-jacente en passant la souris sur le lien, et faire attention aux ressemblances (ex : ecarte-bleue.com et ecarte-bieue.com, ex : univ-lille.fr et uni-lille-fr),
- se méfier des contrefaçons de site WEB, qui sont parfois difficiles à distinguer de l'original,
- consulter le site officiel de votre correspondant (s'il s'agit d'une société), celui-ci ayant souvent une page WEB dédiée aux phishings,
- consulter le site web dédié à la sécurité informatique à l'Université de Lille (ssi.univ-lille.fr), rubrique phishings
- de préférence, pour se rendre sur un site WEB habituel, ne pas cliquer sur le lien proposé dans un courriel, mais saisir directement l'adresse dans le navigateur web, ou passer par un favori.
- ne pas ouvrir une pièce-jointe dès qu'il y a un doute sur l'authenticité de l'expéditeur, ou sur le type de pièce-jointe (surtout, ne jamais exécuter des programmes fournis en pièce-jointe !),
- contre les arnaques des «brouteurs», escrocs se servant de la crédulité ou de la sensibilité des personnes pour soutirer de l'argent, faire une recherche internet basée sur les termes utilisés dans le courriel (très efficace),
- ne pas oublier que les escroqueries peuvent être également réalisées par un ou plusieurs moyens combinés (ex: envoi d'un courriel suivi d'un appel téléphonique), et que les escrocs peuvent être très bien renseignés sur vos habitudes de travail et sur l'organisation de votre entité.

Que faire si j'ai été victime d'un phishing ?

- Première règle : le signaler, ça peut arriver à tout le monde
- Parlez-en autour de vous, prévenez vos collègues
- Faite remonter l'information aux informaticiens de votre direction/composante/laboratoire et aux RSSI de l'Établissement
- Enfin, réduisez les possibles conséquences :

· vous avez communiqué votre mot de passe : changez le immédiatement, et partout où vous avez le même

· vous avez communiqué vos informations bancaires de paiement (numéro de CB, date d'expiration, code CCV) : contactez votre banque pour faire opposition

· vous avez communiqué RIB, pièce d'identité, justificatif de domicile : déposez une plainte ou une « main courante » pour vol de données personnelles et risque d'usurpation d'identité au commissariat de police ou à la gendarmerie. Cette action, même si elle n'est pas suivie d'une enquête permettra au moins de dater l'événement.

••• Phishing : quelques conseils pour ne pas se faire piéger

Les guides en ligne :

intranet>environnement de travail>données personnelles et sécurité informatique

Une question relative aux données personnelles ?
Contactez le délégué à la protection des données :
dpo@univ-lille.fr

Une question relative à la sécurité ?
Contactez le délégué à la protection des données et les responsables de la sécurité des systèmes d'information :
ssi@univ-lille.fr

Retrouvez les informations relatives aux données personnelles sur l'intranet :
environnement de travail > données personnelles et sécurité informatique

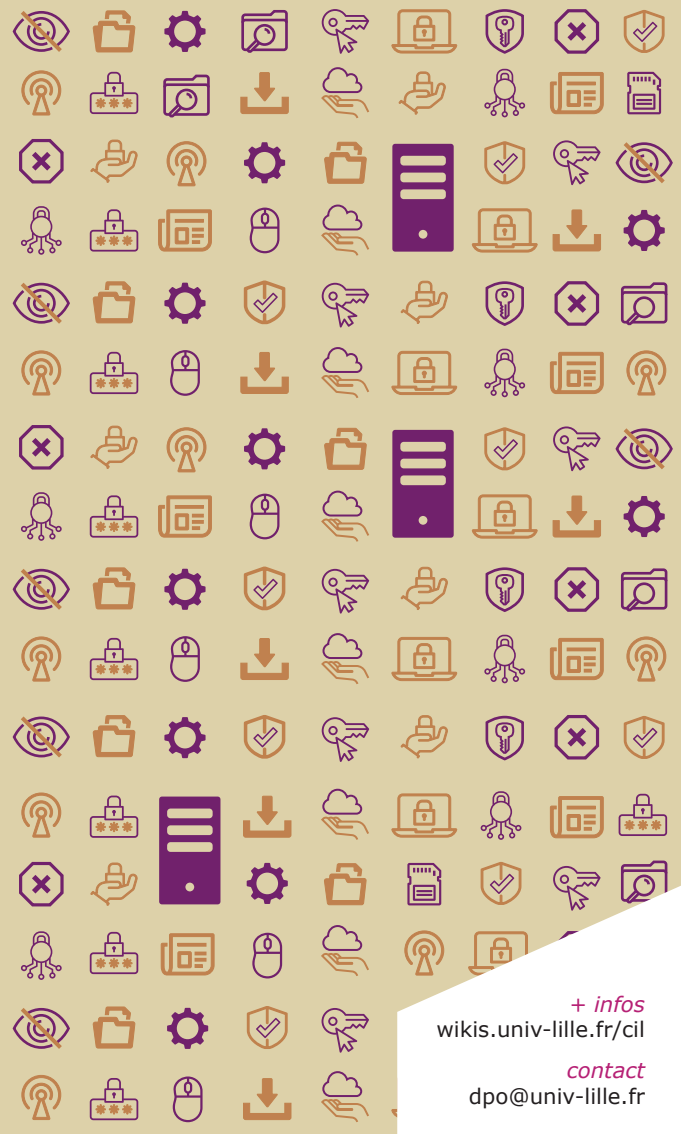
DÉJÀ PARU

- *n°1*
  Loi informatique et liberté : suis-je concerné·e ?
- *n°2*
  Le règlement général sur la protection des données : ce qui change guide
- *n°3*
  Comment chiffrer son disque dur ?
- *n°4*
  Directeur de thèse ou de mémoire

À PARAÎTRE

- *Qu'est ce qu'une recherche impliquant la personne humaine ?*
- *Transférer des données nominatives par messagerie*
- *Contrat de sous-traitance*
- *Faire une enquête anonyme*

©Université de Lille - n°5 - novembre 2018 - Diffusion à 500 exemplaires



+ infos
wikis.univ-lille.fr/cil

contact
dpo@univ-lille.fr