Messagerie électronique

Le courrier électronique est un mode de communication disponible 24 heures sur 24 et qui permet l'échange de tous types de contenus. Il requiert toutefois un minimum de précautions pour assurer une communication fluide et éviter certains désagréments.

Les types de messagerie

Il existe aujourd'hui deux types de messagerie soit :

- celle opérée au travers de clients de messagerie classiques, tels qu'Outlook express, mozilla Thunderbird, etc.,

- les messageries directement accessibles en ligne à partir de n'importe quel ordinateur : les « web-mails ». Yahoo, Hotmail, gmail fournissent les webmails les plus connus.

Ces dernières solutions offrent l'avantage d'une très grande souplesse d'utilisation mais la confidentialité des échanges peut poser problème aux personnes, dans la mesure où celles-ci n'en ont pas le contrôle.
De plus, le respect de la vie privée n'est pas absolument garanti (gmail génère ainsi des publicités basées sur le contenu des messages).

Les bonnes pratiques

Evitez tout ce qui nuit à la clarté du message ou augmente inutilement la taille de l'e-mail. Les signatures longues avec clause de confidentialité, les fonds colorés, les images et v-card attachées sont ainsi à utiliser avec prudence.

N'envoyez pas de pièces jointes volumineuses, à moins que vous ne sachiez déjà que la connexion utilisée par le destinataire en permet la réception.

Pour ne pas risquer de perdre votre temps après coup en de fastidieux envois multiples de pièces jointes, il est plus simple d'envoyer un lien vers un site de téléchargement où les documents auront été préalablement placés. Si vous souhaitez envoyer un même message à des destinataires qui ne se connaissent pas, et à plus forte raison s'ils sont nombreux,

utilisez le champ CCI (Copie Cachée Invisible) pour y copier les différentes adresses. de cette façon elles resteront masquées.

Les désagréments

Scam :

Pratique frauduleuse basée sur un abus de confiance, consistant le plus souvent à dérober des sommes d'argent à des victimes en leur faisant miroiter de plus gros gains.

Spam :

Encore le problème numéro un du courrier électronique, le spam est un message non sollicité envoyé à des milliers ou des dizaines de milliers d'exemplaires. On estime que le trafic de spams représente, selon les pays, 80 à 95% du trafic global des courriels.

Le Clickjacking

Le **Clickjacking** est une technique malveillante visant à pousser un internaute à fournir des informations confidentielles ou à prendre le contrôle de son ordinateur en le poussant à cliquer sur des pages sûres. Il se trouve un cadre invisible sous la page web comme l'effet d'un calque, pour pousser l'internaute à cliquer sur des liens cachés.

Un exemple a été réalisée avec un jeu flash où l'internaute doit cliquer sur des boutons pour marquer des points. Certains clics du jeu font cliquer l'internaute sur des autorisations pour activer la webcam de l'ordinateur.

Pour éviter d'être victime de ce genre d'actions malicieuses, passez par une sécurisation du navigateur web et installez l'extension **Ghostery** disponible sur les 5 navigateurs principaux (**https://www.ghostery.com/fr.)** Cette extension bloque les scripts et diverses techniques de Clickjacking.

Usurpation d'identité : le protocole du courrier électronique est un protocole assez simple, qui ne fournit pas de mécanisme natif permettant d'authentifier à coup sûr que l'émetteur d'un message est bien celui qu'il prétend être.

Il se peut, par exemple, que vos correspondants reçoivent des spams ou des virus qui semblent venir de vous alors que vous n'y êtes évidemment pour rien.

C'est que votre adresse e-mail a été trouvée dans un carnet d'adresses quelconque et sert de substitut à l'envoi de ces e-mails frauduleux d'identité.

Ver (ou « Worm » en anglais) :

Contrairement aux virus qui infectent des fichiers et des supports de données dans un seul et même ordinateur, les vers utilisent le courrier électronique et le carnet d'adresses pour se propager d'ordinateur en ordinateur.

Virus :

La messagerie est un important vecteur de transmission des virus, il ne faut donc absolument jamais ouvrir de pièce jointe à un e-mail si vous ne pouvez pas identifier l'expéditeur.

Il peut arriver que notre identité soit usurpée et utilisée à mauvais escient (suite à la compromission de notre mot de passe ou, tout simplement en créant un compte illégitime à notre nom sur un réseau social x ou y) pour envoyer du **SPAM**, pour rigoler ou juste pour nuire.

Développez votre sens critique. Toute information (**et sa source**) doivent être considérées avec prudence et circonspection !

Le Rançongiciel

Mardi 8 août 2017, de nombreuses entreprises ont été touchées par un virus informatique redoutable. Surnommé «NotPetya», il bloque complètement les ordinateurs et réclame une rançon à ses victimes.

Ce genre de programme est baptisé **«rançongiciel»,** ou **«ransomware»** en anglais. Il s'agit d'un virus informatique qui chiffre les fichiers d'un ordinateur. Les victimes ne peuvent alors plus accéder aux contenus de leur machine. Ces virus se propagent surtout en entreprise, mais peuvent aussi toucher des particuliers. On leur demande généralement de payer une rançon pour récupérer leurs fichiers. D'où le nom de **«rançongiciel».**

Que faire lorsque l'on est victime d'un rançongiciel ?

1. La première chose à faire est de **déconnecter** toutes les machines qui pourraient être reliées à votre ordinateur. Il peut s'agir d'une **clé USB**, d'un **disque dur externe**, d'un **téléphone** portable à charger, etc. **Déconnectez votre ordinateur du réseau** sur lequel il est connecté. **Coupez le WiFi**, **retirez le câble ethernet**.

   L'idée est d'établir une quarantaine autour de la machine infectée, pour que le virus ne puisse pas affecter d'autres appareils, ou se propager par le réseau informatique d'une entreprise ou de particuliers.

Est-ce qu'il faut payer la rançon ?

Non ! Beaucoup de victimes ne récupèrent pas leurs fichiers, même après avoir transféré de l'argent aux pirates. Cela risque par ailleurs de compromettre votre carte bancaire, si vous l'utilisez pour faire un virement.

Si vous savez et pouvez le faire, reformatez votre disque et réinstallez vos programmes. Sinon, contactez un prestataire compétent de cybersécurité qui pourra vous accompagner. Vous pouvez enfin porter plainte au commissariat

Phishing (hameçonnage ou filoutage)

Le *phishing* (hameçonnage ou filoutage) est une technique par laquelle des personnes malveillantes se font passer pour de grandes sociétés ou des organismes financiers qui vous sont familiers en envoyant des mèls frauduleux et récupèrent des mots de passe de comptes bancaires ou numéros de cartes de crédit pour détourner des fonds.

Quel est le principe du phishing ?

Le principe du *phishing* est de récupérer des données personnelles sur internet.

Le moyen utilisé est **l'usurpation d'identité**, adaptée au support numérique.

L'escroquerie repose le plus fréquemment sur la contrefaçon d'un site internet (**celui d'une banque ou d'un marchand en ligne**). L'adresse URL du lien comprise dans le mèl est également **« masquée »** afin de paraître authentique.

Des mèls à connotation alarmiste ou d'autres alléguant d'un prétendu remboursement en faveur de l'internaute sont ensuite massivement adressés.

Ils semblent provenir d'une source de confiance (banque, CAF, impôts, etc.) et invitent à se rendre sur une **page de formulaire imitée** afin de fournir des données personnelles et souvent à caractère financier.

Ces informations sont ensuite récupérées par les *phishers*.

Pendant toute la procédure, la victime croit avoir à faire à un site officiel d'un opérateur qu'elle connaît. Les liens figurant sur la page internet du formulaire sont souvent inactifs.

Comment s'en protéger ?

(source : www.securite-informatique.gouv.fr)

- **Les centres des impôts n'envoient jamais ce genre de courriel.** Ils ne passent jamais par un courrier électronique pour demander à leurs assujettis de saisir leurs informations personnelles.

- **Les banques et organismes sociaux (CAF, mutuelles, etc.) n'envoient jamais ce genre de courriel** : Ils ne passent jamais par un courrier électronique pour demander à leurs clients de saisir leurs informations personnelles. Pour se connecter au site de sa banque il vaut mieux entrer manuellement l'adresse réticulaire (URL) du site dans votre navigateur.

- **Préférer saisir des informations personnelles (coordonnées bancaires, identifiants, etc.) sur des sites internet sécurisés** : un cadenas apparaît dans le navigateur et l'adresse du site commence par **HTTPS** au lieu de http.

- **Ne pas cliquer sur les liens contenus dans les courriers électroniques** : les liens affichés dans les courriers électroniques peuvent en réalité diriger les internautes vers des sites frauduleux. En cas de doute, il est préférable de saisir manuellement l'adresse dans le navigateur.

- **Être vigilant lorsqu'un courriel demande des actions urgentes**.

- **Utiliser le filtre contre le filoutage du navigateur internet** : la plupart des navigateurs (Microsoft Internet Explorer , Mozilla Firefox, Opéra) proposent une fonctionnalité d'avertissement contre le filoutage. Leurs principes peuvent être différents (liste noire, liste blanche, mot clé, etc.) et sans être parfaites, ces fonctions aident à maintenir la vigilance de l'utilisateur.

- **Utiliser un logiciel de filtre anti-pourriel** : la plupart du temps ces tentatives d'escroquerie se diffusent par le biais de courriers électroniques. Même si les logiciels de filtrage ne sont pas parfaits, ils permettent de réduire le nombre de ces courriels.

- **Ne jamais répondre ou transférer ces courriels**.

- **En cas de doute ou de problème, prendre contact rapidement avec son agence bancaire ou l'organisme qui aurait envoyé ce courriel**.

- **D'une manière générale, être vigilant et faire preuve de bon sens** : ne pas croire que ce qui vient de l'internet est forcément vrai.

Signalez l'abus d'utilisation d'informations personnelles aux autorités compétentes.

Si vous pensez avoir été victime d'une escroquerie par *phishing*, signalez le immédiatement sur la plateforme « PHAROS » (plateforme d'harmonisation, d'analyse de recoupement et d'orientation des signalements) à l'adresse suivante :

- **www.internet-signalement.gouv.fr**