Après le « phishing » voici le « vishing »...

Les SPAMS et les HOAX….

…. Deux petites bêtes qui surchargent nos boites mails. Ce ne sont pas des virus, mais ils représentent une perte de temps indéniable pour celui qui les reçoit !

- ✔ L'HOAX est une « imposture » créé à des fins malveillantes ; ce sont souvent des lettres-chaines qui divulguent de fausses informations sur le même modèle que les légendes urbaines ; pour démêler le vrai du faux, un site : http://www.hoaxbuster.com/

- ✔ Le SPAM est un courriel indésirable, qui porte aussi le nom de « pourriel » ; il s'agit en général d'envois en masse, destinés soit à des fins publicitaires soit à l'hameçonnage (ou « phising »).

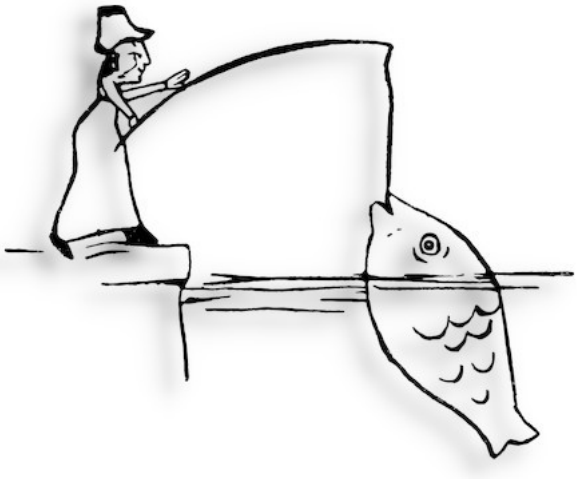
Nous avons tous reçus de faux messages de notre banque, du Trésor Public, de la CAF, de la sécurité sociale nous demandant de fournir notre mot de passe ou bien nos coordonnées bancaires ; sachez qu'aucune administration, qu'elle quelle soit, ne vous demandera ce type de renseignements !

Il est possible de se protéger des spams en suivant quelques règles simples :

- ✔ essayez de ne pas donner votre adresse e-mail à n'importe qui,
- ✔ n'ouvrez pas les messages suspects (vérifiez bien la source) et mettez-les directement dans la « corbeille » ; c'est comme un colis piégé, n'ouvrez surtout pas, ne cliquez sur aucun lien...La curiosité pourrait bien vous jouer un mauvais tour !
- ✔ connectez-vous à : https://www.signal-spam.fr/ et bloquer l'adresse frauduleuse !

Un conseil supplémentaire : jeter systématiquement les « confirmations de lecture » ; elles servent bien souvent à vérifier que votre adresse est valide et vous exposent à encore plus de spams !

Vous avez sans doute entendu parler de l'hameçonnage, plus communément nommé « filoutage » ; c'est une technique employée par les fraudeurs au seule fin de pirater vos données personnelles et entre autre, celle de votre carte bancaire...



La plus utilisée est le « phishing », de l'anglais (fishing), c'est-à-dire « pêche à la ligne », est une arnaque qui consiste à tromper son destinataire et à se faire passer pour un organisme administratif voire bancaire.

Les escrocs débordent de créativité ; du fait de la méfiance du grand public face au « phishing », une nouvelle méthode fait son apparition depuis quelques temps : « le vishing », dérivé de l'anglais « voice ».

Le vishing consiste à passer un appel téléphonique en se faisant passer notamment pour un employé de la banque (ou autre organisme) afin de soutirer vos données personnelles : mots de passe, numéros de comptes bancaires, codes de carte bleue, etc.

Vous pouvez également recevoir un message alarmant tel que « Nous suspectons une transaction non autorisée sur votre compte, rappelez le numéro.... » : **ne rappelez surtout pas ! Contactez soit votre banque, soit l'organisme concerné, en cas de doute.**

Pour se protéger de cette cybercriminalité, restez vigilants. Si malgré tout, vous êtes victime de ces escroqueries, vous pouvez :

- ✔ signaler la tentative de "phishing" sur le site dédié du gouvernement: https://www.internet-signalement.gouv.fr/
- ✔ déposer plainte auprès du commissariat de police le plus près de chez vous,
- ✔ signalez l'arnaque en ligne, comme arnaques-internet.info ou hoaxbuster.com.

Pour en savoir plus :

La cybermalveillance : https://www.inc-conso.fr/content/comment-se-proteger-contre-la-cybermalveillance-0

Le portail de la sécurité informatique : https://fr.wikipedia.org/wiki/Portail:S%C3%A9curit%C3%A9_informatique

La gendarmerie nationale : https://www.gendarmerie.interieur.gouv.fr/Nos-conseils2/Pour-les-particuliers/Me-proteger-sur-Internet/Le-vishing

La DGCCRF : https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/Phishing-hameconnage-ou-filoutage

Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) : https://www.ssi.gouv.fr/entreprise/principales-menaces/cybercriminalite/attaque-par-hameconnage-phishing/

La CNIL : https://www.cnil.fr/fr/spam-phishing-arnaques-signaler-pour-agir

Gare aux faux sites : https://www.police-nationale.interieur.gouv.fr/Actualites/Dossiers/Cybercrime/Prevention-contre-le-phishing

Perceval, un téléservice pour signaler en ligne une fraude à la carte bancaire : https://www.interieur.gouv.fr/Actualites/Infos-pratiques/Perceval-un-teleservice-pour-signaler-en-ligne-une-fraude-a-la-carte-bancaire

Le blog de Denis JACOPINI : https://www.lenetexpert.fr/quest-ce-que-le-smishing/