



Réfléchissez à deux fois avant de cliquer sur un lien!

Tout ce qu'il faut savoir pour reconnaître le phishing à temps en cette période de télétravail et de coronavirus.

Mars 2020



Coronavirus : La une des journaux!



- Un sujet brûlant :
 - Médias : JT, radio, presse
 - Discussion avec notre famille et nos proches
 - Mises à jour quotidiennes
- Différents canaux de communication :
 - Whatsapp
 - SMS
 - Facebook
 - E-mail
- Confinement = télétravail + achat en ligne
 - Masques, gels hydroalcooliques
 - Commander à manger
 - Autres achats en ligne



Mais les cybercriminels s'y retrouvent eux aussi...

- Les cybercriminels sont très créatifs pour adapter leur modus operandi à l'actualité
- Ils savent que nous sommes à l'affut des dernières informations concernant le coronavirus et en profitent
- De par notre curiosité, nous tombons bien souvent dans le panneau des faux sites d'informations



Le phishing ? Késako ?

- Des cybercriminels tentent d'accéder à vos données, voire à vos appareils
- Et c'est souvent vous qui leur fournissez un accès !
- Comment ça ?
 - Etape 1 : Ils envoient un message contenant un lien ou une pièce jointe
 - Etape 2 : Vous ouvrez la pièce jointe ou cliquez sur le lien et êtes redirigé vers un faux site internet
 - Etape 3 : Vous introduisez vos données
 - Numéro de carte bancaire, code PIN, chiffre de sécurité
 - Nom d'utilisateur et mot de passe

➔ Et vous leur fournissez ainsi un accès





ATTENTION AU PHISHING EN LIEN AVEC

1. La vente de masques, de gels hydroalcooliques ou produits désinfectants
2. Des fausses actualités concernant le COVID-19
3. De fausses collectes de fonds pour les victimes





Quelques conseils



Conseil n°1 : lisez l'URL

- Vérifiez toujours l'URL et le nom de domaine de liens avant de cliquer dessus.
 - C'est très facile : il suffit de faire glisser le curseur sur le lien, sans cliquer dessus.
- Un domaine est le mot qui figure juste avant .be, .com . org...
 - delhaize-be.site n'est pas un domaine de Delhaize.
Le domaine correct est delhaize.be
 - Dans www.safeonweb.tips.be, le nom de domaine est « tips » et pas safeonweb
- http:// est moins sécurisé que https://



Conseil n°2 : vérifiez l'adresse de l'expéditeur

- Le domaine de l'adresse e-mail est louche ?
 - @xyz542.be est un nom de domaine louche
 - policefederales@gmail.be : une instance officielle ou une entreprise n'utilise pas d'adresse Gmail ou Hotmail.
- Vous ne connaissez pas l'expéditeur ? Vous n'attendez absolument pas de message de sa part ? Soyez sur vos gardes.



Conseil n°3 : faites attention à la formulation du message

- Le message contient de nombreuses fautes ? Il s'agit presque à coup sûr de phishing.
- Le ton est directif et insistant ?
 - Un expéditeur professionnel, a fortiori une institution financière, ne se montrera jamais insistant.
 - Les messages adressés à des clients ne sont jamais agrémentés de la mention « importance : élevée ». Les criminels utilisent ce stratagème pour vous mettre sous pression.
- Le message suscite fortement votre curiosité?
 - Ne réfléchissez pas à deux mais à cinq fois avant de cliquer. Il s'agit tout simplement d'une façon de vous encourager à cliquer.



Conseil n°4 : faites attention aux messages inattendus

- La communication est inattendue ? Soyez sur vos gardes.
 - Vous n'avez pas commandé de paquet ? Il y a alors très peu de chance que vous receviez un code de tracking ou d'autres informations relatives à un paquet. Ne donnez pas suite à des e-mails qui essaient de vous inciter à cliquer sur des liens.
 - Cela vaut également pour les messages d'une banque ou d'un fournisseur chez qui vous n'êtes pas client.



“Relax,
réfléchissez à
deux fois avant
de cliquer sur
un lien”



Vous avez dit phishing ?

Le phishing est une escroquerie en ligne au moyen de faux emails, sites internet ou messages. Les cybercriminels exploitent la confiance que vous avez, par exemple, en une personne ou en une société. Ils essaient aussi de vous faire peur. Ne tombez pas dans le panneau !

Comment identifier les messages suspects ?

Les messages de phishing :

- arrivent généralement **de façon inattendue** et sans raison
- sont insistants ou tentent d'éveiller votre curiosité
- contiennent des fautes ou utilisent des formulations bizarres
- s'adressent à vous avec **un titre vague** ou utilisent votre adresse email au lieu de votre nom ou prénom
- **proviennent d'un expéditeur inconnu**
- ont un lien qui ne mène pas à un site internet sécurisé

Les faux messages ne sont pas toujours des emails. De plus en plus, les escrocs envoient de faux sms – on parle alors de **Smishing**. Vous pouvez aussi recevoir des messages de phishing via les médias sociaux, comme Facebook ou WhatsApp.





Il est l'heure de s'entraîner !



Corona worse than Ebola?

start now

Learn how to survive the Corona Virus Pandemic sweeping
the world!



 Digital Download Pandemic Guide

To unsubscribe please [click here](#)

If you do not wish to continue
receiving email newsletters [CLICK HERE](#)



Corona worse than Ebola?

start now

Learn how to survive the Corona Virus Pandemic sweeping
the world!



**DIGITAL
DOWNLOAD** Pandemic Guide

To unsubscribe please [click here](#)

If you do not wish to continue
receiving email newsletters [CLICK HERE](#)





De : Safe Mask <From-9748@ort2k.pclpiuisvjit.com>
Envoy : mercredi 4 mars 2020 15:53
Objet : Coronavirus fait peur! Obtenez SafeMask pour vous aider a lutter contre les virus

Coronavirus fait peur! Obtenez SafeMask pour vous aider lutter contre les virus

De: Safe Mask <From-9748@ort2k.pclpiuisvjit.com>
Envoy : mercredi 4 mars 2020 15:53

Objet : Coronavirus fait peur ! Obtenez SafeMask pour vous aider a lutter contre les virus

BREAKING: Number of infected cases surged pass 60,000. Health Experts declares state of emergency...



FFP2 Face Mask Finally Available in the United States Could Help Against Deadly Virus Outbreak

The severe **Coronavirus** is spreading across the globe at a rapid pace. With multiple governments declaring state of emergency, virtually anyone can be infected. The biggest issue is that medical researchers are still unsure how exactly it can spread.



However, what we do know is that the virus is so infective, medical staff are required to wear all protective equipment available — even hazmat suits. One highly probable guess is that the virus spreads by air. Many believe that's how the outbreak began...

That means raw, unfiltered air could potentially infect anyone with the virus. And because it's spreading so quickly, there's no way for sure that scientists can tell which country is safe and which is not. Right now, no place seems to be out of reach for the **Coronavirus**.

[Read More Here >>](#)



De : Safe Mask <From-9748@ort2k.pclpiuisvjit.com>
Envoy : mercredi 4 mars 2020 15:53
Objet : Coronavirus fait peur! Obtenez SafeMask pour vous aider a lutter contre les virus

[Coronavirus fait peur! Obtenez SafeMask pour vous aider lutter contre les virus](#)

De: Safe Mask <From-9748@ort2k.pclpiuisvjit.com>
Envoy : mercredi 4 mars 2020 15:53

Objet : Coronavirus fait peur ! Obtenez SafeMask pour vous aider a lutter contre les virus

BREAKING: Number of infected cases surged pass 60,000. Health Experts declares state of emergency...



FFP2 Face Mask Finally Available in the United States Could Help Against Deadly Virus Outbreak

The severe **Coronavirus** is spreading across the globe at a rapid pace. With multiple governments declaring state of emergency, virtually anyone can be infected. The biggest issue is that medical researchers are still unsure how exactly it can spread.



However, what we do know is that the virus is so infective, medical staff are required to wear all protective equipment available — even hazmat suits. One highly probable guess is that the virus spreads by air. Many believe that's how the outbreak began...

That means raw, unfiltered air could potentially infect anyone with the virus. And because it's spreading so quickly, there's no way for sure that scientists can tell which country is safe and which is not. Right now, no place seems to be out of reach for the **Coronavirus**.

[Read More Here >>](#)



Van: SafeMask Promotion <info@jdnserver.nl>

Datum: 5 maart 2020 om 18:03:15 CET

Aan: [redacted]

Onderwerp: ⚠️ Coronavirus warning: This mask adds an extra layer of protection...

Antwoord aan: info@great.speedskincare.com

[View Offer](#)

The best-selling SafeMask!

SafeMask keeps you and your loved ones safe, even during the worst air pollution occurrences and during the yearly outbreaks of several dangerous viruses.

We also recommend you to take advantage of the very attractive multiple order discounts that is offering. Why not get one for your loved ones or one for your friends? Take advantage now, since these discounts won't last forever.

[Click here to buy SafeMask - 50% Off & Free Shipping!](#)

[If you'd prefer not to receive future emails, Unsubscribe Here:](#)
23638 W. Lyons Avenue #468 3C Newhall, CA 91321



Van: SafeMask Promotion <info@jdnserver.nl>

Datum: 5 maart 2020 om 18:03:15 CET

Aan: [redacted]

Onderwerp: ⚠️ Coronavirus warning! This mask offers an extra layer of protection...

Antwoord aan: info@great.speedskincare.com

[View Offer](#)

The best-selling SafeMask!

SafeMask keeps you and your loved ones safe, even during the worst air pollution occurrences and during the yearly outbreaks of several dangerous viruses.

We also recommend you to take advantage of the very attractive multiple order discounts that is offering. Why not get one for your loved ones or one for your friends? Take advantage now, since these discounts won't last forever.

[Click here to buy SafeMask - 50% Off & Free Shipping!](#)

If you'd prefer not to receive future emails, [Unsubscribe Here](#):
23638 W. Lyons Avenue #468 3C Newhall, CA 91321





Beste 2dehands-gebruiker,

De snelle verspreiding van het coronavirus en de huidige maatregelen van het kabinet hebben ingrijpende gevolgen voor iedereen.

Dat geldt ook voor 2dehands.be. De afgelopen dagen is gebleken dat goed en veilig handelen in deze snel veranderende omstandigheden een moeilijke opgave is.

Het welzijn van onze klanten, collegas en medewerkers weegt daarin zwaar.

Dat heeft ons ertoe gebracht om zo spoedig mogelijk extra maatregelen te nemen, dit geldt in elk geval t/m maandag 6 april.

Naar aanleiding hiervan bent u als 2dehands klant verplicht uw apparaat of toestel in kwestie opnieuw te registreren, en of deze te verlengen in verband met onze veiligheidsstandaarden omtrent Mijn 2dehands.

De extra stap is verplicht vanwege de nieuwe standaard regels van de twee-factor-authenticatie en dient als extra maatregel tegen het coronavirus.

lees verder

Hoe werkt het?

- Stap 1 - Je logt in met je gebruikersnaam en wachtwoord, zoals je dat nu ook doet.
- Stap 2 - Je krijgt een nieuw scherm, waarin je een koper of verkoper kunt controleren met de twee-factor authenticatie gekoppeld aan uw rekeningnummer, heel eenvoudig als Bancontact dus.

Uit ons systeem blijkt dat het account gekoppeld aan e-mailadres [REDACTED] nog niet (volledig) voldoet aan alle eisen om gebruik te maken van de twee-factor-authenticatie, rond optijd de verificatie controle af om probleemloos gebruik te kunnen blijven maken van onze platform.

[Naar Mijn 2dehands](#)

Als je niks doet, worden al zoekertjes op 21 maart '20 automatisch verwijderd.

Tip: Onder meer van belang bij een effectieve bestrijding is het snel opmerken van besmette gevallen en verdere zorg spoedig te verlenen. Om te voorkomen dat het virus zich kan verspreiden adviseren wij u de 2F per direct te activeren en tijdelijk fysieke handel te mijden.

Met vriendelijke groeten,
Het 2dehands-te2



Beste 2dehands-gebruiker,

De snelle verspreiding van het coronavirus en de huidige maatregelen van het kabinet hebben ingrijpende gevolgen voor iedereen. Dat geldt ook voor 2dehands.be. De afgelopen dagen is gebleken dat goed en veilig handelen in deze snel veranderende omstandigheden een moeilijke opgave is. Het welzijn van onze klanten, collegas en medewerkers weegt daarin zwaar. Dat heeft ons ertoe gebracht om zo spoedig mogelijk extra maatregelen te nemen, dit geldt in elk geval t/m maandag 6 april.

Naar aanleiding hiervan bent u als 2dehands klant verplicht uw apparaat of toestel in kwestie opnieuw te registreren, en of deze te verlengen in verband met onze veiligheidsstandaarden omtrent Mijn 2dehands. De extra stap is verplicht vanwege de nieuwe standaard regels van de twee-factor-authenticatie en dient als extra maatregel tegen het coronavirus. lees verder

Hoe werkt het?

- Stap 1 - Je logt in met je gebruikersnaam en wachtwoord, zoals je dat nu ook doet.
- Stap 2 - Je krijgt een nieuw scherm, waarin je een koper of verkoper kunt controleren met de twee-factor authenticatie gekoppeld aan uw rekeningnummer, heel eenvoudig als contact dus.

Uit ons systeem blijkt dat het account nog niet is gemaakt van de twee-factor-authenticatie om probleemloos gebruik te kunnen maken.

<http://2dehandscorona.ootoyasushifood.com/>

Click or tap to follow link.


Naar Mijn 2dehands

Als je niks doet, worden al zoekertjes op 21 maart '20 automatisch verwijderd.

Tip: Onder meer van belang bij een effectieve bestrijding is het snel opmerken van besmette gevallen en verdere zorg spoedig te verlenen. Om te voorkomen dat het virus zich kan verspreiden adviseren wij u de 2F per direct te activeren en tijdelijk fysieke handel te mijden.

Met vriendelijke groeten,
Het 2dehands-te2





J'ai reçu un message de phishing. Que faire ?



Bravo ! Vous avez identifié un message suspect

- Transférez-le à suspect@safeonweb.be
- Le message vient d'une banque ou d'une organisation connue ?
 - Transférez-le à l'organisation ou la banque en question. Ils apprécient d'être mis au courant lorsque leur nom est exploité à des fins de phishing. Les banques ont une adresse e-mail spécifiquement dédiée : phishing@NOMDELABANQUE.be
- Vous avez reçu le message suspect sur votre adresse professionnelle ?
 - Transférez-le à votre service ICT. Une démarche est peut-être déjà prévue en interne.
- Supprimez le message



Mince ! Vous avez cliqué ?!

- Le message a été transmis à vos amis ?
 - Mettez-les en garde !
- Vous avez communiqué un mot de passe ?
 - Changez le mot de passe partout où vous l'utilisez
- Vous avez communiqué des coordonnées bancaires ?
 - Prévenez votre banque et Cardstop (070/344344, numéro à conserver dans les contacts)
- Un programme risque d'avoir été installé ?
 - Effectuez un scan antivirus
- Cela vous est arrivé au travail ?
 - Prévenez votre service informatique. Ils peuvent éviter que d'autres soient pris au piège ou qu'un virus continue à se propager.
- Supprimez le message





En savoir plus sur le phishing ?

- www.safeonweb.be
- Suivez-nous sur Facebook : <https://www.facebook.com/Safeonweb.be/>
- Suivez-nous sur Twitter : https://twitter.com/safeonweb_be
- Suivez-nous sur YouTube : [Safeonweb.be](https://www.youtube.com/Safeonweb.be)





Participer à nos
campagnes de
sensibilisation ?

Tout le matériel de campagne est
disponible sur www.safeonweb.be



Relax!

And think twice before
clicking on a link



Une présentation
proposée par
Safeonweb dans
le cadre de la
campagne de
2019

