

Activité - Lanceur.euse.s d'alertes et journalistes

TOUTES LES FICHES

par Nothing 2hide



Description

Grâce à cette activité, les participant.e.s pourront comprendre les enjeux autour de la confidentialité des données, donner des pistes d'outils pour protéger ses échanges, comprendre les potentiels points d'interception, comprendre la différence entre anonymat et chiffrement, comprendre la notion de lanceur d'alerte.

Objectifs

- Enjeux de confidentialité des données
- Outils et méthodes pour protéger ses échanges
- Différencier anonymat et chiffrement
- Sensibilisation sur le rôle des lanceur.euse.s d'alertes

Compétences travaillées

Création de mail
Connaissance de service web renforçant l'anonymat et la sécurisation des données

Pré-requis

Avoir participé ou lu les fiches activités Signal, "un chemin Tortueux", Communiquer par mail... de manière chiffrée (Protonmail), et metadata

Matériel

deux salles ou deux espaces séparés
tables chaises
ordinateurs
connexion Internet
clé USB
retroproj

Contenus utilisés

NA

WORKFLOW

1 Mise en situation (chouette du roleplay!!)

- l'animateur.ice divise en plusieurs groupes les participant.e.s. L'idéal étant par binôme, 2 lanceur.euse.s d'alerte et 2 journalistes forme un groupe de travail.
- L'a... ux lanceur.euse.s d'a...

Isolez le q



t expliquez-leur la



situation :

Vous travaillez dans une grosse entreprise spécialisée dans les énergies fossiles (EnerFoss). Vous avez eu connaissance d'une information capitale : votre entreprise n'est pas aussi respectueuse de l'environnement qu'elle le prétend et elle exploite des concessions minières en Asie du sud est de manière illégale. Par ailleurs les conditions de travail sont inacceptables. Vous avez en main un document qui permet de prouver tout ça.

Vous décidez de tout transmettre à la presse pour que le scandale sorte tout en protégeant votre identité pour ne pas que votre employeur.euse ne vous poursuive.

Vous remettez le mail public des journalistes de leur groupe de travail, premier

contact. un simple mail pour se faire connaître et détenir des informations susceptibles d'intéresser le journaliste. **Et seulement après** vous leur remettrez la clé USB qui contiendra le fichier sensible des lanceurs d'alerte. Pour le fichier, choisissez ce que vous voulez en fonction du contexte, une image, ou sinon nous vous proposons un fichier bourré de méta données contenant des infos hyper sensibles : la [recette du gloubi bouлга](#) au format PDF.

Rejoignez **le groupe de journalistes**, et dites leur : "regardez vos e-mails".

Une fois qu'ielles ont tou.te.s pris connaissance du mail, demandez leur qu'est-ce qu'ils feraient dans l'instant ? 1 réponse par groupe.

La bonne réponse est, si toutefois si le mail est jugé sérieux, de regarder l'adresse mail qui envoie, il serait catastrophique pour la sécurité et l'anonymat que le.a lanceur.euse d'alerte utilise son mail professionnel (toto@enerfoss.com) par exemple, en effet, toutes les boîtes ayant des activités économiquement fortes surveillent tous les mails entrants et sortants.

Ceci dit, il faut maintenant que le.a journaliste confirme la prise de contact en répondant et assure la sécurité des communications et des potentiels fichiers qui seront échangés ! Vaste programme !!!

L'idée est de proposer un éventail d'outils qu'ils pourront utiliser comme bon leur semble, comme des briques à empiler pour arriver à un cheminement qui réduira les possibilités d'identifier la source. Avec ce qui suit, ielles pourront s'en donner à cœur de joie et même trouver voir inventer une méthode nouvelle ! À vous de choisir pour la présentation des outils, soit en début de jeu, soit pendant le jeu, en mode pédagogie inversée.

2

Déroulé

Les deux groupes ont **une heure** pour envoyer et recevoir le document de la manière la plus sécurisée possible. Demandez aux participant.e.s de noter les étapes de de leur processus sur une feuille afin de faire un petit compte rendu conjoint avec les lanceur.euse.s d'alerte une fois l'heure passé, les problèmes rencontrés, les failles possibles, les risques, .. un debriefing de salle de rédac. en somme.

1. Après la présentation des outils et la mise en situation qui dure une petite demi heure, – si vous avez choisi de les présenter en amont –
2. Donnez une heure aux équipes de lanceur d'alerte et de journaliste pour s'échanger le fichier sensible
3. Gardez une demi heure pour débriefer avec tout le monde. Chaque groupe désigne un.e rapporteur.euse, un pour les lanceur.euse.s d'alerte et un pour les journalistes, qui viendront expliquer comment ils se sont échangés le document. Si vous utilisez le document de la recette du gloubi-bouлга bourré de méta données (jetez-y un œil !) vérifiez bien que les journalistes les ont

nettoyées.

Astuce qui marche bien :

Demandez à chaque groupe de journalistes et lanceur.euse.s d'alerte de se trouver un nom. Quelques exemples de noms pertinents pour l'atelier :

- les Wikileaks
- les Luxleaks
- Les évadés du fisc
- les Edward Snowden
- etc.

3

Annexe : les outils utiles pour cet atelier

Cet atelier fait appel à quelques outils technique en ligne simple d'utilisation. Vous pouvez les présenter soit en amont de la mise en situation,

- [Utilisez des Emails jetables](#)
- [Mission impossible staïle : envoyer des notes qui s'autodétruisent](#)
- [Transmettez des fichiers chiffrés en drag & drop avec send.firefox.com](#)
- [Attention aux metadonnées qui pourraient vous trahir !](#)

Bonus, vous pouvez lancer cet atelier en fin de cycle après avoir réalisé avec les participant.e.s les ateliers suivants :

- [Envoyez des mails chiffrés pour garantir la confidentialité du contenu de vos emails](#)
- [Utilisez Signal, l'application mobile pour communiquer simplement de manière chiffré](#)
- [Apprenez à vous créer un mot de passe à toute épreuve](#)

Transmettre un fichier de façon sécurisé

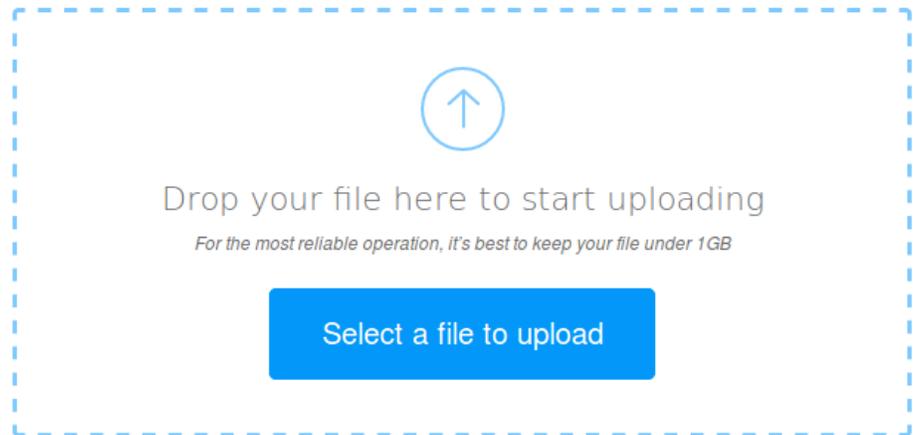
Envoyer un fichier sensible par e-mail en pièce-jointe n'est pas sécurisé à moins de le chiffrer avec un outil dédié, ce qui n'est pas à la porté de tou.te.s. Il existe des services proposé par des "tiers de confiance" nous avons tendance à plus faire confiance à Mozilla qui propose le service <https://send.firefox.com/> plutôt qu'à Wetransfer qui d'ailleurs ne protège pas le fichier avec un mot de passe et ne passe que par e-mail. Là tout se passe dans le navigateur SAUF la transmission du mot de passe qui devra se faire par un autre canal sécurisé.

La page d'accueil est clair :

Private, Encrypted File Sharing

Send files through a safe, private, and encrypted link that automatically expires to ensure your stuff does not remain online forever.

[Learn more](#)



Cliquez sur Select a file to upload (Sélectionnez le fichier à transmettre) votre explorateur de fichier apparait, selectionnez directement l'emplacement de la clé usb et sélectionnez le fichier et [OK]. La page suivante apparaitra:

The link to your file will expire
after **1 download** ▼ or 24
hours.

Copy and share the link to send your file: Balkany-galette.pdf

<https://send.firefox.com/download/fd37d91>

Copy to clipboard

Require a password to download this file

Delete file

[Send another file](#)

Votre fichier a été envoyer sur le site de façon sécurisé par défaut car votre navigateur utilise HTTPS, et mieux encore si vous utilisez TorBrowser. Comme indiqué le site génère un lien UNIQUE et complexe qui vous faudra transmettre à votre interlocuteur. Le site n'autorise qu'un seul téléchargement et passé 24 heure le fichier disparaît. Si par exemple regarde votre historique de navigation et clique sur le lien, hop il n'y aura plus rien !

On va quand même rajouter un mot de passe pour être SÛR ! Si quelqu'un intercepte le lien par exemple sur la boite mail de votre interlocuteur. elle ne pourra rien en faire puisqu'il n'aura pas le mot de passe:

The link to your file will expire
after **1 download** ▼ or 24
hours.

Copy and share the link to send your file: Balkany-galette.pdf

<https://send.firefox.com/download/fd37d91>

Copy to clipboard

Require a password to download this file

●●●●●●●●●●

Add password

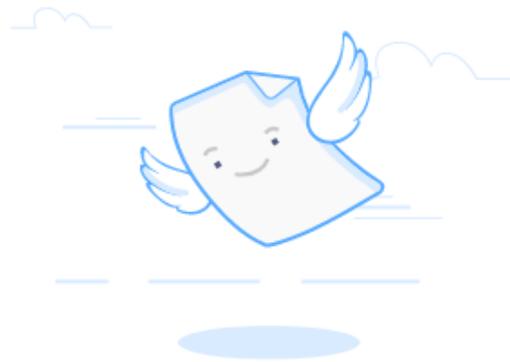
Delete file

[Send another file](#)

Et voilà vous pouvez envoyer le lien à votre contact par mail ou par SMS ou et le mot de passe par un autre canal sécurisé (Signal), il cliquera sur le lien et >>

Download Encrypted File

Your friend is sending you a file with Firefox Send, a service that allows you to share files with a safe, private, and encrypted link that automatically expires to ensure your stuff does not remain online forever.



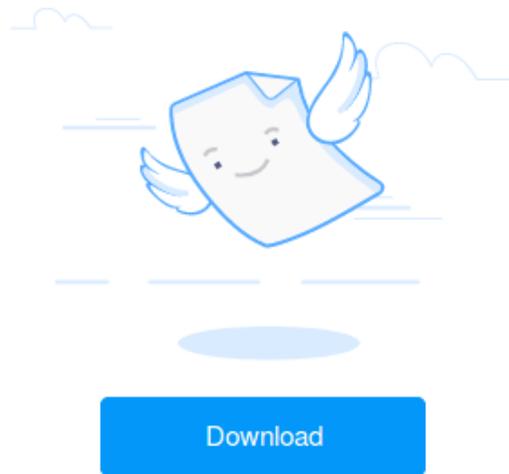
Enter Password

[Try Firefox Send](#)

Il rentre le mot de passe hop hop hop !

Download Balkany-galette.pdf (6.8kB)

Your friend is sending you a file with Firefox Send, a service that allows you to share files with a safe, private, and encrypted link that automatically expires to ensure your stuff does not remain online forever.

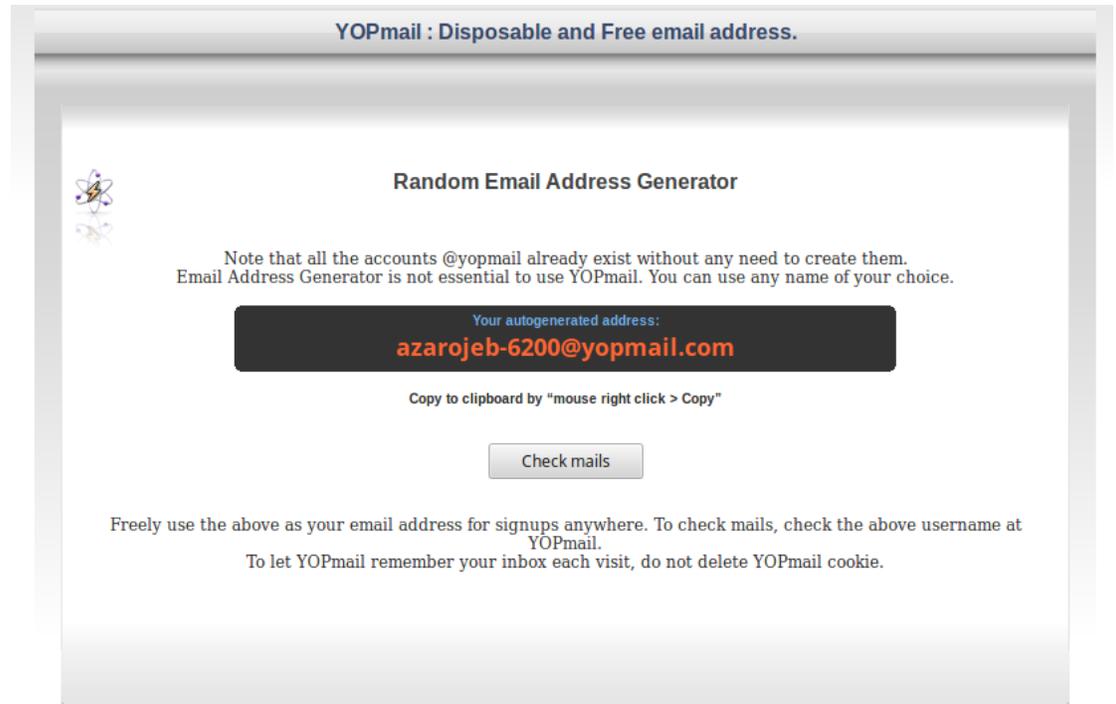


[Try Firefox Send](#)

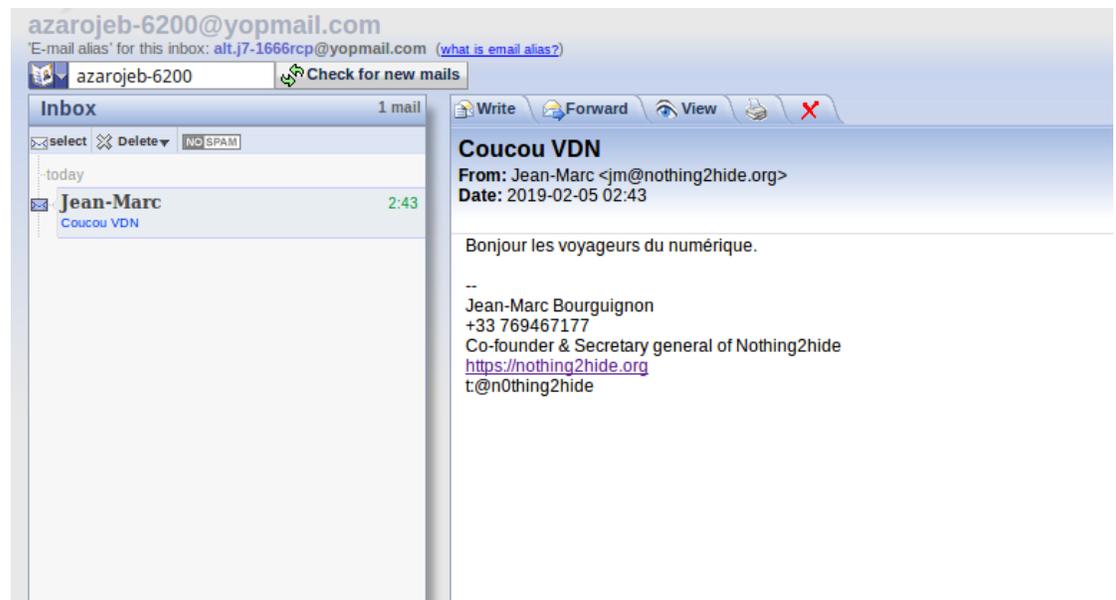
TADAAAAMMM en 5 mn like a boss j'ai transmis un fichier de façon sécurisé !

Un e-mail jetable ?

Avoir une adresse e-mail éphémère simplement aujourd'hui est une tannée, tout les services vous demanderons votre compte Facebook, Gmail, téléphone, Il serait tellement bien d'avoir la possibilité d'obtenir une adresse e-mail pour 1 échange et hop fini ! Et voila ! [YOPMAIL](#) (rien à voir avec la boisson lactée mais du coup ça aide pour s'en souvenir :).



Page d'accueil on ne peut plus clair, dès l'ouverture YopMail vous génère une adresse email aléatoire



Copiez l'adresse pour la communiquer à un contact et cliquez sur check mails

Hop une adresse mail fonctionnelle en 5 secondes, vous pouvez revenir dessus quand vous le voulez en tapant : azarojeb-6200 dans le champ à gauche de Check for new mails (Vous pouvez vous y rendre maintenant mais hey j'ai effacé mon mail hein). Ce genre de service n'est pas "top sécurisé" mais peut rendre service, à vous d'être imaginaire.ve ?

Notes jetables à la mission impossible

Un peu dans le même esprit que la transmission de fichier protégé et qui s'auto-détruit s'il est lu, il y a Privnote <https://privnote.com/#>
Pour tout simplement envoyer un message à une personne et s'assurer que elle seule le lira.

Nouvelle note ?

Écrivez votre note ici...

Créer une note Montrer les options

[Ecrire une nouvelle note](#) [Support](#) [Blog](#) Français
[Partager vos commentaires](#) [Vie privée](#) [Twitter](#) [Traduisez dans votre langue !](#)
[À propos](#) [Facebook](#)

L'accueil de se service est toujours aussi simple

La note s'autodétruit

après lecture

Ne pas demander de confirmation avant de montrer et détruire la note.

Mot de passe manuel.

Entrez un mot de passe pour chiffrer la note.

Verifiez votre mot de passe

Notification de destruction.

Notification par e-mail lorsque la note sera détruite.

Nom de la référence de la note (optionnel)

Créer une note

Désactiver les options

On choisit la langue en bas à droite, regardons les options avant d'écrire

Le lien vers la note est prêt.



<https://privnote.com/nvrOnPZ4>

La note va s'autodétruire après lecture.

Sélectionner le
lien

Lien e-mail

Détruire la note maintenant

Mot de passe manuel.

Il faut un mot passe pour lire la note.

Montrer le mot de passe

Faites votre choix, après lecture ou 1 heure ou plus ... un mot de passe, écrivez votre message et cliquez sur Créer une note et voilà !

Il ne vous reste qu'à transmettre le lien en jaune à votre contact et voilà, seul lui pourra le lire et ensuite pouffff plus rien. Ca ne laisse aucune trace sauf éventuellement dans l'historique de votre navigateur comme quoi vous avez été sur privnote mais comme vous êtes malin vous avez ÉVIDEMMENT ouvert une fenêtre de navigation privé dans votre navigateur préféré qui ne laisse pas d'historique hein ?

Attention aux méta données

Les méta-données comme vu dans l'atelier qui lui est consacré peuvent donner des informations sensibles, qui a créé le fichier, quand, où, Il faut donc avant de publier, ou d'envoyer un fichier être sur qu'il contient le minimum d'indice qui pourrait aider à identifier le lanceur.euse d'alertes. Pour cela il y a un service tout fraîchement mis en ligne : <https://mat2-web.dustri.org/> qui ne supporte pour l'instant que les fichiers images (photos, jpeg, ..) mais très vite il supportera pdf



>> Remove metadata

Upload your image, get a *cleaned* one in response.

Please note that while we do not keep a copy of your image, there is no way that you could be certain about this: act accordingly.

Browse...

No file selected.

UPLOAD

© jvoisin - source - ▼

Sobriété, simplicité, efficacité !



>> Metadata removed

mat2 managed to remove **all metadata** from your file.

⌵ DOWNLOAD CLEANED FILE

Not a single metadata was found by mat2, odds are that your file was already clean!

On clique sur Browse pour aller chercher notre fichier que nous souhaitons nettoyer nous cliquons sur upload et voilà !