

L'art du spam

By Source-La & TRH

Introduction

- 1. Cet e-book est à but éducatif, je ne serais en aucun cas responsable si quelqu'un venais à l'utiliser à des fins malsaines.*
- 2. La revente de toute information et le phishing sont sévèrement punissables par la loi.*
- 3. La revente de cette e-book est totalement interdite, il est entièrement gratuit.*
- 4. Cet e-book a été rédigé par Source-La & TRH.*
- 5. Pour toutes question, vous aurez quelques moyens pour me contacter à la fin de l'e-book.*

L'objectif de l'ebook

Mon objectif avec cet e-book est de vous apprendre à savoir mettre en place un site de phishing et un spam.

Toutes les informations pour monter un site de phishing sont incluses par la suite.

Sommaire

*Qu'est ce que le phishing -/-
l'hameçonnage/spam ?*

L'SMTP

L'hébergement

La Letter

Les Mail-List

Mailer

Qu'est ce que le phishing/spam ?

Le Phishing -/- L'hameçonnage

Le phishing est utilisé depuis la nuit des temps sur internet.

Celui-ci est basé sur l'usurpation d'un site généralement connu du destinataire.

Une des méthodes de phishing la plus répandue est celle du Fake Paypal ; on peut également citer le phishing bancaire et celui concernant les GAFAM (Apple, Google, Facebook ,Microsoft ,Amazon)

Il permet entre autre de récupérer des informations sur la victime mais plus particulièrement des données bancaire pour les utiliser à des fins frauduleuses.

Généralement le phishing va se baser sur un événement inhabituel pour susciter une réaction de panique chez la victime.

Le spam

Le spam comme son nom l'indique consiste à envoyer à grande échelle des mails.

L'objet du mail contient généralement un problème de compte, une offre alléchante ; un message poussant le destinataire à cliquer sur le mail.

Mais alors comment la victime, rentre-t-elle ses coordonnées bancaires ? Grâce à l'usurpation d'un site qui lui fera croire que c'est le site officiel (alors que ça ne l'est pas) .

On l'utilise également pour arnaquer « scam », (grosse somme d'argent , tirage au sort etc).

Nous nous focaliseront uniquement sur l'usurpation de site de grandes sociétés car c'est plus facile à effectuer et c'est plus rentable.

L'hébergement

L'hébergement

Ce système nous permettra d'héberger notre site de phishing pour pouvoir par la suite l'envoyer avec le spam.

Il y a plusieurs type d'hébergement.

1. Vous pouvez utiliser un VPS (virtual private server) pour pouvoir mettre votre scam dessus (Nous aborderons pas cela, mais vous pouvez chercher de votre côté si vous le souhaitez) .

2.Vous pouvez utiliser aussi un service d'host (nous verrons cela par la suite) .

3.Si vous êtes forts en informatique , vous pouvez utiliser un site shell (Je n'utilise pas ça mais c'est très utilisé, je peux éventuellement vous conseiller un vendeur de confiance.)

L'hébergement Service d'host

L'hébergement (Service d'host)

Nous allons voir dans cette partie là comment mettre en place un host.

Les configurer pour qu'ils soient prêt à être utilisés et faire en sorte qu'ils tiennent un maximum de temps.

Nous allons utiliser le site « Godaddy », il offre un service d'hébergement ainsi que des noms de domaine.

Je l'ai utilisé pendant pas mal de temps, si vous faites attention vous devriez le faire sauter (RedFlag) en une semaine.

L'installation ne prends pas beaucoup de temps. (Au début vous aurez peut être un peu de mal mais avec le temps ça viendra tout seul)

L'hébergement (Service d'host)

Pour commencez nous allons nous rentre sur le site.

Dirigez vous vers Domaine -> Rechercher un nom de domaine vous allez pouvoir choisir un nom de domaine.

Ici je vous conseille vivement de prendre quelque chose qui attire l'attention de la victime sans pour autant l'alarmer comme «verifcationclients.com» .

Une fois que vous avez sélectionné votre NDD, profitez-en pour prendre un « Hébergement Web Linux » (Il vous seras proposé quand vous cliquerez sur « Voir mon panier » ,désactivez tout le reste.

Vous pouvez le card, mais je vous conseille si vous le pouvez de mettre les informations de la personne avec la carte de crédit que vous allez utiliser , cela augmente grandement la durée de vie de l'host

PS: Faites attention , Godaddy va vouloir vous faire payer une somme assez importante , vérifiez bien la durée de chaque article et prenez le plus bas.

verifcationclients.com
Enregistrement de domaine .COM 18,99 €
50 % de réduction

2 Années
Renouvellement pour 22,96 €/an

170 000 fois par an. C'est la fréquence à laquelle les criminels tentent de voler des domaines. Protégez votre domaine. @

Confidentialité et protection de domaine complètes 8,39 €/an par domaine 16,79 € Ajouter

Hébergement Linux Économie avec cPanel 32,88 €
12 Mois
Renouvellement pour 8,99 €/mois

Voir les avertissements relatifs à la condition des offres

Vider mon panier

Sous-total 51,87 €
Impôts et taxes 10,71 €

Vous disposez d'un code promotionnel ?

Total (EUR) 62,58 €

← Menu principal

Domaines

Un site Web doit avoir un nom de domaine. À l'instar d'une adresse postale qui indique l'endroit où vous vivez, un domaine permet aux clients d'accéder directement à votre site Web. Nous pouvons vous aider à en trouver un que vous aimez. [Plus de détails...](#)

TROUVER UN DOMAINE

Recherche de nom de domaine

Nous recommandons fortement la Confidentialité et la protection de domaine complètes mais cela est une fonctionnalité optionnelle.

Sélectionner un plan

☐ Confidentialité et protection de domaine complètes 8,39 €/domaine par an 16,79 €
[Voir les détails](#)

☐ Protection et sécurité de domaine Ultimate 13,19 €/domaine par an 26,38 €
[Voir les détails](#)

☒ Non merci

☐ Démarrez votre site Web GRATUITEMENT.
Créez un meilleur site Web en moins d'une heure, afin que les gens visitent votre domaine avant plus qu'une page « en construction ».

Hébergement Web Linux
Installation en un clic de WordPress, Drupal, Joomla et bien d'autres encore. Un hébergement cPanel® fiable pour les sites Web complets.
Domaine gratuit inclus* avec achat.
Pour seulement 3,29 €/mois
Économie - 3,29 €/mois

Créez une adresse e-mail qui correspond à votre nom de domaine.
Ayez une allure professionnelle et inspirez la confiance avec une adresse e-mail personnalisée comme You@verifcationclients.com
Pour seulement 2,99 €/mois
Non merci

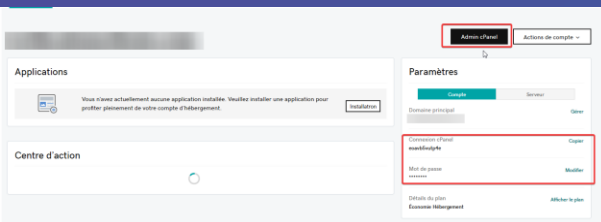
L'hébergement (Service d'host)

*Une fois cela fait, il ne vous reste plus qu'à le configurer
(Valider le compte avec un email valable il se peut que le
mail de confirmation prenne un peu de temps à venir
,soyez patient)*

*Godaddy propose directement d'utiliser le nom de
domaine sur le host ce qui fait gagner pas mal de temps
vis-à-vis des redirections .*

*Quand l'installation sera terminée vous devrez installer
un certificat SSL car sinon si la victime est sur Iphone par
exemple elle va voir « Site non sécurisé » .*

*Pour cela nous allons utiliser le site « SslForFree » ,
pensez à modifier le mot de passe de votre FTP sur
l'espace Godaddy (Si ça ne fonctionne pas , créez un accès
sur le Cpanel)*

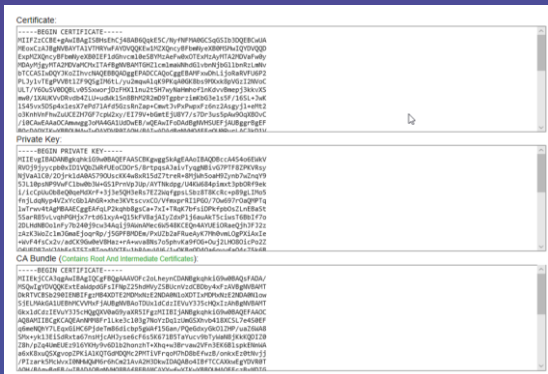


L'hébergement (Service d'host)

Quand vous aurez terminé de régler l'host et après avoir récupéré les accès FTP, il faudra s'occuper d'installer le SSL. Pour cela allez sur « SslForFree », mettez votre nom de domaine (Attention car le site est bug du coup il va mettre en double votre host ,modifiez l'url pour que la requête soit faite uniquement pour votre domaine)

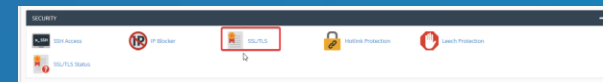


Choisissez ensuite « Automatic FTP Verification » insérez vos login FTP, il va ensuite vérifier que l'host vous appartient bien.



La vérification du site finie, vous aurez 3 cases « Certificate » « Private Key » « CA Bundle » nous allons nous en servir pour installer le SSL sur le Cpanel.

Rendez vous sur le Cpanel de votre host dans la section SSL et dans « Install and Manage SSL for your site (HTTPS) » ensuite vous mettez ce que vous avez récupéré sur SslForFree dans les cases correspondantes ainsi que « Install Certificate ».



L'hébergement (Service d'host)

L'installation du SSL terminée, il ne vous reste plus qu'à mettre votre scamma.

Vous devrez vous rendre sur votre serveur avec un logiciel adéquat (J'utilise Filezilla mais vous pouvez également utiliser le FTP directement sur le Cpanel)

Une fois dessus rendez-vous sur « Public_HTML » vous aurez juste à déposer le dossier de votre scamma.

Une fois cela fait, votre page de phishing sera prête , vous pouvez maintenant l'utiliser pour votre spam.

Attention car si votre scamma est détecté , votre page se fera instant red donc votre site sera inutilisable cela viens des antibots ou du code détecté généralement.



Les Leads/Mail-List

Les Leads/Mail-List

Qu'est ce que sont des « leads/mail-list » ?

Les leads/mail-list sont une liste de mails , celles que vous cibleriez pour votre spam .La qualité dépendra généralement de si les personnes on déjà été victime de phishing. (Les personne qui n'ont jamais été victime de spam seront plus facilement attirable vers votre mail de phishing) .

Évitez aussi les mail-list publiques car elle sont passées autant de fois que Discord sur Kulture.

Je vais vous montrer les différents moyens de vous procuré vos mail-list.

1. Acheter vos mail-list

2. Faire du dump de DB de site. (Je vais vous redirigez vers une vidéo pour cela mais l'e-book cracking que j'ai fait sur Lilith sera disponible , j'y explique comment faire avec un peu plus en détails) .

Les Leads/Mail-List

Je vais vous montrer où acheter vos mail-list et vous donner quelque conseils pour éviter de prendre de la mauvaise qualité.

Le prix des mail-list dépendras de la quantité de mail qu'elle contiendra.

Mais attentions la plus grosse erreur que vous pourrez faire est d'acheter une mail list de 300 000 mail à 40€ par exemple mais la moitié peut être déjà spam car publique.

Vous avez différents sites pour vous procurer cela.

[Xleet.to](#)

[Olux.to](#)

Je n'ai pas spécialement de préférence, il existe d'autre sites , si vous cherchez un peu vous pourrez trouver assez facilement.

Les Leads/Mail-List

Je prendrais pour exemple le site Xleet mais le principe est le même sur les autres sites, je vous déconseille fortement d'acheter des Smtip/Host, la qualité de ce que les gens revendent est vraiment douteuse. (Pareil pour Olux, vous pouvez quand même essayer pour vous faire votre propre avis)

Pour commencer allez sur le site, créez votre compte et ensuite allez dans la catégorie « Leads → Email Only »

Vous pourrez trouver tout type de mails, de tout pays.

Modifiez les critères pour n'avoir que des mails Français

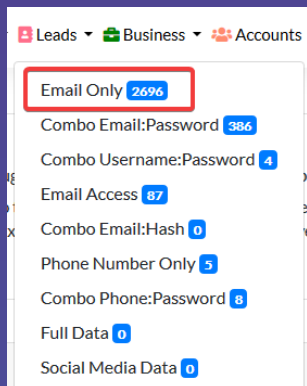
Maintenant, vous devrez prendre l'offre la plus avantageuse, évitez néanmoins les trop grosses mail lists.

Regardez aussi les « proof » qu'ils proposent, ça permet de regarder un peu à quoi ressemblent les mails et de vous faire un avis sur la qualité.

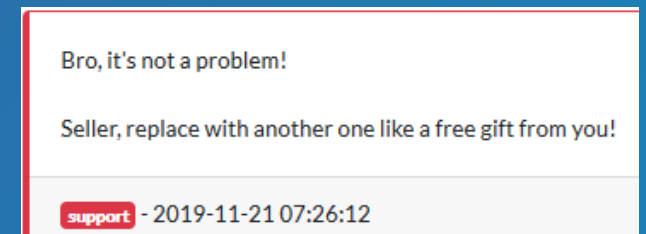
Une fois que vous avez choisi votre mail-list achetez-la.

Petit Bonus : Vous pouvez essayer de la faire refund, pour soit être remboursé, soit en avoir une seconde pour le prix d'une. Les sites remboursent assez facilement.

Ensuite je vous conseille de cliquer sur « Date Created » Cela permettra de voir ce qui a été posté récemment, ensuite regardez dans « Provider » pour voir les domaines concernés (Orange, Yahoo..ect).



Description:	Provider:	type:	Country:	Seller:	
<input type="text"/>	<input type="text"/>	Email Only	<input type="text" value="French Republic"/>	Select Seller	<input type="button" value="Filter"/>



L'SMTP

L'SMTP

Un SMTP est un serveur d'envoi de mail « **Simple Mail Transfer Protocol** »

Vous en aurez besoin pour pouvoir envoyer vos mail contenant la letter pour ensuite les rediriger vers votre site de phishing.

Vous avez de multiples possibilités pour vous en procurer, j'ai utilisé **Sendgrid** pendant des mois avant de passer à autre chose.

Dans cette partie je vais vous montrer comment vous procurer des « Old Log » pour pouvoir les utiliser par la suite.

Vous pouvez aussi essayer d'autre service/tech comme crack directement le SMTP de Shell... une tonne de possibilité s'ouvre à vous mais on ne s'attardera pas là dessus.

L'SMTP

Pour pouvoir cracker des Sendgrid, on va faire du checking avec Openbullet (La config seras fournie dans le dossier.)

Cracker des Old Log permettra de soit les card si le compte est gratuit ou de les utiliser si le compte est payant, ils ne sauteront pas d'un coup contrairement à des logs récents. (N'essayez pas de créer un compte, je vous garantis que c'est une perte de temps car il sautera dès l'instant où vous lancerez un spam)

Il se peut que des logs Sendgrid n'inbox pas certains domaines donc ne cherchez pas à forcer .Faites des tests simples ,cela permet de vérifier efficacement.

Si vous cardez le log en question, faites le avec une CC qui est live et pas dead car il se peut qu'ils la prennent mais que le SMTP saute au bout de ~100 mails.

L'SMTP

Je vais vous montrer comment cracker des Sendgrid, ma config seras donnée, elle est modifiée pour qu'elle bannisse les comptes désactivés donc tout les hit seront actifs et les hits « Custom » indiqueront que le compte est désactivé.

Openbullet sera fournis avec l'e-book (Si vous ne savez pas l'utiliser vous pouvez cliquer sur [cette vidéo](#)).

Une fois que vous aurez hit un log, connectez vous a celui-ci, je vais vous donner quelque petites astuces pour bien l'utiliser.

Surtout, ne modifiez jamais les login du compte car le propriétaire du compte risque de le voir et de changer le mot de passe et vous perdrez le compte pour de bon. (Il reçoit une notif mail pour les changements de mot de passe mais pas pour le reste)

L'SMTP

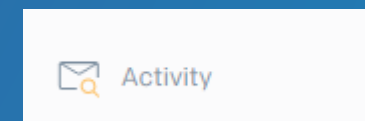
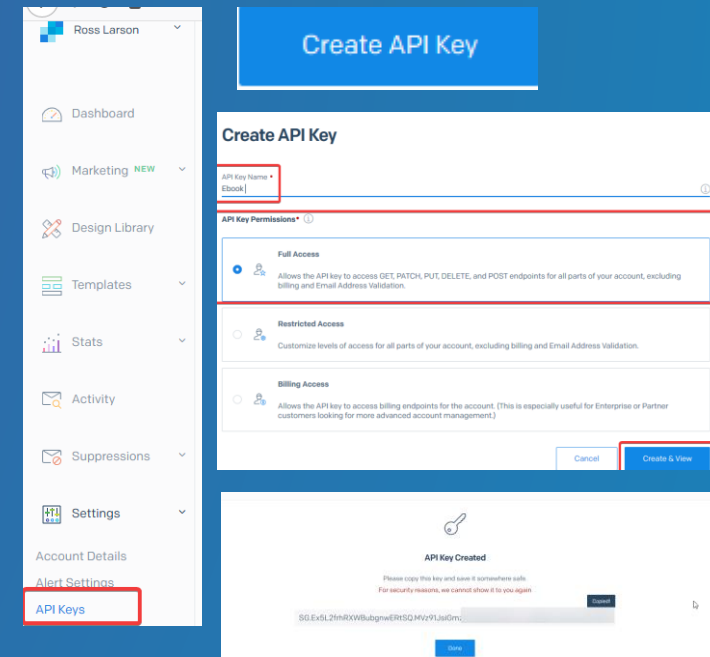
Une fois connecté au compte, vous pourrez vérifier si le compte est de type « paid », l'abonnement qu'il contient, s'il est gratuit de le carder par la suite.

Créez une Apikey dans la partie dédiée à cela -> Gardez la key Apikey vous en aurez besoin.

Vérifier si il inbox votre domaine (Faites un test sans letter ,mettez un sujet bidon et une connerie genre coucou ça va) si celui-ci inbox essayez avec votre letter , si ça passe vous pouvez le card.

Il y a une fonctionnalité qui permet de voir si le mail est bounce ou pas ,de voir si la personne a ouvert le mail et cliqué sur le lien ; allez sur Activity pour voir cela.

Quand vous cardez celui-ci , ne prenez pas l'offre a 100 000 ,prenez en premier 40 000 mails , si le smtp fonctionne toujours après 35k mail montez a 100k..ect.



La Letter

La letter

La letter sera le contenu de votre mail, le but d'une letter de type phishing est de faire peur à la personne pour la faire cliquer sur votre lien de phishing.

Les letter doivent être faites correctement , dans le cas contraire les domaines les détectent comme du spam, elles n'iront donc pas dans les mails prioritaires.

Vous pouvez les faire vous-même si vous avez des connaissances en HTML + CSS.

Quand les letter sont détectées essayez de regarder en premier le bouton menant à votre site ainsi que les images (Vous les retirez et vous effectuez des tests pour voir ce qui est flag) si ça ne vient pas de là ,ça peut également venir de votre smtp.

Enfin ,effectuez pas mal de tests avant de conclure quelque chose.

Je mettrais quelques lettres dans le pack pour que vous puissiez vous faire une idée .

La letter

Pour une rédaction clean et éviter le spam je vais vous donner quelque conseils.

Il faut savoir que les messageries utilisent un système de « spam score », plus votre score est haut plus les chances que votre mail aille dans les spam est élevé.

1. Eviter les liens flag : Si votre nom de domaine contient un mot « blacklist » vous irez probablement en spam , privilégiez un site qui propose de raccourcir votre lien.

2. Faites attention à la taille de votre image : Si vous télécharger le logo d'un site ou même d'une autre letter « officielle » modifiez la taille avec un logiciel car ce n'est pas en modifiant juste la taille avec la poignée que ça modifiera la taille réelle et les anti-spam vérifient beaucoup cela.

3. Évitez des mots/terme utilisés par le spammeur : Si vous utilisez des mots comme « Formulaire » ou même des mots en majuscule ,cela augmente les chances que votre letter aille dans les spam.

Il y a aussi quelque petits trucs à savoir sur l'identification de l'expéditeur du mail (Vous) .

La blacklist : Les listes noirs contiennent toute les ip flag ,cela vous fera partir instantanément en spam.

La Signature DKIM : DKIM veut dire « Domain Keys Identified Mail » il s'agit d'un système d'authentification qui permet de savoir si le message viens d'un système autorisé.

Les règle SPF : SPF veut dire « Sender Policy Framework » Elle ressemble un peu a la signature DKIM, cela permet d'identifier l'expéditeur (Ça évite de pouvoir envoyer un mail à votre nom).

La Mailer

Le Mailer

Le mailer est un logiciel/script permettant d'envoyer des mails en masse.

Le mailer le plus connu est « Ultramailer » il est très simple à prendre en main, l'interface est fluide.

Je vais vous montrer comment il fonctionne et comment le configurer .

Le logiciel est fournis dans le pack avec la clé d'activation.

Pour ceux qui est des scripts , nous n'allons pas nous intéresser à cela mais vous pouvez tout de même vous informer si vous le souhaitez ; généralement les script sont sous forme de PHP Mailer.

Le Mailer

*Après avoir installé Ultramailer, activez le logiciel ,
sinon vous aurez un problème de limitation.*

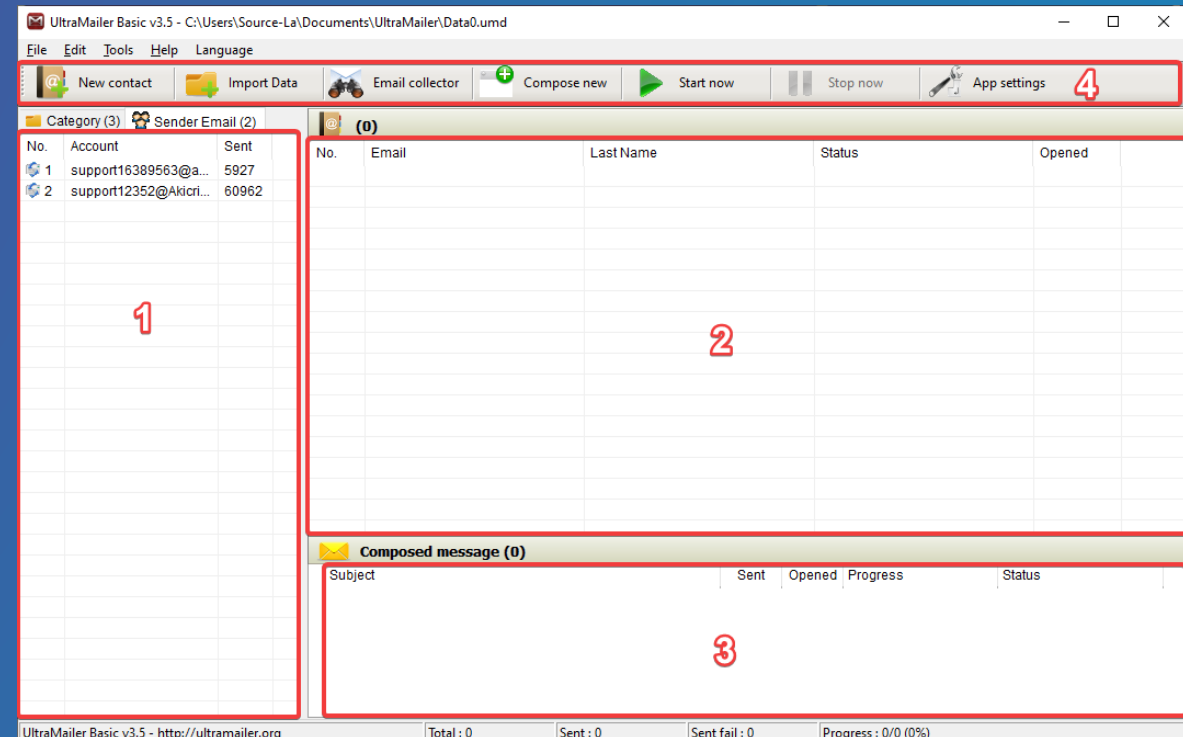
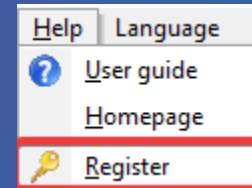
On va faire un petit tour rapide du logiciel.

*1. Vous pouvez mettre vos serveur SMTP, les catégories
permettent de mettre différentes listes de mail.*

2. La liste de mail sera à mettre ici.

*3. Composed Message, c'est ici qu'on réglera les mails
qu'on va envoyer (La letter, le sujet du mail) .*

*4. Start Now et Stop Now pour pouvoir lancer/stop le
spam, App Setting pour régler la fréquence ainsi que
d'autres petits réglages, Import Data pour importer
votre mail-list, Compose New pour créer un nouveau
mail.*



Le Mailer

Pour mettre un SMTP sur votre Ultramailer, il suffit d'aller dans « Sender Mail », de faire un clic droit sur la zone blanche et New Sender.

Ici vous allez pouvoir mettre vos options pour votre SMTP.

Sur le screen que j'ai mis vous aurez la config pour Sendgrid mais le principe est le même pour tout autre SMTP.

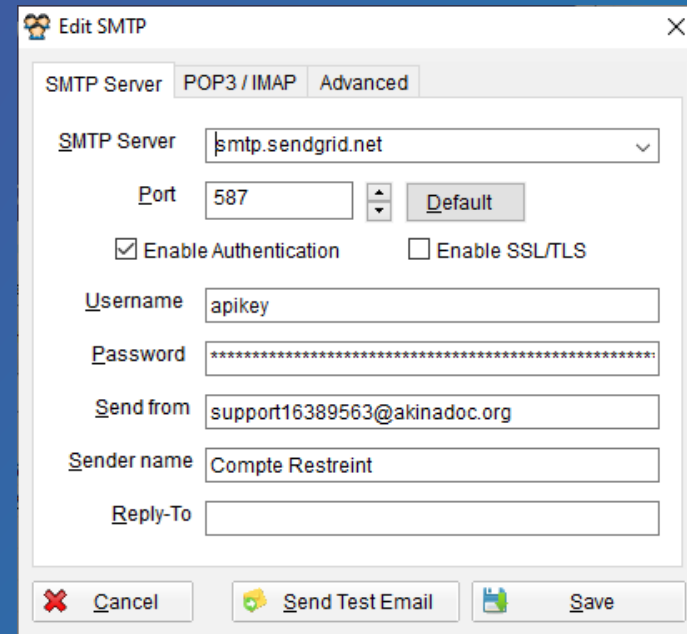
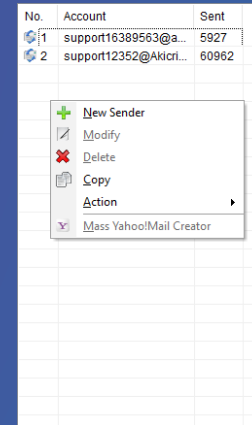
Pour ce qui est du Sender Name, n'hésitez pas à le changer si ça n'inbox pas ou autre.

Send From, je modifie seulement les chiffres.

Username pour Sendgrid « Apikey »

Password dans la partie SMTP, la grande ligne quand vous créez une apikey est le password.

Pour le port vous pouvez essayer 25,465,587.



Le Mailer

Maintenant, il faut mettre en place la contenu du mail.

Pour cela cliquez sur « Compose New », une fenêtre s'ouvre.

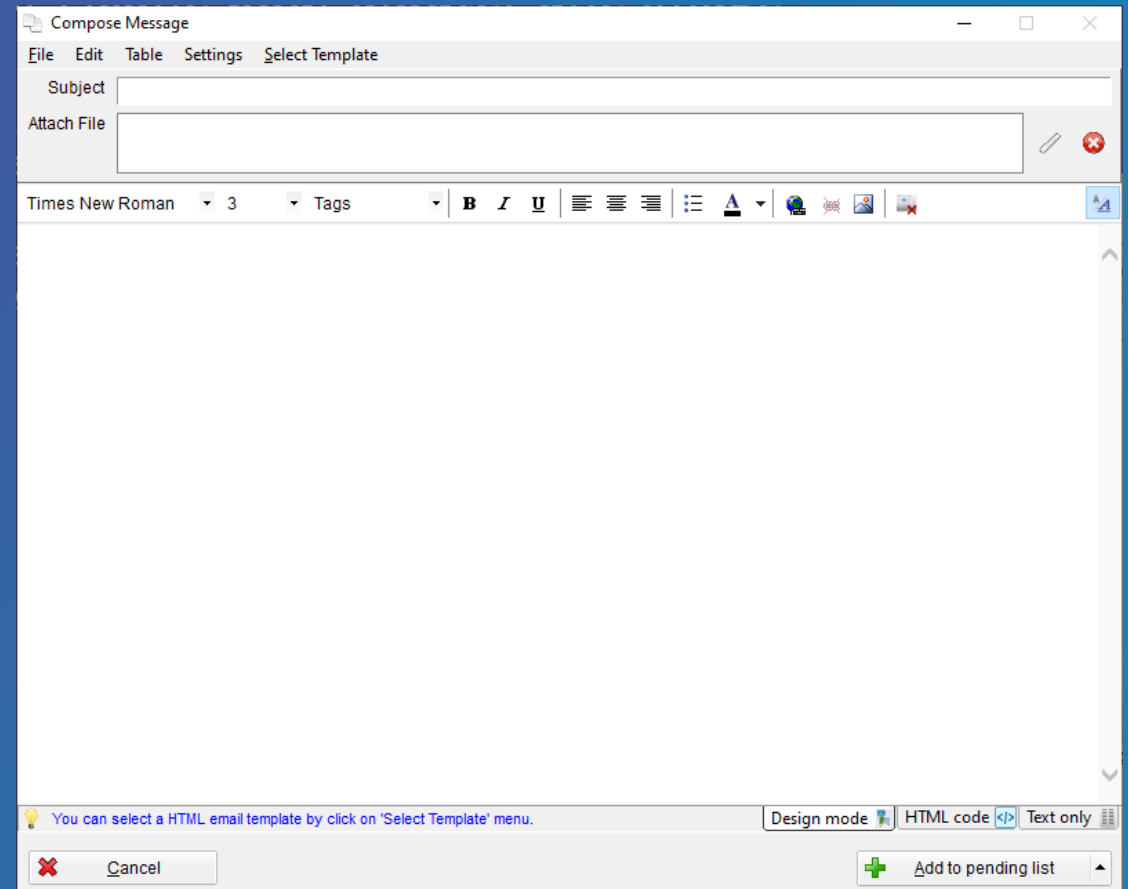
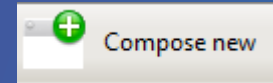
Dans le subject on mettra le sujet de notre mail. (Ce qui apparaît au milieu , pas à gauche sur la messagerie)

Attach File , n'y touchez pas , on ne souhaite pas envoyer de fichier.

En bas a droite vous pouvez voir Design Mode , quand le code HTML seras mis vous aurez votre letter d'affiché .

HTML Code, vous mettrez le code de votre letter ici.

Text Only on y toucheras pas.



Le Mailer

Il reste juste à régler les paramètres d'envoi de mail, cliquez sur App Settings

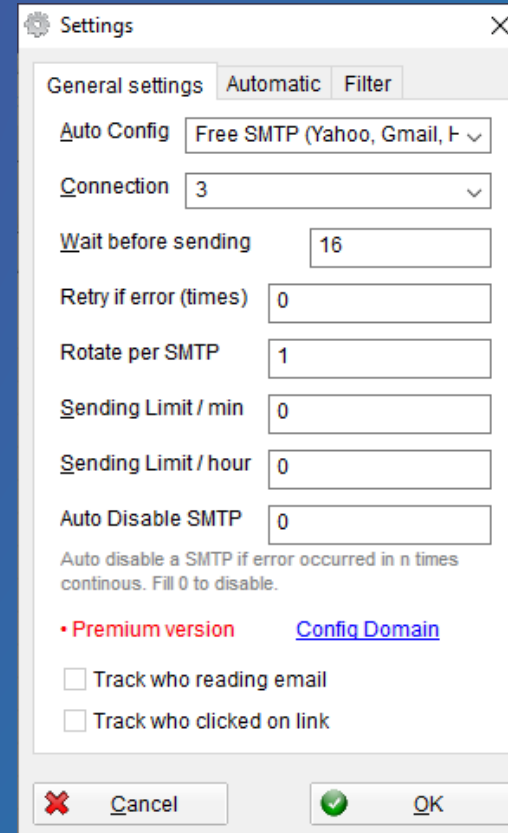
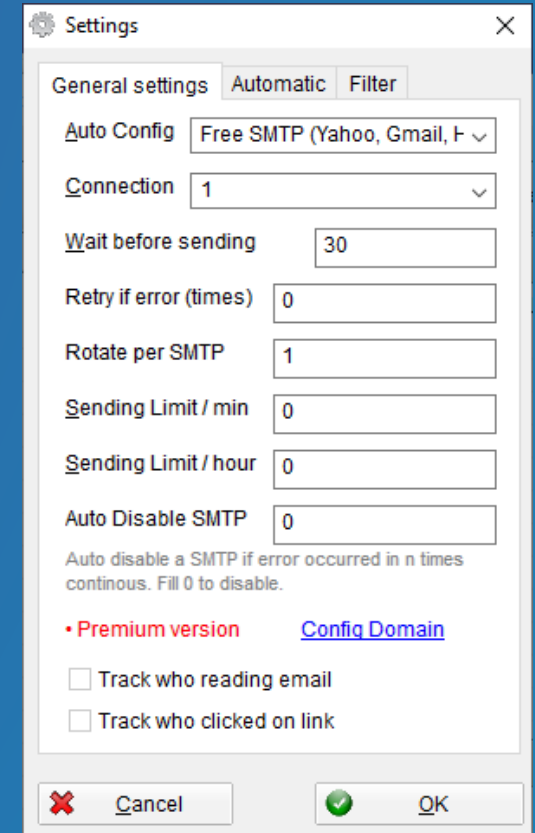


Si vous lancez un spam sans délai vous allez faire sauter votre SMTP car la messagerie va recevoir beaucoup de mail arrivant du même SMTP et de la même IP et donc refuser le mail (Bounces) et faire sauter le SMTP au passage.

Il est conseillé avec un SMTP fresh de n'avoir qu'un seul mail à la fois , « Connection » , 30 sec de délai et « Wait Before Sending » .

Ça sera long mais vous serez sûr de ne pas le faire sauter (S'il saute au bout du 120e mail environs c'est que la CC avec lequel vous l'avez card était DD)

Si vous avez un SMTP qui a au minimum 10K mails envoyés et qu'il fonctionne toujours , vous pouvez mettre 3 connexions et 16 de delay comme sur le screen.

A screenshot of the "Settings" window. The "General settings" tab is selected. The "Auto Config" dropdown is set to "Free SMTP (Yahoo, Gmail, F...". The "Connection" dropdown is set to "3". The "Wait before sending" input field contains "16". The "Retry if error (times)" input field contains "0". The "Rotate per SMTP" input field contains "1". The "Sending Limit / min" input field contains "0". The "Sending Limit / hour" input field contains "0". The "Auto Disable SMTP" input field contains "0". Below these fields, there is a note: "Auto disable a SMTP if error occurred in n times continuous. Fill 0 to disable." There are two checkboxes: "Track who reading email" and "Track who clicked on link", both of which are unchecked. At the bottom, there are "Cancel" and "OK" buttons.A screenshot of the "Settings" window. The "General settings" tab is selected. The "Auto Config" dropdown is set to "Free SMTP (Yahoo, Gmail, F...". The "Connection" dropdown is set to "1". The "Wait before sending" input field contains "30". The "Retry if error (times)" input field contains "0". The "Rotate per SMTP" input field contains "1". The "Sending Limit / min" input field contains "0". The "Sending Limit / hour" input field contains "0". The "Auto Disable SMTP" input field contains "0". Below these fields, there is a note: "Auto disable a SMTP if error occurred in n times continuous. Fill 0 to disable." There are two checkboxes: "Track who reading email" and "Track who clicked on link", both of which are unchecked. At the bottom, there are "Cancel" and "OK" buttons.

Conclusion

Merci d'avoir lu cette E-book !

Je vous remercie d'avoir suivi jusqu'au bout.

Pour toute question vous pouvez me DM sur Discord (Je donne pas mon tag car je saute assez souvent, mais vous pouvez me retrouver sur les serveurs communautaires)

Je souhaite remercier ceux qui m'ont aidé pour l'écriture de cette e-book.

Remerciements spéciaux à Fantarte pour c'est précieux conseils et à Yoob pour la mise en page .

Maintenant vous avez toute les carte en main pour être un Pro-Spammer.

#FreePh4nT0M