

Pour échanger conseils et astuces afin d'optimiser la gestion des blogs de l'ARA.

Edition n° 8 du 1er mai 2014

Bonjour,

Pour tout internaute, la multiplication des services web proposés génère une multiplication équivalente de mots de passe. Il n'est pas toujours évident de se souvenir de tous et pas très simple d'en trouver de nouveaux qui soient réellement sécurisés.

Devant le grand nombre de mots de passe à mémoriser, la tentation est d'utiliser toujours le même ou de ne se servir que de mots de passe faciles à retenir. On peut également être tenté de stocker tous ses mots de passe sur son ordinateur.

On se dit ensuite que son Firewall et son anti-virus suffiront mais, si on cède à ces solutions de facilité, on devient une proie rêvée pour les pirates informatiques.

En tant que particulier, on ne s'inquiètera "que" de ses transactions bancaires ou commerciales (Paypal, E-Carte bleue, accès aux sites marchands) et de l'utilisation frauduleuse de son ordinateur.

En tant que responsable de la gestion de blogs ou de sites web, on doit être beaucoup plus vigilant car on peut mettre en péril les contenus de tous les blogs que l'on gère et de tous les sites web qui les hébergent.

Vous l'avez deviné, dans ce numéro 8 de la "lettre aux bloggers", nous allons aborder les thèmes de la sécurité et de la confidentialité sur votre ordinateur et sur votre messagerie.

Sans céder à la paranoïa inhérente à ces thèmes, nous allons chercher des solutions simples et préconiser des habitudes de travail faciles à mettre en uvre.

***Concernant la sécurité**, nous allons parler de la gestion de vos identifiants et de vos mots de passe.*

***Concernant la confidentialité**, j'aimerais que nous abordions la gestion de vos messages privées et de vos messages publics.*

Pour ne pas cantonner ce numéro à des préoccupations essentiellement sécuritaires, nous allons également traiter de sujets comme l'utilisation de boutons dans vos articles et vos pages et comme l'enrichissement de votre éditeur de texte.

Je vous souhaite une bonne lecture de cette "lettre aux bloggers". Pour les prochains numéros, faites-moi part des sujets qui vous intéresseraient.

Cordialement, Pierre Favre

Au sommaire de cette lettre aux bloggers n°8 :

Protéger mes informations confidentielles : pourquoi et comment ? 4

- Gérer les mots de passe sur son ordinateur 4
- Mon anti-virus et mon FireWall ne me protègent donc pas ? 4
- Comment protéger mon ordinateur malgré les carences des anti-virus et des firewall ? 5
- Utiliser un gestionnaire de mots de passe 5
- On récapitule ? 6
- Quelques sites à parcourir sur le piratage et la sécurité... 6

Messages : à la recherche de la confidentialité. 7

- Adresse de messagerie privée et adresse de messagerie publique. 7
- Quelle différence entre POP et IMAP ? 7
- Partage des messages avec d'autres membres d'une association. 8
- Bien choisir son adresse de messagerie publique. 8
- Le risque d'exposition aux spams. 8

L'utilisation de boutons dans vos articles et dans vos pages. 9

- Des boutons pour faire quoi dans les blogs ARA ? 9
- Placer une URL dans chaque bouton 9
- Paramétrage d'un bouton sur votre blog ARA. 9
- Utilisation d'un bouton ou d'un lien texte ou image ? 9

Comment optimiser l'utilisation de votre éditeur de texte 11

- L'éditeur de texte utilisé dans nos blogs ARA 11
- Les réglages de l'éditeur TinyMCE Advanced 11
- Des outils intéressants... ou non dans la barre d'outils de votre éditeur 12
- Pour conclure avec l'utilisation de l'éditeur TinyMCE Advanced 12

Protéger mes informations confidentielles : pourquoi et comment ?



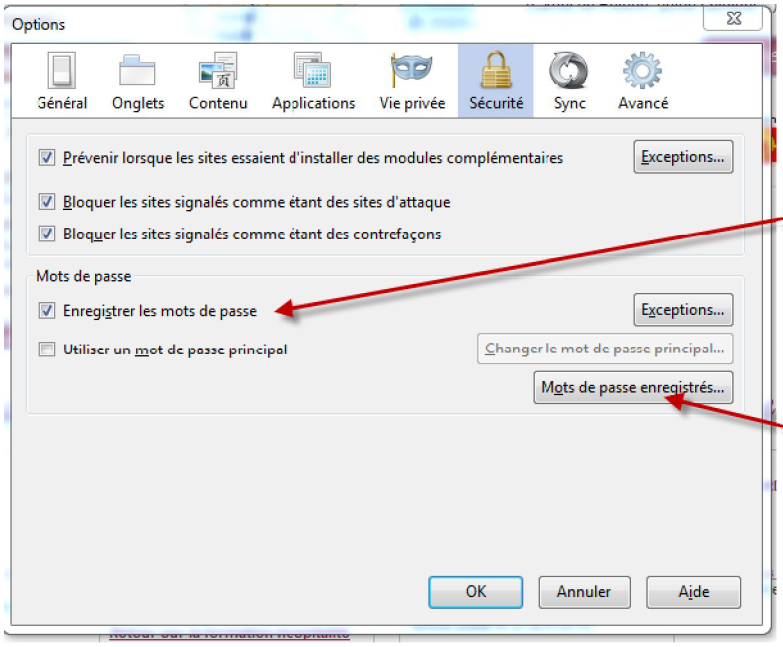
Quand on parle d'informations confidentielles sur un ordinateur, on évoque surtout la gestion des mots de passe permettant d'accéder à des services sur le web. Mais on peut également avoir envie de protéger des fichiers contenant des informations personnelles ou confidentielles (codes, testaments, dispositions bancaires, etc.).

Si on "laisse traîner" ces informations confidentielles sur son ordinateur sans protection, elles risquent d'être rapidement pillées et... exploitées.

Gérer les mots de passe sur son ordinateur

Comme on l'a dit plus haut, devant la multiplication des mots de passe, un utilisateur cède souvent à la facilité. Soit il va utiliser systématiquement le même mot de passe partout (et ce mot de passe sera facile à mémoriser donc facile à "craquer"), soit il va stocker ses mots de passe sur son navigateur préféré.

Sur Firefox, cela va donner cela :

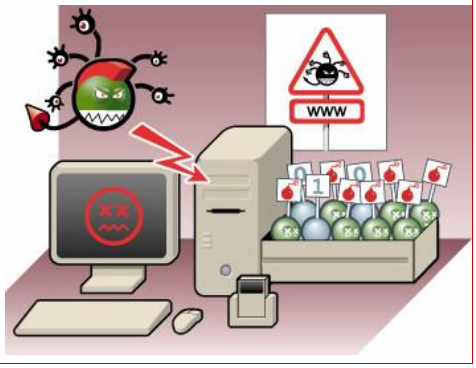


Dans le menu "Options" de Firefox, si cette case est cochée, tous vos mots de passe seront enregistrés.

A tout moment, vous pouvez consulter les mots de passe mémorisés sur votre navigateur !!!

Cette solution est très confortable mais elle va considérablement diminuer votre niveau de sécurité. En tant que particulier, c'est un risque que vous pouvez courir si vous ne gérez ni vos comptes bancaires, ni vos impôts, ni vos paiements via votre ordinateur. En tant qu'administrateur d'un blog ou d'un site web, c'est beaucoup plus discutable !

Mon anti-virus et mon FireWall ne me protègent donc pas ?



Un antivirus protège contre les codes malveillants quôil connaît ou quôil reconnaît. Le temps que lôéditeur écrive lôempreinte (on parle aussi parfois de signature du virus) dôun nouveau virus et que lôantivirus la télécharge, lôinternaute nôest pas protégé.

Il est donc indispensable dôutiliser un antivirus à jour.

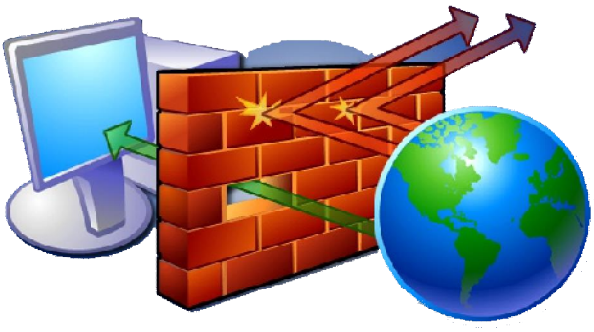
Un antivirus peut fonctionner de deux manières différentes : tout dôabord à partir dôune base dôempreintes de virus puis, éventuellement en complément, dôun système dôintelligence artificielle pour détecter certains comportements suspects. A chaque fois quôun nouveau logiciel malveillant est détecté, le fournisseur de votre antivirus alimente lôencyclopédie constituée de lôensemble des empreintes, puis la

diffuse par lôinternet pour que son antivirus puisse le détecter.

On comprend alors aisément quôil est indispensable de maintenir à jour la liste des empreintes virales. Ainsi, un antivirus qui nôaura pas été mis à jour depuis plusieurs jours *vous donnera un faux sentiment de sécurité* et sera incapable de détecter les nouvelles menaces.

Attention : un antivirus ne constitue pas une protection intégrale contre tous les risques. La vigilance de lôutilisateur sur des comportements anormaux reste indispensable. Comme toute application, un antivirus doit être mis à jour (non seulement sa base dôempreintes mais également le logiciel lui-même).

Un Firewall nôest pas (non plus) lôoutil de protection absolu. Même si ces équipements sont capables dôassurer des fonctions de sécurité évoluées (filtrage plus ou moins fin de quasiment tous les protocoles, authentifications fortes, canaux de communication sécurisés, journalisation .... et analyse du trafic, administration centralisée de plusieurs Firewallsé). Cependant, ils ne peuvent pas :



- Faire une analyse sémantique du contenu des flux (certains types de backdoors, canaux cachésé)
- Sôaffranchir du système dôexploitation,
- Garantir une étanchéité de 100%,
- Protéger le réseau des attaques internes ou, plus généralement, des attaques ne passant pas par eux.

Comment protéger mon ordinateur malgré les carences des anti-virus et des firewall ?

La principale protection de votre ordinateur dépend de votre comportement avant tout.

Vous devez éviter de vous promener n'importe où sur le web, vous devez éviter d'ouvrir n'importe quelle pièce jointe sur les messages que vous recevez et vous devez être prudent avant de cliquer sur un lien.

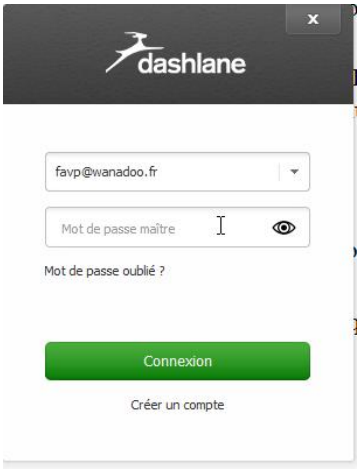
Vous devez choisir un anti-virus + Firewall sérieux : évitez les logiciels gratuits qui ne gèrent pas les mises à jour avec le même sérieux que les produits payants : nous avons vu plus haut que la fiabilité d'un anti-virus dépend de la qualité et de la périodicité des mises à jour de sa " base dôempreintes"...

Avec votre anti-virus, vous devez analyser complètement votre ordinateur une fois par mois au moins. En effet, la "protection résidente" qu'offre votre anti-virus ne couvre que la mémoire, certaines zones de votre disque principal et les flux entrants. Les pirates le savent, vous vous en doutez bien.

Enfin, vous pouvez adopter des outils et des méthodes pour améliorer votre protection :

- Installation d'un "coffre-fort" ou d'un "trousseau d'accès" qui sont des logiciels permettant de regrouper, de stocker et de partager vos mots de passe et vos fichiers confidentiels. Le stockage se fait souvent sur un site web sécurisé. Lorsque vous vous connectez, les informations sont chargées en mémoire mais pas stockées dans un fichier de votre ordinateur.
- Méthodes : ne jamais mémoriser les mots de passe sur votre ordinateur, consulter vos mails en ligne pour éliminer ceux qui ne vous conviennent pas avant de rapatrier les bons sur une "messagerie client", être méfiant.

Utiliser un gestionnaire de mots de passe



Les "gestionnaires de mot de passe" sont des logiciels (gratuits ou non) que l'on retrouve aussi bien sur Mac que sur PC.

Leur principe est toujours le même : ils mémorisent tous les mots de passe utilisés sur l'ordinateur pour les stocker sur un site web sécurisé. Sur votre ordinateur, ces mots de passe seront automatiquement proposés sur les bonnes zones à renseigner.

Pour bénéficier du "rapatriement" de tous ces mots de passe, il suffit de saisir un mot de passe principal soit au démarrage soit à partir de l'instant où vous en avez besoin. Jusqu'à ce que l'ordinateur soit éteint, ces mots passe resteront en mémoire.

Avantages :

- Rien n'est stocké sur votre ordinateur. Vos informations confidentielles sont physiquement stockées sur un site sécurisé.
- Vous pouvez utiliser des mots de passe complexes puisque vous n'avez plus à les mémoriser.
- Vos mots de passe peuvent être partagés sur vos ordinateurs, votre tablette et votre smartphone.
- Vous pouvez également sauvegarder des fichiers entiers dans un "coffre-fort numérique". Même chose avec des mots de passe ou des identifiants divers (codes de cartes bleues, codes PIN, authentification WiFi, copie de vos papiers d'identité, etc.).
- Simplicité de mise en oeuvre et d'utilisation.

Ces logiciels sont également appelés "Trousseaux d'accès" (sur Mac) ou "coffre-fort" dans certains anti-virus comme Bit-Defender. Cependant, méfiez-vous des packages anti-virus + gestionnaire de mots de passe. En effet, les pirates s'en prennent d'abord aux anti-virus et Bit-Defender, par exemple, est le plus connu.

Des avis et des tests vous aident à faire le meilleur choix et à attester de la sécurité et de la fiabilité des logiciels :

- https://www.dashlane.com/fr (Dashlane gratuit ou Dashlane Premium ?).
- http://www.securitemac.com/trousseau-d-acces (la sécurité sur Mac).
- http://www.koingosw.com/products/dataguardian.php (un concurrent à Dashlane sur Mac ou sur PC).

On récapitule ?

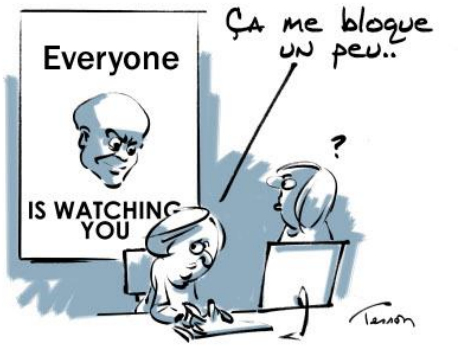
- ✓ Soyez prudents dans l'utilisation du web et de la messagerie.
- ✓ Ne stockez pas vos mots de passe dans votre navigateur web ou votre outil de messagerie.
- ✓ Utilisez un gestionnaire de mots de passe qui va stocker vos identifiants + password à l'extérieur de votre ordinateur.
- ✓ N'hésitez pas à utiliser des mots de passe complexes (plus de 12 caractères mêlant chiffres et lettres minuscules et majuscules) car ils seront gérés par votre gestionnaire de mots de passe.
- ✓ Utilisez un anti-virus et un firewall sérieux et régulièrement mis à jour (à chaque connexion).
- ✓ Avec votre anti-virus, effectuez une analyse complète et détaillée de votre ordinateur au moins une fois par mois.
- ✓ Evitez de transmettre vos identifiants par mail.
- ✓ Croisez les doigts !

Quelques sites à parcourir sur le piratage et la sécurité

- http://www.securite-informatique.gouv.fr (page très complète sur la sécurité informatique sous tous ses aspects).
- http://projet.piratage.free.fr/techniques.html (techniques de piratage : instructif).
- http://www.securitepc.fr/mesuresecurite.html (quelques conseils de sécurité).

Fin de l'article " Protéger mes informations confidentielles : pourquoi et comment ?"

Messages : à la recherche de la confidentialité.



Echanger des messages au sein d'une association est absolument nécessaire. Cela amène certains responsables de cette association à afficher leur adresse mail sur des pages web publiques.

Dans cette logique, chacun doit faire attention à la protection de sa vie privée et aux risques d'exposition aux spams.

Nous allons aborder ici quelques concepts pour concilier la nécessité de communiquer et les impératifs de la vie privée.

Adresse de messagerie privée et adresse de messagerie publique.

Lorsqu'on recherche la confidentialité et la protection de sa vie privée, on ne livre pas son adresse de messagerie privée au vu et au su de tout le monde... tout particulièrement sur internet. On se crée une adresse de messagerie "publique" (chez Google, par exemple) que l'on utilisera pour tous les échanges au sein d'une association.

Ainsi, on pourra afficher cette adresse publique sur un site web ou un blog. Les messages reçus seront parfaitement distincts des messages privés. Quand on choisira cette adresse de messagerie publique, on vérifiera qu'elle fonctionne en mode IMAP.

Quelle différence entre POP et IMAP ?

POP(Post Office Protocol) : le protocole POP a été conçu pour vous permettre de récupérer votre courrier sur une machine distante quand vous nôêtes pas connecté en permanence à Internet. Le protocole POP bloque votre boîte aux lettres pendant que vous y accédez, ne permettant pas à une autre connexion dôaccéder en même temps à votre courrier.

Lôévolution du courrier électronique vers le multimédia et le manque de flexibilité de POP favorisent lôémergence dôun nouveau protocole : lôIMAP

IMAP(Interactive Mail Access Protocol) : lôIMAP est un autre protocole moins utilisé que POP mais qui offre plus de possibilités. Avec IMAP, *tous vos courriers et vos dossiers de messages restent sur le serveur*. A chaque fois que vous vous connectez au serveur par IMAP, vous nôeffectuez plus une relève des messages, mais une synchronisation des messages (exactement comme pour les newsgroups, pour ceux qui les connaissent). Le logiciel vous affiche alors une copie de votre boîte aux lettres, archives comprises. Comme lôoriginal reste sur le serveur, vous pouvez avoir accès à votre courrier à partir de nõimporte quel ordinateur, n'importe où dans le monde.

De plus comme seuls les en-têtes des messages sont téléchargés dans un premier temps, lôaffichage de la liste des messages est souvent beaucoup plus rapide avec IMAP lorsquõil y a un grand nombre de (nouveaux) messages sur le serveur.

IMAP devrait progressivement remplacer POP.

Lequel choisir ?

Si vous utilisez votre compte de messagerie à titre personnel et que vous n'être pas très mobile, optez pour le protocole POP. Tous vos messages étant conservés sur votre ordinateur : pensez à faire des sauvegardes régulièrement.

Si vous utilisez votre compte de messagerie à titre professionnel ou si vous devez partager vos messages avec d'autres, optez plutôt pour le protocole IMAP. Dans la mesure où vos messages restent sur le serveur du fournisseur d'accès, vous pouvez partager de l'information avec d'autres et transmettre un historique de communication à un remplaçant.

En IMAP, attention à l'espace qui vous est alloué sur le serveur du fournisseur d'accès. Comme cet espace est limité, vous serez obligés dôeffacer de temps en temps les e-mails qui ne vous sont pas utiles. Une autre solution consiste à utiliser lôIMAP afin de profiter de ses nombreux avantages et de sauvegarder de temps en temps de vieux messages en local sur votre ordinateur.

Partage des messages avec d'autres membres d'une association.

Dans une association, on occupe une fonction "officielle" pendant un certain temps puis on passe la main à un remplaçant qui peut être intéressé par l'historique des messages publics échangés.

Avec une messagerie POP, ce partage sera quasiment impossible car il faudrait les exporter de son ordinateur avant de les renvoyer à son remplaçant... qui devra les importer sur sa propre messagerie.

Avec une messagerie IMAP, il suffira de partager les identifiants de connexion pour retrouver tous les messages en ligne.

Dans le cas où l'on travaille en équipe, le problème est le même. On partage ses identifiants avec les autres membres de l'équipe et, ainsi, chaque membre peut accéder aux messages sans craindre de les "vider" du serveur.

Bien choisir son adresse de messagerie publique.

Une adresse de messagerie publique ne doit pas contenir de nom et de prénom puisqu'elle doit pouvoir être transmise à une autre membre de l'association.

Elle doit évoquer la fonction occupée par le membre. Exemples pour l'ARA : ara.informatique@gmail.com, blogara.ardeche@gmail.com ou ara.bulletin@gmail.com.

Le risque d'exposition aux spams.

Quand une adresse de messagerie est affichée sur un site web (ou un blog) et assortie d'un lien de type "mailto:", elle peut faire l'objet de spams. Pour éviter de recevoir des mails indésirables sur son adresse privée, il y a deux solutions :

1. Utiliser systématiquement une adresse de messagerie publique.
2. Ne pas créer de lien de type "mailto:mon@adresse".

Sur les blogs de l'ARA, vous pouvez créer des liens sur des adresses de messagerie avec la fonction javascript "envoi_message()". Utilisez-la systématiquement à la place des "mailto".

Exemple sur la page "Pour nous joindre" du blog de la Haute-Savoie :

```
<p>Courriel : <a title="Cliquez ICI pour envoyer un courriel au responsable de la Haute-Savoie" href="javascript:envoi_message('haute-savoie@amis-st-jacques.org');">haute-savoie@amis-st-jacques.org</a></p>
```

Sur l'ensemble du site web de l'ARA, les liens de type "mailto" ont pratiquement disparu partout. Seules quelques vieilles pages peuvent encore en contenir...

Fin de l'article " Messages : à la recherche de la confidentialité."

L'utilisation de boutons dans vos articles et dans vos pages.



Un bouton présente mieux qu'un simple lien. L'accès à un objet lié via un bouton est plus efficace... et plus esthétique qu'un lien orthographié avec quelque chose du genre "Cliquez ICI".

Depuis avril 2014, tous les blogs ARA permettent de paramétrer des boutons puis de les insérer dans vos articles et dans vos pages.

Des boutons pour faire quoi dans les blogs ARA ?

Dans les blogs ARA, il faut toujours chercher à homogénéiser la présentation des articles et des pages sur l'ensemble du site web. En ce qui concerne l'appel d'une image, d'un fichier PDF ou d'une page liée, on ne disposait, jusqu'ici, que de liens plus ou moins visibles et plus ou moins harmonieux.

Faute de mieux, on retrouvait souvent des liens sur des textes genre "Cliquez ICI". Aujourd'hui, nous pouvons faire bien mieux que cela avec l'emploi de boutons.

En plus de leur aspect plus "professionnel", les boutons sont réutilisables dans plusieurs articles ou pages. Par exemple, vous pouvez créer un bouton libellé "Pour nous contacter" utilisable un peu partout dans votre blog.

Placer une URL dans chaque bouton .

Qui dit lien dit URL.

Dans chacun des boutons que nous allons créer dans nos blogs, on ne pourra placer qu'une URL statique (le bouton ne permet pas de changer d'URL en fonction du contexte).

Certes, l'URL associée au bouton est statique mais elle peut s'appuyer sur les fonctions javascript à votre disposition dans les blogs ARA. Citons, entre autres :

- `javascript:call_window('URL',hauteur en pixels,largeur en pixels)` avec, par exemple `javascript:call_window('http://haute-savoie.amis-st-jacques.org/?page_id=279',1020,760)`
- `javascript:envoi_message('adresse_messagerie')` avec, par exemple `javascript:envoi_message('ara.informatique@gmail.com')`

Paramétrage d'un bouton sur votre blog ARA.

http://webmaster.amis-st-jacques.org/wp-uploads/telechargements/mes_documents_pdf/METHODE_DETAILLEE_CREATION_ARTICLE.pdf .

Utilisation d'un bouton ou d'un lien texte ou image ?

Nous avons vu qu'un bouton pointe sur une URL et une seule. Ce paramètre URL n'est pas modifiable une fois le bouton inséré dans un article ou une page.

La conséquence est qu'il vous faudra autant de boutons que d'URL différentes. Or la gestion des boutons n'est pas évidente (pas de tri sur le nom "technique" du bouton).

Ma préconisation est donc d'utiliser des boutons pour pointer sur des liens utilisables partout (comme "*Pour nous joindre*", "*Nos permanences*", "*Besoins urgents d'hospitaliers*", "*Liste des sorties*" ou "*Ecrivez à la secrétaire*") :



Par contre, si vous utilisez des URL spécifiques sur un article ou une page (lien sur un document PDF ou sur un diaporama relatant une sortie ou un évènement isolé), il vaut mieux créer le lien sur un texte comme ci-dessous, par exemple :

- Récit de notre sortie sur le plateau de Beauregard.
- Diaporama regroupant les photos des participants

Textes utilisés pour des liens spécifiques à un article ou à une page.

Evitez impérativement les "Cliquez ICI" qui finissent par ne plus rien dire (un lien texte doit donner une indication un peu plus explicite).

Dernière possibilité pour un lien spécifiques : utilisez la (les) vignette(s) positionnée dans votre article.

Fin de l'article " L'utilisation de boutons dans vos articles et dans vos pages."

Comment optimiser l'utilisation de votre éditeur de texte.



Pour rédiger articles et pages dans vos blogs ARA, vous utilisez l'éditeur intégré.

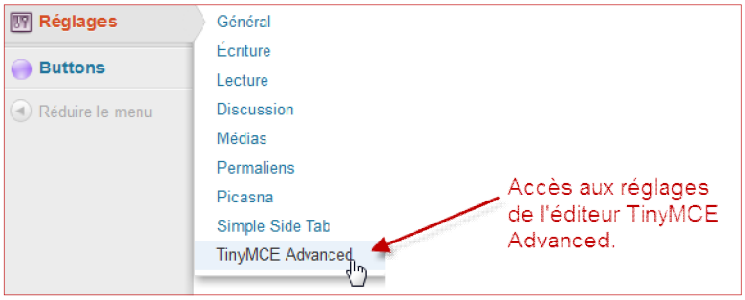
En fait, cet éditeur a été paramétré pour vous proposer un certain nombre de fonctions mais vous pouvez le personnaliser voire l'enrichir avec de nouvelles fonctions de mise en page.

L'éditeur de texte utilisé dans nos blogs ARA

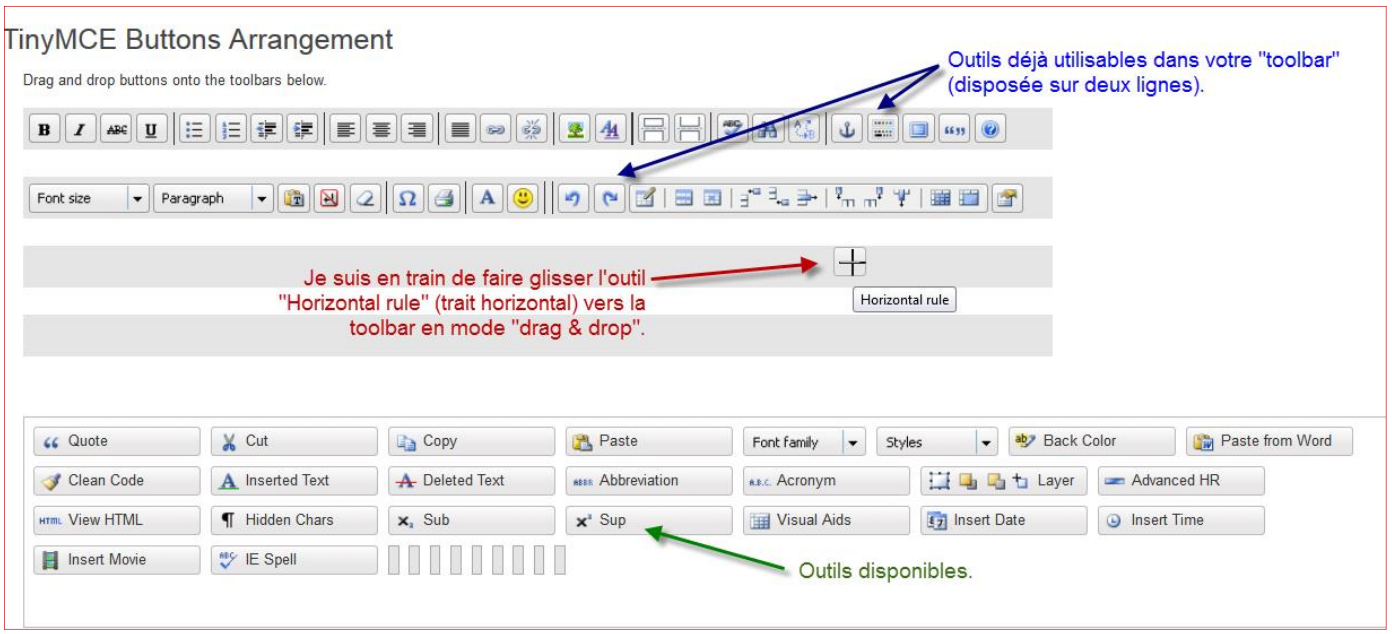
Dans tous les blogs ARA, nous utilisons les mêmes outils et les mêmes extensions.
Notre éditeur de texte répond au doux nom de "TinyMCE Advanced". Il fonctionne en Wysiwyg avec un onglet "Visuel" et un onglet "Texte". Cela signifie que, quand on positionne une image ou un paragraphe en mode "Visuel", on génère automatiquement du code dans la partie texte.
Le problème du Wysiwyg est qu'il est parfois approximatif en matière de mise en page (en particulier quand on modifie sa saisie à plusieurs reprises). Si l'on souhaite maîtriser *complètement* la présentation d'un article ou d'une page, on doit passer en mode "Texte" et travailler sur le code HTML.
Cependant, avec des outils adéquats dans son éditeur en mode visuel, on peut éviter d'en arriver à cette extrémité.

Les réglages de l'éditeur TinyMCE Advanced

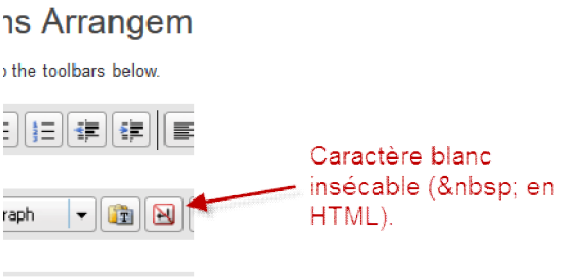
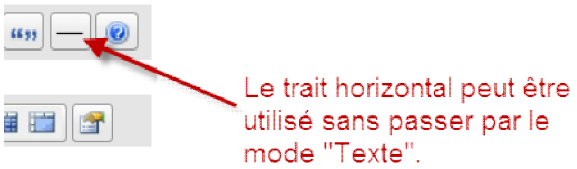
Si l'on souhaite rajouter des outils à la "barre d'outils" de notre éditeur, nous devons passer par les réglages de TinyMCE Advanced dans nos blogs respectifs.



Par "drag & drop", nous allons pouvoir ajouter, supprimer et ordonner les outils dont nous souhaitons disposer dans notre "barre d'outils" (toolbar). :



Des outils intéressants... ou non dans la barre d'outils de votre éditeur

Caractère blanc insécable :  	***Pourquoi :*** En HTML, les éléments ne contenant que des caractères blancs normaux sont considérés comme vides. Un paragraphe (ou une ligne) qui contient simplement un caractère "espace" aura une hauteur nulle. Par contre, un espace insécable est un type spécial de caractère espace qui n'est pas considérée comme négligeable par le HTML (bien que cela dépende du navigateur), de sorte qu'il peut être utilisé comme contenu pour un paragraphe non vide. ***Remarques :*** En mode visuel, vous pouvez insérer un certain nombre de caractères insécables où bon vous semble et enregistrer ou publier immédiatement votre article. Si vous souhaitez revenir plus tard sur votre article pour le modifier (ou si vous faites un clic sur l'onglet "Texte" puis sur l'onglet "Visuel", vous perdrez ces caractères insécables. La solution est de passer en mode "Texte" et de ne plus revenir en mode "Visuel" (à réserver à ceux qui connaissent un peu le HTML).
Le trait horizontal :  	***Pourquoi :*** Il peut être intéressant de tirer un trait horizontal dans un article ou une page de votre blog ne serait-ce que pour séparer un texte d'un groupe de liens ou de boutons : En HTML, le trait horizontal se note <HR> . Il peut être assorti d'attributs comme la longueur ou la couleur. ***Remarques :*** En mode visuel, vous pouvez insérer des traits horizontaux sans risque de les voir disparaître. Faites simplement attention à l'endroit où vous les placez. Si vous vous trompez, le plus simple est de faire immédiatement un <CTRL + Z> qui annule l'opération précédente.
~~*Les fonctions d'édition :*~~  	***Pourquoi :*** Les fonctions d'édition (couper, copier, coller) sont disponibles mais elles risquent de surcharger votre toolbar pour rien si vous avez l'habitude des appuis-touche. ***Remarques :*** Faites <CTRL +X> pour couper , <CTRL +C> pour copier et <CTRL + V> pour coller ce que vous avez copié ou que vous avez coupé. Cela vous évitera d'afficher ces fonctions dans votre toolbar.

Pour conclure avec l'utilisation de l'éditeur TinyMCE Advanced

Travailler avec un éditeur Wysiwyg comme TinyMCE Advanced peut être frustrant quand on souhaite rajouter des caractères blancs dans une ligne ou rajouter des lignes blanches.
En dehors du fait d'utiliser l'éditeur Wysiwyg, on est également contraints par le "Thème" utilisé sur votre blog. Ce thème impose des couleurs et des présentations que vous ne pouvez forcer qu'à grand' peine.
Pour l'insertion d'espaces et de lignes "blanches", l'utilisation de caractères insécables est une solution "one shot" : c'est à dire que cela va fonctionner si on sauvegarde ou si l'on publie tout de suite. Malheureusement, à la reprise de notre article, on aura perdu ces caractères insécables et on aura perdu également les lignes "blanches" (retour à la ligne + caractère insécable).
Vérifiez fréquemment votre travail en effectuant des "aperçus".

Enfin, si vous souhaitez obtenir une présentation de qualité et maîtriser cette présentation, vous devrez passer en mode "Texte", travailler sur le code HTML et NE JAMAIS REVENIR EN MODE "VISUEL" sur un article ou une page !

Voilà, ce huitième numéro de la "lettre aux bloggers" s'achève ici.
J'espère qu'il vous aura apporté quelques éclaircissements sur votre activité de "blogmaster de l'ARA".

Pour le prochain numéro, vous pouvez me proposer de nouveaux sujets en écrivant à web@amis-st-jacques.org

A bientôt sur les blogs de l'ARA.