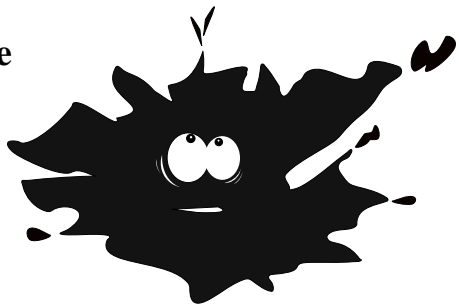
Hors sujet – Communication écrite
29 – Les liens



Durée : 15 à 25 minutes

Cinquième fiche sur le travail de communication écrite, avec de vrai pièges cette fois !
PS : Les taches squattent, faites semblant de ne pas les voir, elles finiront bien par partir ...

11 – Liens, rallonges et pistes piégées

Il nous arrive de partager des ressources intéressantes, présentes sur Internet, à nos interlocuteurs.

Dans ce cas là, plutôt que de leur envoyer la ressource en pièce jointe il est préférable de leur faire passer uniquement le lien vers la ressource, exactement comme pour le partage de fichiers volumineux présenté sur la fiche précédente, mais c'est encore plus vrai lorsque la ressource est déjà disponible sur Internet.
Il est alors inutile de la copier à nouveau pour la diffuser, toujours pour la même idée de limitation de l'espace de stockage nécessaire sur les serveurs et de la bande passante et de l'énergie utilisée.

Cependant il y a quelques pièges à éviter, d'une part quand c'est vous qui envoyez les liens, mais aussi, et surtout, quand c'est vous qui recevez les liens.

11.1 – Envoyer des liens courts

Lorsque vous indiquez une ressource sur Internet vous devez donner son "URL" (Uniform_Resource_Locator).
L'URL est l'adresse d'une ressource sur Internet.
Cependant, il arrive que ces URL soient à rallonge et ressemblent à ce genre de liens :

> http://www.nathael.net/CPC/#anchor_contact?id=page%20du%20cours%20de%204%C3%A8me&origine=PDF_cours&inutile=osef&sujet=Syst%C3%A8me%20d%27arrosage%20automatique&fiche=29&tracker=04C78FG6HD4

Il existe cependant des outils en ligne qui vous permettent de "raccourcir" ces URL, comme celui proposé par l'association Framasoft : https://frama.link/

Je l'ai utilisé pour transformer le lien ci-dessus en un lien plus court : https://frama.link/LienPlusCourt

Travail à faire :
Renvoyez moi ce même lien, mais avec un autre nom, sur le même principe que ce que j'ai fait.

11.2 – Sans informations personnelles

Les liens à rallonge tels que celui que j'ai mis en exemple plus haut sont parfois inutilement long. C'est d'ailleurs le cas de celui ci. Il donne la même chose que "http://www.nathael.net/CPC/". J'ai volontairement ajouté des informations inutiles, mais parfois ces informations sont utilisées pour vous identifier et suivre votre comportement sur Internet, comme ici : "track/click?u=0c272aa42cc5d055f&id=ed96359&e=dc47c01".

Il est parfois impossible de supprimer cette partie sans perdre le lien original, qui ne vous sera donné que si vous suivez la piste, comme c'est le cas avec le lien "raccourci" donné plus haut, mais bien souvent vous pouvez

supprimer toute la partie après le point d'interrogation (?), ainsi que le point d'interrogation, et conserver toute l'information utile, sans donner vos informations personnelles et sans permettre au site de vous suivre à la trace.

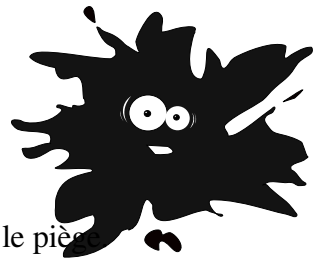
C'est souvent le cas avec les liens des pages des sites de vente en ligne, et avec les liens dans les emails commerciaux.

11.3 – Liens piégés

Mais le pire, ce n'est pas ces liens à rallonge, ce sont les liens présents dans les faux emails d'alerte que vous recevrez, et qui vous feront croire qu'il s'agit de votre banque, de votre fournisseur d'accès à Internet, ou d'un ami dans le besoin, bloqué à l'étranger et que vous devez aider à tout prix ... et si vous suivez ces pistes, cela risque bien de vous coûter très cher !

Ces messages sont parfois tellement ressemblant que même les personnes les plus attentives se font avoir, par exemple parce que le message tombe pile au moment ou il devient crédible (pour vous avertir d'un problème de paiement alors que vous êtes justement à découvert par exemple).
Ces messages peuvent être des emails, mais aussi des SMS, des messages privés sur des forums de discussion, ou tout autre technique qui permettrait de vous contacter de façon privilégiée, pour vous prendre au piège.

Pour détecter ces messages, ce n'est pas toujours simple.
Bien souvent, le sujet sera choisi pour vous faire peur :
- Votre compte a été piraté!
- Message urgent
- Message confidentiel
- Refus de renouvellement
- Prélèvement rejeté par votre banque
- ...



Et la liste est potentiellement très très très longue !
Autant de sujets qui peuvent vous faire paniquer, et vous faire tomber dans le piège.

Ce type de piège a un nom : le phishing (ou hameçonnage (lien Wikipedia) en Français).

Le principe est toujours le même : le message affiche un lien qui semble valide, comme par exemple celui-ci :
https://fr.wikipedia.org/wiki/Hameçonnage
Sauf que le vrai lien ne vous conduira pas vers Wikipedia, mais vers un piège.

Dans le cas du phishing, vous arriverez sur un site très ressemblant à celui que vous pensez consulter, mais qui ne sera qu'une copie du vrai site.
Mis en confiance, vous allez alors saisir vos identifiants et mots de passe … et c'est alors déjà trop tard, l'attaquant a votre mot de passe sur le vrai site et peut l'utiliser pour s'y connecter et, par exemple, vider vos comptes bancaires.

Un premier indice, très simple à détecter, c'est que l'adresse réelle ne correspond pas à l'adresse affichée dans le message. La plupart des logiciels vous afficheront le lien réel dans une info-bulle ou en bas de page lorsque vous avez la souris au dessus du lien. Si les deux adresses sont différentes, ne suivez pas la piste !

Il y a d'autres techniques pour détecter ces problèmes, je vous laisse les lire sur la page Wikipedia (la vraie !)

PS : la bonne piste est ici : http://www.nathael.net/CPC/hammecon_ok.html !