Votre boite mail

Mieux gérer votre boite mail pour gagner en productivité

FICHE OUTILS N°3-4

Introduction

Nous passons environ 10 heures chaque semaine sur notre boite email !
Un simple gain d'efficacité de 10% nous fera donc gagner 1 heure de vie supplémentaire chaque semaine, soit une demi journée chaque mois !

Gagner en productivité dans la consultation et le traitement de vos emails.

Avant d'écrire un email, estimer si c'est le moyen le plus approprié pour communiquer :
- Utiliser les réunions pour expliquer ou comprendre des situations complexes
- Utiliser la messagerie instantanée pour des réponses rapides
- Utiliser des espaces collaboratifs pour partager et travailler sur des documents en équipe.

Quelques astuces de productivité pour le traitement et l'organisation des emails.

- Réduisez le nombre de consultations de votre boite email à 2 à 4 fois maximum par demi/journée : Décidez vous-même de la fréquence de façon raisonnée et consciente, et n'imaginez pas que « tout le monde » s'attend à ce que vous répondiez immédiatement à vos emails.

- Planifiez le traitement des emails à des plages fixes dans votre agenda (par exemple matin, midi, après-midi et soir) et **supprimez l'affichage des alertes emails.**

- Réalisez une action pour chaque email consulté.
  Une règle applicable par exemple est celle des 4 D :
  - S'il s'agit d'un email non important **D**elete it (le supprimer) immédiatement
  - Si l'email peut être traité en moins de deux minutes « **D**o-it » (le traiter)
  - Si l'email ne vous est pas destiné **D**elegate it (le déléguer)
  - Si vous devez le traiter mais cela prend plus de 2 minutes (incluant sa lecture) **D**efer it (reporter son traitement).

CNAS
L'action sociale sourire compris

- **Filtrez vos emails par sujet ou dossier**, cela vous permet de traiter plusieurs emails d'un même sujet en même temps.
  Organisez des dossiers de classement (arborescence structurée) dans la messagerie en fonction des thèmes (dossier client, dossier fournisseur,...) et de vos priorités (traitement / recherche) et utilisez des règles de classement automatique pour vous aider à traiter vos emails. Par exemple, faites des répertoires avec les emails adressés en direct, en copie, venant de votre supérieur direct, venant de liste de diffusion, etc.... Créez notamment des répertoires spécifiques pour les emails non prioritaires dans l'activité : lettres d'informations, correspondances personnelles,...

- Utilisez le « volet de lecture » de votre logiciel de messagerie afin de visualiser le contenu de vos emails en même temps que la liste des emails.

- Utilisez la visualisation par conversation (« thread ») pour condenser l'ensemble des échanges à partir d'un même email de départ.

- Désinscrivez vous des news-letter que vous n'ouvrez jamais et indiquez à vos correspondants de ne plus vous envoyer certains emails s'il n'est pas pertinent que vous les receviez.

- Utilisez des marqueurs de suivi pour les emails à traiter ou en attente de réponse.

- Utilisez systématiquement un moteur de recherche local pour rechercher des emails ou des fichiers (recherche effectuée quelle que soit la localisation de l'élément en bénéficiant de la puissance de l'indexation pré-constituée).

Délégation et absence

- Indiquez votre statut d'absence si vous n'êtes pas en mesure de consulter vos emails afin que vos correspondants puissent adapter leur communication si nécessaire (renvoi automatique d'un email d'absence).

- Utilisez les règles de délégation si vous partagez des boites de messagerie au sein d'une équipe ou entre un manager et son assistante.

Attention au phishing (source DGCCRF)

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 emails frauduleux et récupèrent des mots de passe de comptes bancaires ou numéros de cartes de crédit pour détourner des fonds.
(Voir plus d'informations en annexe de ce document)

Choisir et gérer ses mots de passes : Source « Comment ça marche »

Avec la multiplication des comptes d'utilisateurs nécessitant une authentification, ces derniers sont de plus en plus difficiles à mémoriser. Pourtant, le choix de mots de passe complexe est crucial. Avec quelques conseils de base, et des outils pratiques, il est assez facile de bien choisir, sécuriser et gérer ses mots de passe.
(Voir plus d'informations en annexe de ce document)

Ce qu'il faut retenir de ce chapitre

- Choisissez le nombre de consultations quotidien de votre boite email.
- Supprimez l'affichage des alertes emails.
- Filtrez ou classez dès réception vos emails par sujet ou dossier.
- Appliquez la règle des 4 D (Delete, Do, Delegate, Defer).
- Soyez vigilant au phishing.
- Soyez vigilant dans le choix de vos mots de passe.

EXERCICE

Pendant les 2 jours qui viennent, changez vos habitudes vis à vis de vos email avec ces 4 exercices :

- Supprimer l'affichage des alertes emails (sur votre PC et votre mobile)
- Une consultation (et traitement) de vos email en début et fin de matinée et d'après midi.
- Désinscrivez vous de au moins 1 news letter par jour
- Testez la règle des 4 D

Au delà de cette période, adaptez une méthode dans le même esprit qui vous convient

FICHE OUTIL N°3-4

Pour aller plus loin :
Prévenir le phishing : Bon sens et vigilance.

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 l'email est également « masquée » afin de paraître authentique.
Des emails 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 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, 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.

* 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 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-spam : 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, contactez directement l'émetteur .

Signalez l'abus d'utilisation d'informations personnelles aux autorités compétentes sur www.internet-signalement.gouv.fr

CNAS
L'action sociale sourire compris

Comment choisir un mot de passe ? Cinq conseils de base

Il n'existe pas de "recette" permettant de sécuriser à 100% un mot de passe, mais des conseils simples suffisent pour bien prendre en compte cet aspect :

Longueur du mot de passe

- Choisir un mot de passe d'une longueur minimum de 8 caractères : idéalement, il doit être composé d'au moins 14 caractères. La longueur du mot de passe est primordiale si vous optez pour une chaîne de caractères du même type pour une question de mémorisation (ex : seulement des lettres ou des chiffres).

Utiliser toutes les possibilités du clavier

- Combiner les types de caractères : lettres, chiffres, symboles et signes diacritiques (^,¨,$,!,#/, etc.) éventuellement les lettres majuscules si le service (ex : adresse email) est sensible à la casse.

Recourir à la mnémotechnique

Une chaîne de caractères trop complexe peut être difficile à mémoriser, surtout si elle est peu signifiante. Un moyen simple pour associer mémorisation et complexité du mot de passe est de partir d'une phrase ou d'un mot qui fait sens. Si votre passion est la calligraphie, pourquoi ne pas partir de là. Vous pouvez changer l'ordre des lettres, puis intercaler des chiffres et des symboles.
Ex : "phie33gra£cali%"

Un mot de passe pour chaque compte d'utilisateur

Avec la multiplication des comptes et accès nécessitant une authentification, la tentation est d'opter pour un mot de passe unique. Dans la mesure du possible (c'est à dire de ses capacités de mémorisation), il est conseillé de choisir un mot de passe par compte. A défaut, il est recommandé d'appliquer cette règle aux accès les plus sensibles (ex : banque en ligne)... Les gestionnaires de mots de passe comme Keepass permettent de pallier cette difficulté (voir plus bas).

Changer fréquemment de mots de passe

Le renouvellement fréquent des mots de passe est une astuce simple pour éviter les attaques de type phishing (usurpation d'identité).

En savoir plus sur :

https://www.commentcamarche.com/faq/29818-choisir-securiser-et-gerer-ses-mots-de-passe.