Les emails frauduleux

Quelques conseils

Mise à jour 01/03/21

Plan de la présentation

- Conseils de base
- Exemples d’emails frauduleux
- Que faire en cas de piratage

Quelques chiffres

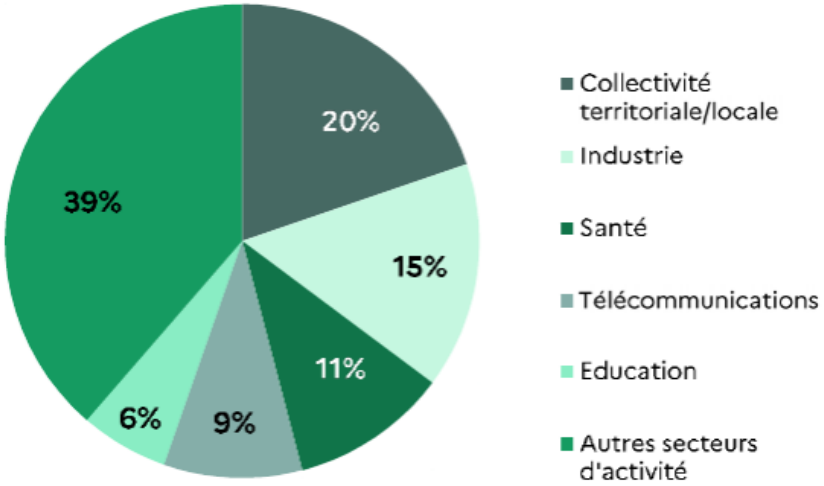
x4

nombre d'attaques par **rançongiciels** traitées par l'ANSSI entre 2019 et 2020

1re

menace pour les entreprises et les collectivités en 2020 selon cybermalveillance.gouv.fr

Secteurs d'activités touchés par les rançongiciels en 2020 en France



Les récentes attaques sur les centres hospitaliers de Dax-Côte d'Argent et de Villefranche-sur-Saône, nous montrent la criticité de cette menace dans notre quotidien.

Données ANSSI | Agence nationale de la sécurité des systèmes d'information

Conseils de base

- Avoir des produits à jour
  - Sur PC ou Mac : système d'exploitation à jour (Windows update activé)
  - Sur téléphone et tablettes : système d'exploitation à jour (Mise à jour Android par exemple)
- Avoir un antivirus et si possible un pare feu
  - Activé et mis à jour
- Avoir plusieurs mots de passe robustes
  - A modifier si doute
- Avoir plusieurs adresses email dont une dédiée Spam
  - Adresse à utiliser quand risque et suspecte par définition
  - Permet de faire un comparatif entre adresses
- Double authentification
- Effectuer des sauvegardes régulières

Mot de passe

Qu'est-ce qu'un mot de passe robuste ?

- **L'ANSSI recommande que la longueur d'un mot de passe soit corrélée avec la criticité du service auquel il donne accès**, avec un minimum de **9 caractères pour les services peu critiques** (dont la compromission ne donnerait accès à aucune information personnelle, financière et n'impacterait pas le fonctionnement de l'entreprise) et un minimum de **14 caractères pour les services critiques** ;
- Un mot de passe robuste comporte **des capitales et des minuscules, des chiffres et des caractères spéciaux** ;
- Ces mots de passe ne doivent comporter aucun élément personnel (tel qu'une date de naissance ou un prénom);
- Il est possible d'avoir recours à une phrase de passe (*passphrase* en anglais). Les phrases de passe consistent à choisir aléatoirement un certain nombre de mots parmi un corpus déterminé (comme le dictionnaire de la langue française). Les *passphrases* sont souvent bien plus longues que les mots de passe « classiques », mais sont aussi pour certains utilisateurs plus simples à mémoriser.

Qu'est-ce qu'une bonne politique de mots de passe ?

- **Il faut des mots de passe différents pour chaque service nécessitant une authentification**. Il convient en particulier de ne jamais utiliser un même mot de passe pour sa messagerie personnelle et sa messagerie professionnelle ;
- Un coffre-fort de mots de passe peut vous aider à générer des mots de passe robustes et ne pas avoir à les mémoriser. Il permet de sauvegarder l'ensemble des mots de passe dans un fichier chiffré, accessible uniquement par un seul et unique mot de passe. Il est préférable d'utiliser un coffre-fort certifié par l'ANSSI ;
- Le succès d'une bonne politique de choix des mots de passe nécessite une sensibilisation des utilisateurs aux risques liés au choix d'un mot de passe qui serait trop facile à deviner.
  Il faut activer une authentification multifacteurs quand elle est proposée par le fournisseur de service (mail, banque, etc.). De nombreux services permettent désormais de renforcer le

ANSSI | Agence nationale de la sécurité des systèmes d'information

Emails frauduleux
Définition

Il faut distinguer l'email frauduleux du spam

- SPAM : email non désiré qui fait la pub pour un produit, un service ; il est sans réel danger ;

- Emails frauduleux : email non désiré dont l'objectif est :
  - l'escroquerie (récupérer des informations bancaires, extorquer de l'argent, ..)
  - Le piratage informatique (rediriger vers des sites douteux, enregistrer les frappes sur le clavier, redémarrer l'ordinateur, bloquer les fichiers perso, …)

Il faut donc s'en prémunir

Emails frauduleux

Type

Le spam électronique

Le spam électronique, également appelé courrier indésirable ou pourriel, désigne une communication électronique non sollicitée à des fins publicitaires, commerciales ou malveillantes. Dans la majorité des cas, il s'agit de messages de prospection commerciale ne respectant pas les obligations légales en matière de consentement des destinataires, mais il peut également revêtir un caractère malveillant.

EN SAVOIR PLUS →

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

Emails frauduleux

Type

L'hameçonnage (phishing)

L'hameçonnage (ou phishing en anglais) est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles et/ou bancaires en se faisant passer pour un tiers de confiance. L'hameçonnage peut avoir différentes conséquences comme le vol d'informations personnelles ou professionnelles pour en faire un usage frauduleux.

EN SAVOIR PLUS →

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

Chantage à l'ordinateur ou à la webcam prétendus piratés

Le chantage à l'ordinateur ou à la webcam prétendus piratés (dit également « cryptoporno ») désigne un type d'escroquerie qui vise à vous faire croire que vos équipements ont été piratés afin de vous soutirer de l'argent.

EN SAVOIR PLUS →

Emails frauduleux

Type

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

Emails frauduleux

Les conséquences

Le piratage de compte

Le piratage de compte désigne la prise de contrôle par un individu malveillant d'un compte (messagerie, réseau social...) au détriment de son propriétaire légitime. Il peut avoir différentes conséquences comme l'usurpation d'identité, le vol de données bancaires...

EN SAVOIR PLUS →

Les rançongiciels (ransomwares)

Un rançongiciel (ransomware en anglais) est un logiciel malveillant qui bloque l'accès à l'appareil ou à des fichiers en les chiffrant et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès. Dans la majorité des cas, les cybercriminels exploitent des vulnérabilités connues dans les logiciels, mais dont les correctifs n'ont pas été mis à jour par les victimes.

EN SAVOIR PLUS →

Faire face aux arnaques au faux support technique

Votre appareil semble bloqué et on vous demande de rappeler d'urgence un numéro de support technique ? L'arnaque au faux support technique consiste à effrayer la victime pour ensuite la convaincre de payer un pseudo-dépannage informatique et/ou à acheter des logiciels inutiles, voire nuisibles.

EN SAVOIR PLUS →

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

Emails frauduleux

Expéditeur

L'expéditeur de l'email frauduleux se fait passer pour :

- Un ami
- Une banque (Crédit agricole, La Banque Postale, …)
- Un service administratif (Impôts, CAF, …)
- Un fournisseur (EDF, ENGIE, ….)
- Vous (c'est votre adresse qui vous écrit)

- Ou pas

Il faut donc être réellement vigilant

Vérifier toujours en premier lieu l'adresse de l'expéditeur (et celui à qui l'email est envoyé)

Emails frauduleux

Un émetteur reconnu ne vous demandera pas d'informations sensibles

- Une banque ne vous demandera pas votre mot de passe, votre numéro de carte bleue, ….
- Quelques prétextes assez courants :
  - ✓ Votre compte a été désactivé
  - ✓ Votre mot de passe a expiré
  - ✓ Vous avez un colis qui va arriver
  - ✓ Vous avez gagné un cadeau du fait de votre fidélité

  - – Si vous avez un doute contacter votre conseiller habituel directement et ne répondez pas à l'email
  - – Ne pas répondre à l'email
  - – Ne cliquez pas, n'appelez pas le numéro proposé, n'ouvrez pas une pièce jointe

Emails frauduleux

Un émetteur vous demande une rançon

- Surtout ne payez pas
- Quelques prétextes assez courants :
  - Il a enregistré avec votre webcam des scènes pornographiques
  - Il a bloqué vos données

  - Ne paniquez pas et ne répondez pas à l'email
  - Faire un scan antivirus de son PC puis le rallumer
  - Si les documents sont effectivement inaccessibles utilisez une sauvegarde
  - Prévenez de l'arnaque

Emails frauduleux

Exemples : tentatives d'arnaque

De DURAND Dominique <dorninique.chicard@orange.fr>
Sujet **Dominique -mesure**
Réponse à DURAND Dominique <dorninique.chicard@orange.fr>

Coucou,

Bonne année 2021 et tous nos vœux pour cette nouvelle année qui nous espérons sera bien meilleure que la précédente...

J espère que tu vas bien

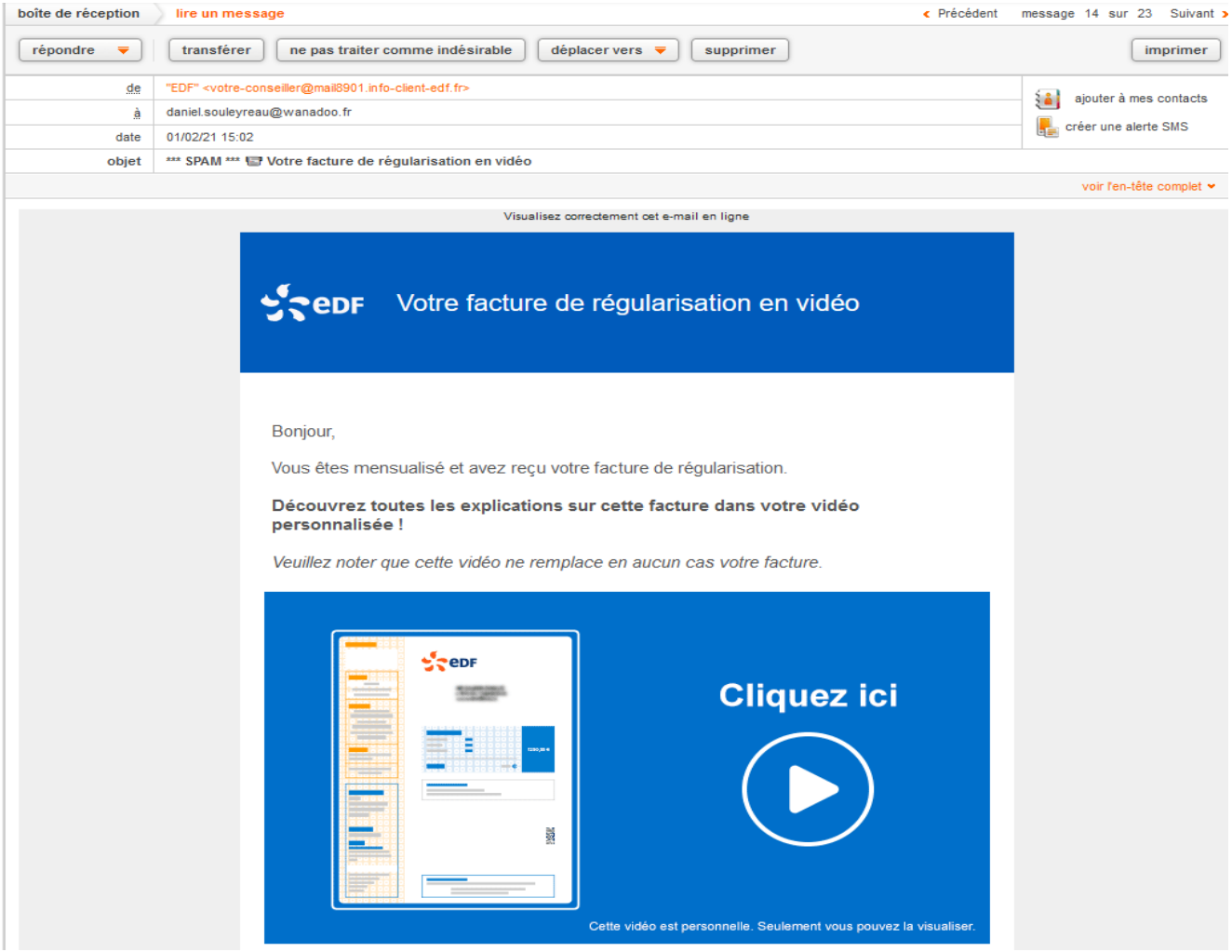
Serait-il possible de communiquer par mail?

MERCI BISES

Bonne réception, Dominique

Emails frauduleux

Exemples : tentative de phishing



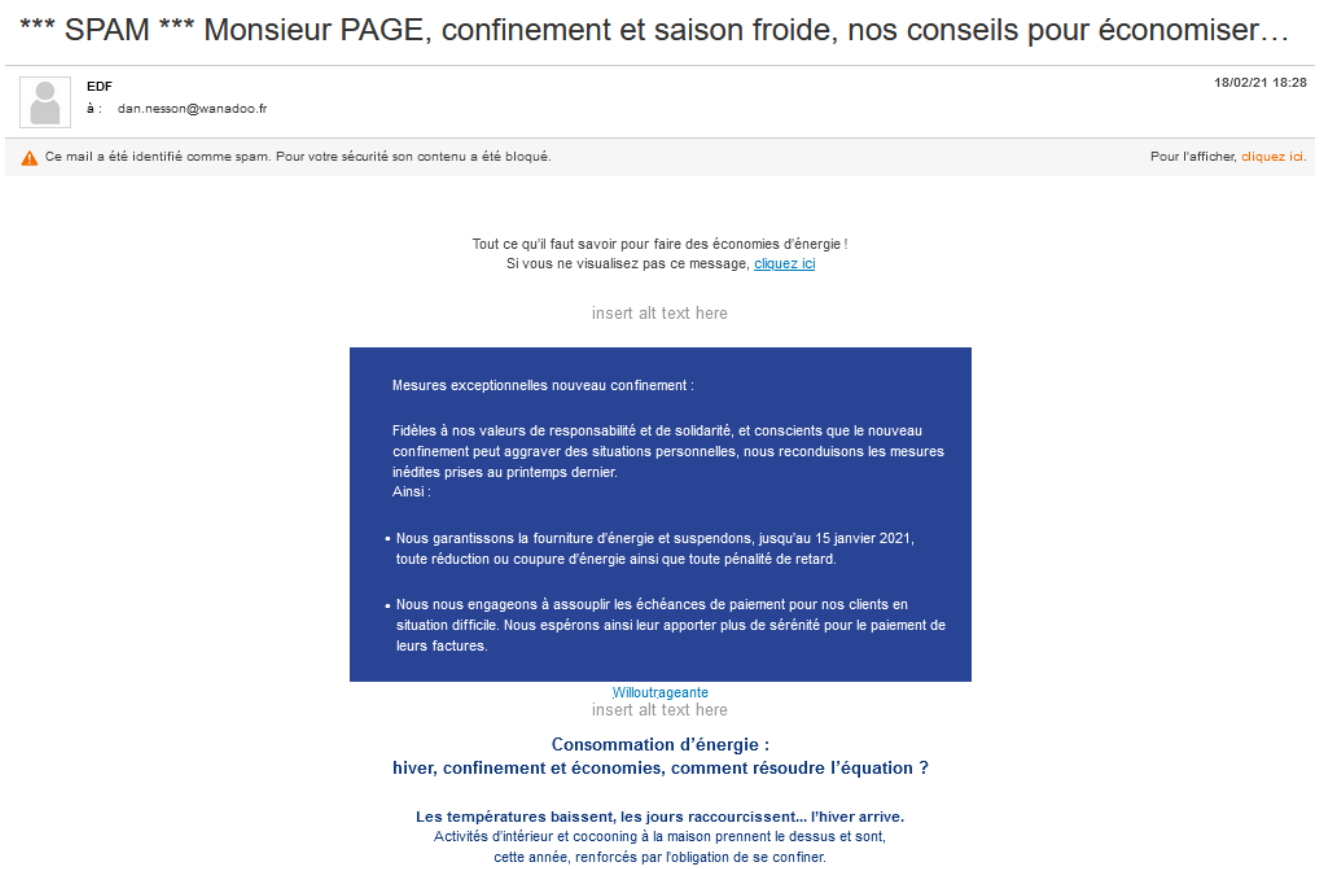
Emails frauduleux

Exemples : tentative de phishing

☐	Post	*** SPAM *** KS47F9171DSWE	15:57
☐	Post	*** SPAM *** CUN38N201KC6R	12:51
☐	Post	*** SPAM *** ZU1RM09QMQKWQ	12:41
☐	LinkedIn	*** SPAM *** Votre profil est apparu cette semaine dans les résultats de 2 recherches	11:12
☐	Post	*** SPAM *** VEUVW9ZV5GJMV	10:29
☐	Post	*** SPAM *** MG87WEMY4HZKB	07:00
☐	Bandsintown	*** SPAM *** Nouveau: Angerfist @ BigCityBeats World Club Dome - Las Vegas 2021	03:03
☐	eoue	*** SPAM ***	01:53
☐	EDF	*** SPAM *** Monsieur PAGE, confinement et saison froide, nos conseils pour économiser l'énergie.	hier
☐	Post	*** SPAM *** 3UT9XDZVSPUU6	hier
☐	Post	*** SPAM *** XMM16F18FELFZ	hier
☐	Post	*** SPAM *** FXN8PVZ0LFXX2	hier
☐	Post	*** SPAM *** FU2DVF4UAQ9U1	hier

Emails frauduleux

Exemples : tentative de phishing



*** SPAM *** Monsieur PAGE, confinement et saison froide, nos conseils pour économiser…

EDF
à : dan.nesson@wanadoo.fr

18/02/21 18:28

Ce mail a été identifié comme spam. Pour votre sécurité son contenu a été bloqué. Pour l'afficher, cliquez ici.

Tout ce qu'il faut savoir pour faire des économies d'énergie !
Si vous ne visualisez pas ce message, cliquez ici

insert alt text here

Mesures exceptionnelles nouveau confinement :

Fidèles à nos valeurs de responsabilité et de solidarité, et conscients que le nouveau confinement peut aggraver des situations personnelles, nous reconduisons les mesures inédites prises au printemps dernier.
Ainsi :

- Nous garantissons la fourniture d'énergie et suspendons, jusqu'au 15 janvier 2021, toute réduction ou coupure d'énergie ainsi que toute pénalité de retard.
- Nous nous engageons à assouplir les échéances de paiement pour nos clients en situation difficile. Nous espérons ainsi leur apporter plus de sérénité pour le paiement de leurs factures.

Willoutrageante
insert alt text here

Consommation d'énergie :
hiver, confinement et économies, comment résoudre l'équation ?

Les températures baissent, les jours raccourcissent... l'hiver arrive.
Activités d'intérieur et cocooning à la maison prennent le dessus et sont, cette année, renforcés par l'obligation de se confiner.

Emails frauduleux

Adresse email (spam)

☐	Covid-19	*** SPAM *** Covid-19	dimanche
☐	Covid-19	*** SPAM *** Covid-19	dimanche
☐	Covid-19	*** SPAM *** Covid-19	dimanche

*** SPAM *** Covid-19

Covid-19
à : anne.baumgarten@orange.fr

21/02/21 11:59

Danger! Notification urgente Covid-19!

*** SPAM *** Covid-19

Covid-19
à : elsa.difraya@orange.fr

20/02/21 09:35

Danger! Notification urgente Covid-19!

Adresse email (normale)

☐	Covid-19	Covid-19	20/02/21 11:42	2.3 ko
☐	Castorama	Nous déclarons la saison du jardin... OU...	20/02/21 08:13	98.9 ko

boîte de réception › lire un message

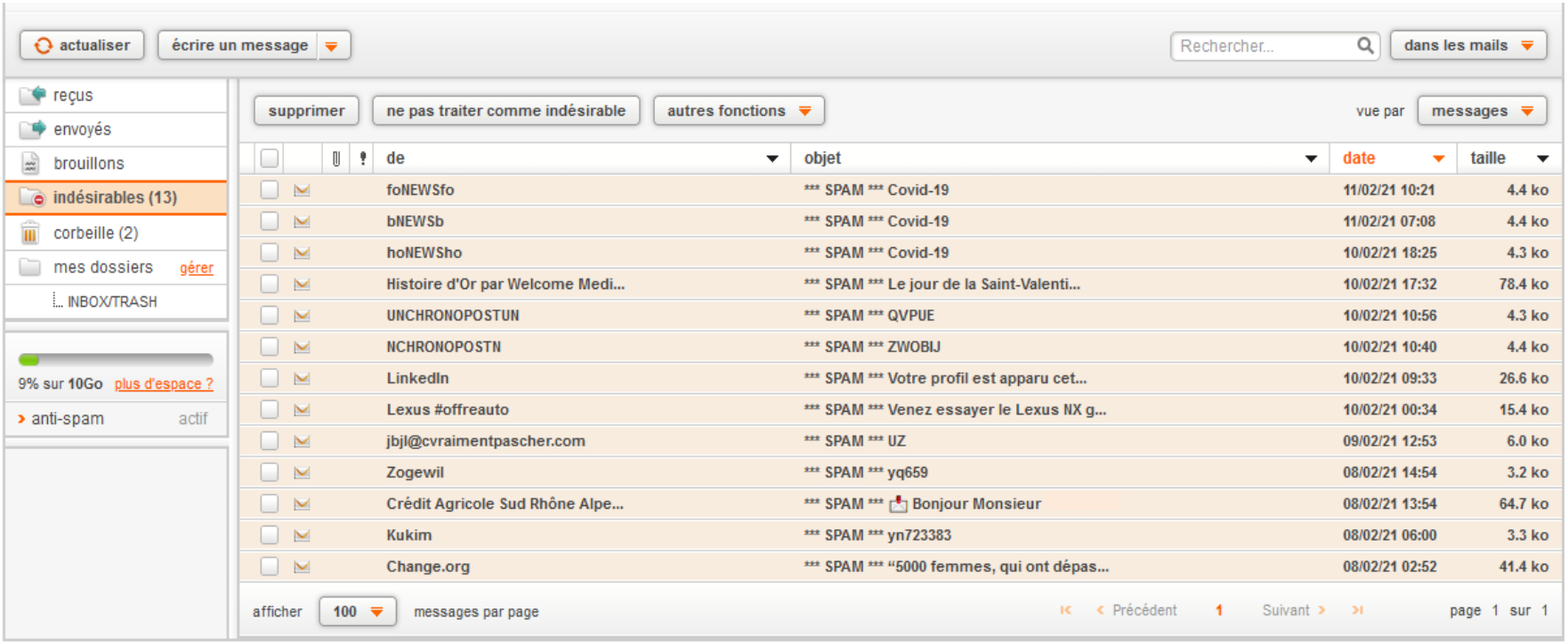
répondre | transférer | traiter comme indésirable | déplacer vers | supprimer

de	"Covid-19" <hklma@bigbluehosting.com>
à	d.zaoui@wanadoo.fr
date	20/02/21 11:42
objet	Covid-19

Danger! Notification urgente Covid-19!

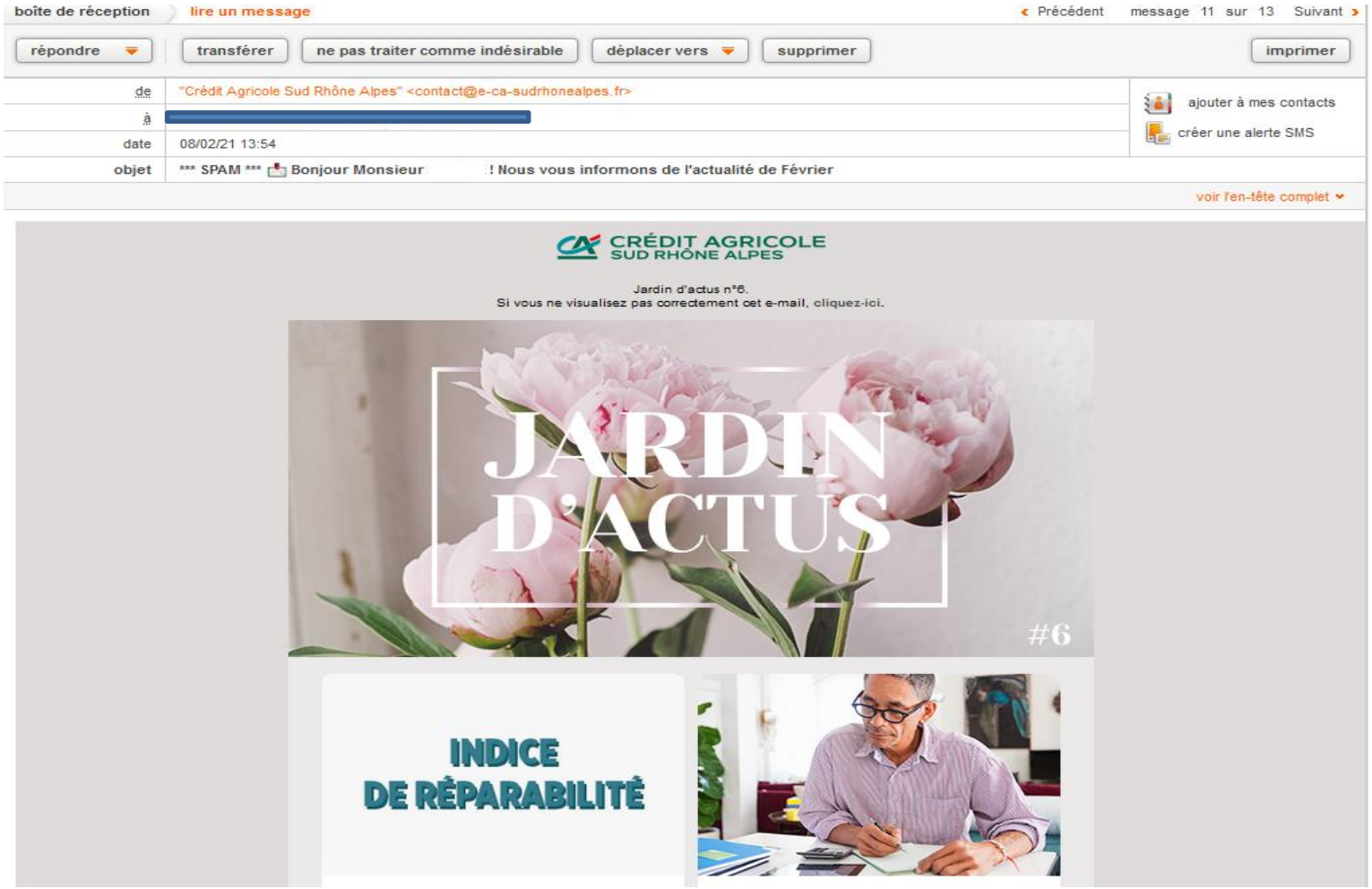
Emails frauduleux

Exemples d'ensemble d'indésirables



Emails frauduleux

Exemple de faux indésirable



Conclusion - Préconisations

- Restez toujours vigilants
  - ➢ Sans paranoïa mais :
    - Vérifier toujours l'adresse de l'expéditeur et l'adresse à qui est envoyé l'email ;
    - Vérifier les logos, les fautes d'orthographe, la qualité des images ;
    - Vérifier aussi la pertinence des adresses des sites mentionnés dans l'email.
  - ➢ Si vous utilisez un logiciel de messagerie :
    - Vérifier de temps en temps les spams sur le serveur
- Ne cédez pas à la tentation
  - ➢ Les affaires en or, les cadeaux ou les appels sexy sont des pièges
    - Ne cliquez pas et n'ouvrez pas les pièces jointes si vous avez un doute
- Ne transmettez jamais d'informations de type mot de passe, numéros de compte, carte bleue par email
  - ➢ Allez sur les sites officiels pour cela (https:\\...)

Conclusion - Préconisations

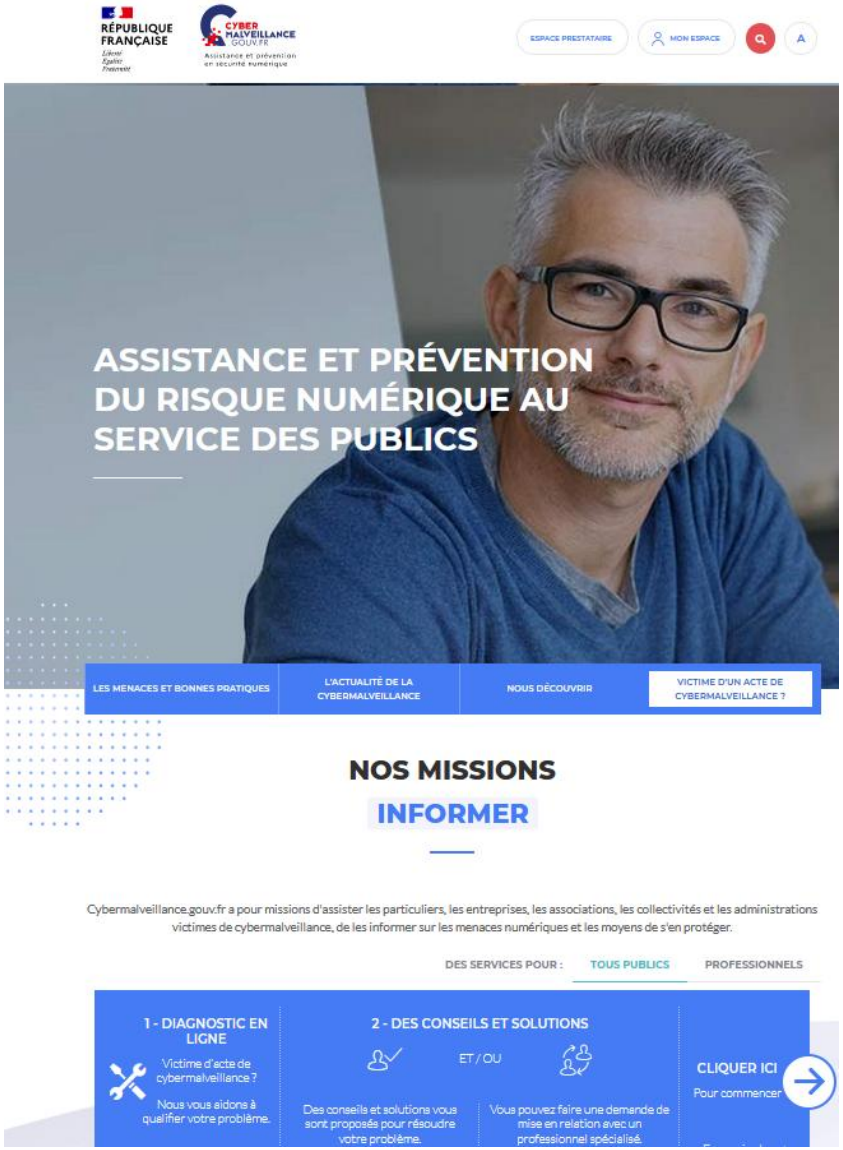
- Utilisez une adresse email dédiée pour les arnaques
  - L'employer pour les commandes internet par exemple
  - Conserver l'adresse perso uniquement pour les organismes « officiels »
- Ayez différents mots de passe robustes mais faciles à retenir
- Maintenez vos systèmes à jour
  - PC, MAC, tablettes, téléphones
  - Utilisez antivirus et pare-feu
- Conservez une sauvegarde des vos fichiers essentiels
- Utilisez la double authentification quand cela est possible

Vous avez répondu à un email frauduleux

- Modifiez tout de suite le mot de passe et les mots de passe associés si besoin
  - Par un autre moyen si possible (autre PC, téléphone, …)
- Réalisez une analyse antivirus
- Surveillez vos comptes bancaires
- Envoyer l'email à :www.internet-signalement.gouv.fr
- Si l'adresse et votre compte ont été piratés :
  - Essayer mot de passe oublié
  - Joindre votre fournisseur d'accès par un autre moyen

Vous avez répondu à un email frauduleux

- Utilisez la plateforme :
  - ➢ cybermalveillance.gouv.fr
  - ➢ Avec les fiches de conseils et de solutions



Vous avez répondu à un email frauduleux

Piratage de compte

Extraits du site cybermalveillance.gouv.fr

[Conseils préventifs]

Vérifiez l'adresse du site qui s'affiche dans votre navigateur. Si cela ne correspond pas exactement au site concerné, il s'agit certainement d'un site frauduleux. Il suffit parfois d'un seul caractère changeant pour vous tromper.

Déconnectez-vous systématiquement de votre compte après utilisation pour éviter que quelqu'un puisse y accéder après vous.

Si vous ne pouvez plus vous connecter à votre compte, **CONTACTEZ LE SERVICE CONCERNÉ POUR SIGNALER VOTRE PIRATAGE ET DEMANDEZ LA RÉINITIALISATION DE VOTRE MOT DE PASSE.**

Dans vos paramètres de récupération de compte, **ASSUREZ-VOUS QUE VOTRE NUMÉRO DE TÉLÉPHONE ET VOTRE ADRESSE MAIL DE RÉCUPÉRATION SOIENT LES BONS**. Si ce n'est pas le cas, changez-les immédiatement.

CHANGEZ AU PLUS VITE VOTRE MOT DE PASSE et choisissez-en un solide (voir notre fiche sur la gestion des mots de passe). Et si possible, **ACTIVEZ LA DOUBLE AUTHENTIFICATION.**

CHANGEZ SANS TARDER LE MOT DE PASSE PIRATÉ SUR TOUS LES AUTRES SITES OU COMPTES SUR LESQUELS VOUS POUVIEZ L'UTILISER.

PRÉVENEZ TOUS VOS CONTACTS DE CE PIRATAGE pour qu'ils ne soient pas victimes à leur tour des cybercriminels qui les contacteraient en usurpant votre identité.

VÉRIFIEZ QU'AUCUNE PUBLICATION OU COMMANDE N'A ÉTÉ RÉALISÉE avec le compte piraté.

Si vos coordonnées bancaires étaient disponibles sur le compte piraté, surveillez vos comptes, **PRÉVENEZ IMMÉDIATEMENT VOTRE BANQUE** et faites au besoin opposition aux moyens de paiement concernés.

En fonction du préjudice subi, **DÉPOSEZ PLAINTE** au commissariat de police ou à la gendarmerie ou écrivez au procureur de la République dont vous dépendez en fournissant toutes les preuves en votre possession.

Vous avez répondu à un email frauduleux

Webcam – crypto porno

Extraits du site cybermalveillance.gouv.fr

Conseil préventif

Évitez les sites non sûrs ou illicites, tels ceux qui hébergent des contrefaçons (musique, films, logiciels…) ou certains sites pornographiques qui peuvent infecter votre machine ou héberger des régies publicitaires douteuses.

NE PANIQUEZ PAS. En effet, vous n'avez sans doute rien de réellement compromettant à vous reprocher.

NE RÉPONDEZ PAS. Il ne faut jamais répondre à de telles menaces de chantage qui montrent aux cybercriminels que votre adresse de messagerie est « valide » et que vous portez de l'intérêt au message de chantage qu'ils vous ont envoyé.

NE PAYEZ PAS LA RANÇON. Et ce, même si vous aviez un doute. En effet, aucune mise à exécution des menaces n'a été démontrée jusqu'à présent et vous alimenteriez donc inutilement ce système criminel.

CONSERVEZ LES PREUVES. Faites des captures d'écran, conservez les messages qui pourront vous servir pour signaler cette tentative d'extorsion aux autorités.

CHANGEZ AU PLUS VITE VOTRE MOT DE PASSE partout où vous l'utilisez s'il a été divulgué ou au moindre doute et choisissez-en un solide (tous nos conseils pour gérer vos mots de passe).

CONTACTEZ VOTRE BANQUE si vous avez payé la rançon pour essayer de faire annuler la transaction.

DÉPOSEZ PLAINTE au commissariat de police ou à la brigade de gendarmerie ou en adressant votre plainte au procureur de la république du tribunal de grande instance dont vous dépendez.

Vous avez répondu à un email frauduleux

Faux support technique

Extraits du site cybermalveillance.gouv.fr

NE RÉPONDEZ PAS AUX SOLLICITATIONS et n'appelez jamais le numéro indiqué.

CONSERVEZ TOUTES LES PREUVES. Photographiez votre écran au besoin.

S'il semble « bloqué », **REDÉMARREZ VOTRE APPAREIL.** Cela peut suffire à régler le problème.

Si votre navigateur reste incontrôlable, **PURGEZ LE CACHE, SUPPRIMEZ LES COOKIES, RÉINITIALISEZ LES PARAMÈTRES PAR DÉFAUT** et si cela ne suffit pas, supprimez et recréez votre profil.

DÉSINSTALLEZ TOUTE NOUVELLE APPLICATION SUSPECTE présente sur votre appareil.

FAITES UNE ANALYSE ANTIVIRUS approfondie de votre machine.

Si un faux technicien a pris le contrôle de votre machine, **DÉSINSTALLEZ LE PROGRAMME DE GESTION À DISTANCE, ET CHANGEZ TOUS VOS MOTS DE PASSE.** En cas de doute ou si vous n'arrivez pas à reprendre le contrôle de votre équipement par vous-même, vous pouvez faire appel à un prestataire référencé sur www.cybermalveillance.gouv.fr.

Si vous avez fourni vos coordonnées bancaires ou n° de carte de crédit, **FAITES OPPOSITION** sans délai. Si un paiement est débité sur votre compte, **EXIGEZ LE REMBOURSEMENT** en indiquant que vous déposez plainte.

Si vous avez été contacté par un faux support technique, **SIGNALEZ LES FAITS AU MINISTÈRE DE L'INTÉRIEUR** sur sa plateforme Internet-signalement.gouv.fr.

DÉPOSEZ PLAINTE au commissariat de police ou à la brigade de gendarmerie ou en écrivant au procureur de la République dont vous dépendez. Faites vous, au besoin, assister par un avocat spécialisé.