SURFEZ EN SÉCURITE !

PARTIE 1 : RECONNAITRE LES RISQUES

LES MAILS

envoyé : 20 mars 2023 à 16:31
de : Service clients leboncoin <aide@capturetruth.com>
à : Ani @orange.fr>
objet : Compte piraté - dossier N°28956802

Bonjour,

Nous avons bien reçu votre demande **N°28956802**.

Notre réponse vous parviendra dans les meilleurs délais.

Pour suivre ou mettre à jour votre demande, rendez-vous dans la section Mes demandes de notre centre d'aide.

Si toutefois vous n'avez plus accès à votre compte, répondez à cet email.

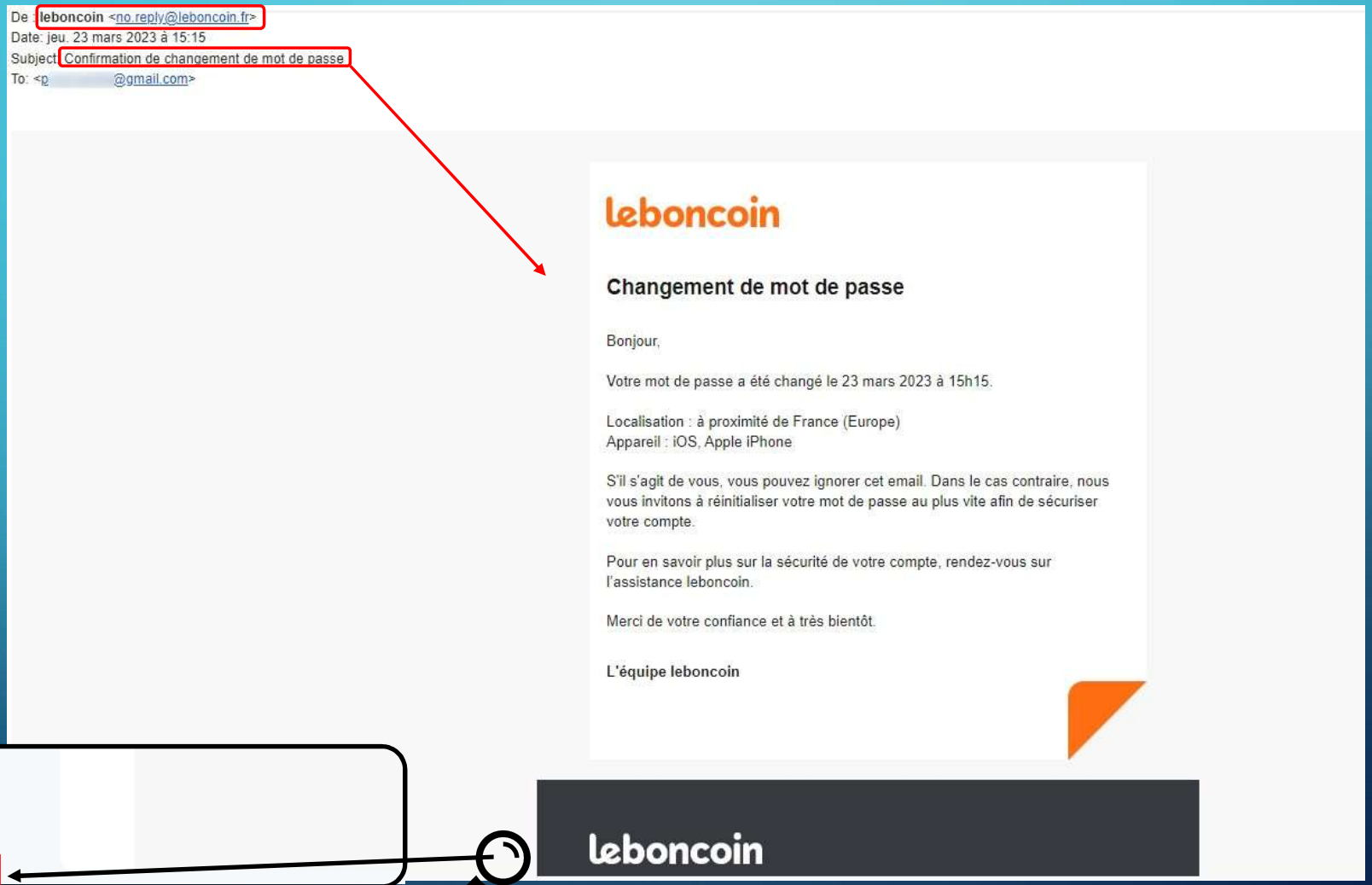
Pour faciliter le traitement, si votre demande est déjà en cours, nous invitons à ne pas en créer une nouvelle.

Pour plus d'informations, n'hésitez pas également à consulter notre Centre d'aide.

Votre Service Clients leboncoin

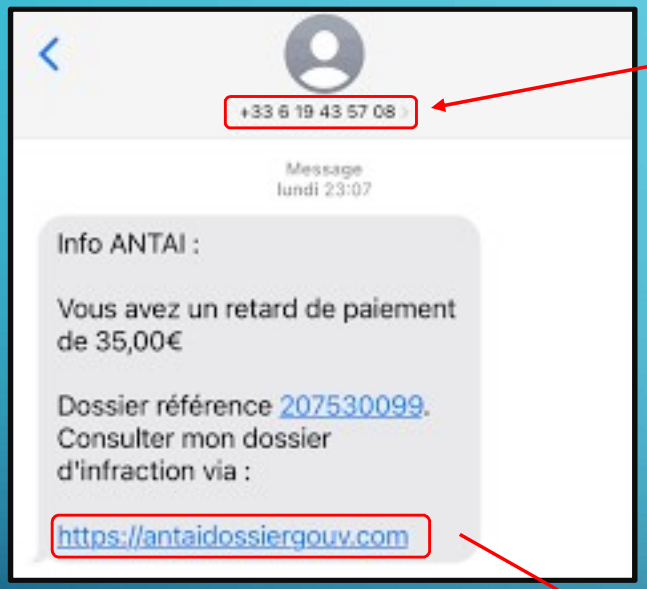
Cet e-mail provient de Leboncoin.

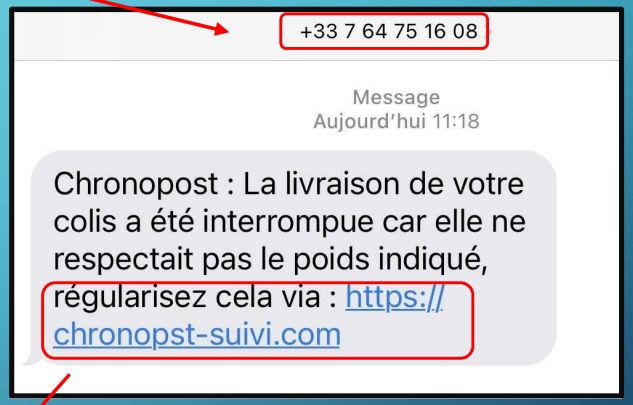
LES MAILS


De : leboncoin <no.reply@leboncoin.fr>
Date: jeu. 23 mars 2023 à 15:15
Subject: Confirmation de changement de mot de passe
To: <p @gmail.com>
leboncoin
Changement de mot de passe
Bonjour,
Votre mot de passe a été changé le 23 mars 2023 à 15h15.
Localisation : à proximité de France (Europe)
Appareil : iOS, Apple iPhone
S'il s'agit de vous, vous pouvez ignorer cet email. Dans le cas contraire, nous vous invitons à réinitialiser votre mot de passe au plus vite afin de sécuriser votre compte.
Pour en savoir plus sur la sécurité de votre compte, rendez-vous sur l'assistance leboncoin.
Merci de votre confiance et à très bientôt.
L'équipe leboncoin
https://www.leboncoin.fr
leboncoin

LES SMS

Utilisation d'un numéro personnel …





Lien vers des sites frauduleux

Les sites officiels se terminent par : «exemple.gouv.fr »!

LES BONS REFLEXE EN CAS DE DOUTE :

LES MAILS

1°) Je Vérifie l'adresse e-mail exacte de l'expéditeur (…….@……..)

2°) Je Vérifie la cohérence entre l'objet et le contenu du mail

3°) Je vérifie les adresses des liens en passant la souris dessus (sans cliquer)

BLOQUER L'EXPEDITEUR !

LES SMS

1°) Je vérifie l'expéditeur, si nécessaire en cherchant sur internet.

2°) Je réfléchi au contexte du sms (ex : Sms qui informe de la réception d'un colis alors que vous n'avez rien commandé

3°) Je ne clique pas dans les liens du sms

4°) Je ne donne jamais d'identifiant ou mot de passe

5°) Si nécessaire, je prends contacts directement avec le service client de l'entreprise concernée (ex : appeler directement edf, demander de l'aider sur le site officiel,…)

LES APPELS TELEPHONIQUES

1°) Je ne réponds pas, les personnes laissent un message
2°) Je bloque le numéro appelant
3°) JE téléphone au service client concerné si besoin (ex : banque)

RÉACTIONS - TÉMOIGNAGES

ET VOUS ?

CA VOUS EST ARRIVÉ ?

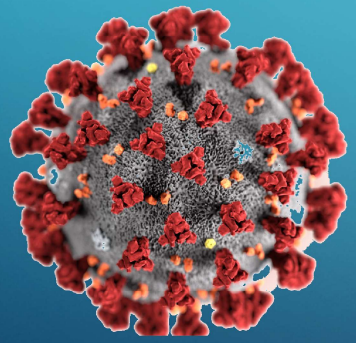
LES MAUVAIS LIENS

https://www.citratubindo.com/clang?lang=en&url=//bit%2e%f0%9d%91%99y/3ys0cbn
Cliquez ou appuyez pour suivre le lien.
re demande **N°28956802**.

Citratubindo1.url

Chronopost : La livraison de votre colis a été interrompue car elle ne respectait pas le poids indiqué, régularisez cela via : https://chronopst-suivi.com

Malwares, programmes malveillant



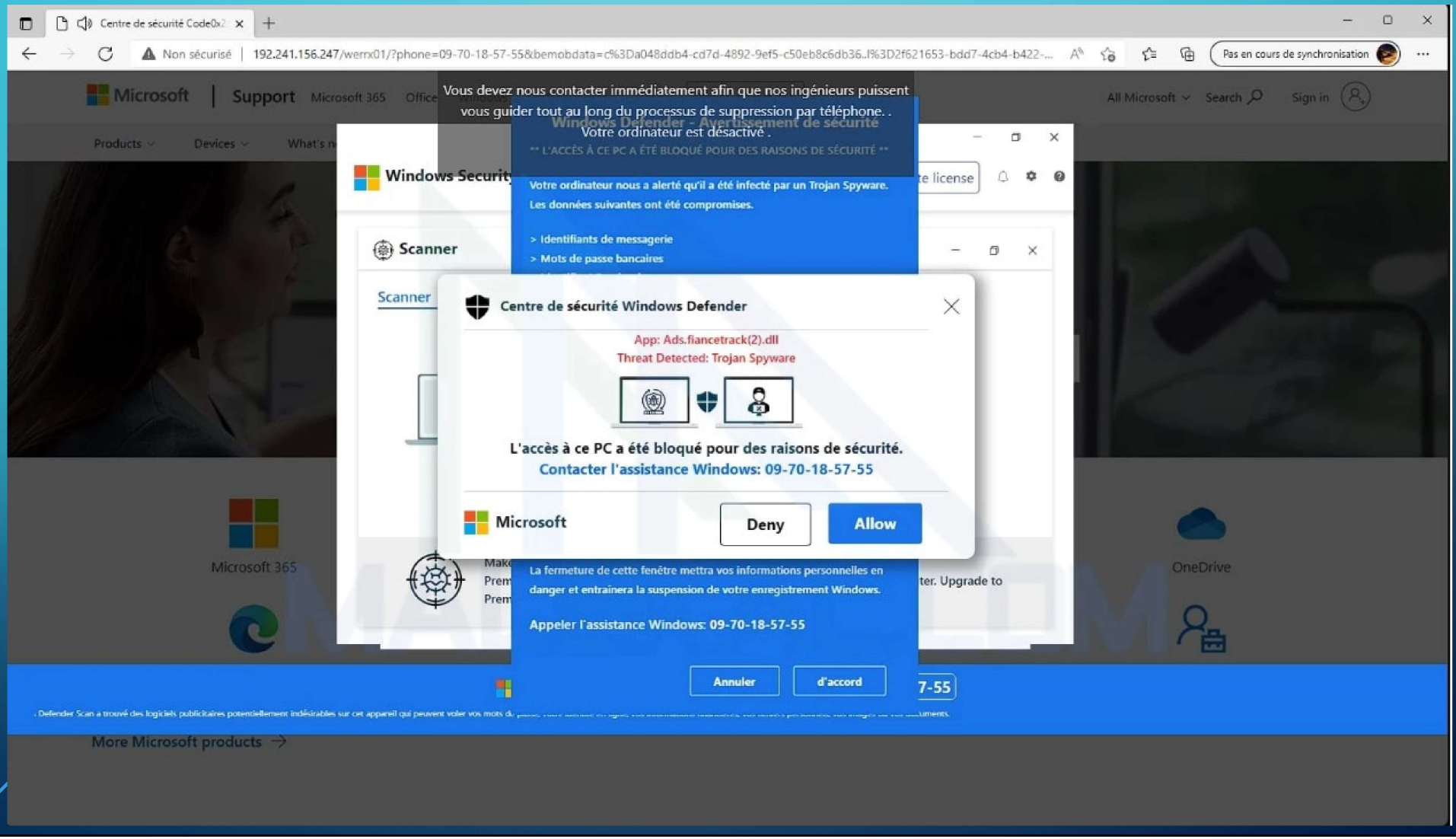
Virus

Ransomware

Arnaques et fraudes

Phishing (hameçonnage) :
C'est vous le poisson !

LES MAUVAIS LIENS : L'ALERTE AU FAUX SUPPORT TECHNIQUE



1min58.url

L'ALERTE AU FAUX SUPPORT TECHNIQUE

PREVENIR

1°) Garder son système d'exploitation à jour

2°) Garder son Antivirus à jour

3°) Installer un bloqueur de publicité (adblock)

1°) Garder son sang froid malgré le bruit et la pression que vous pouvez ressentir

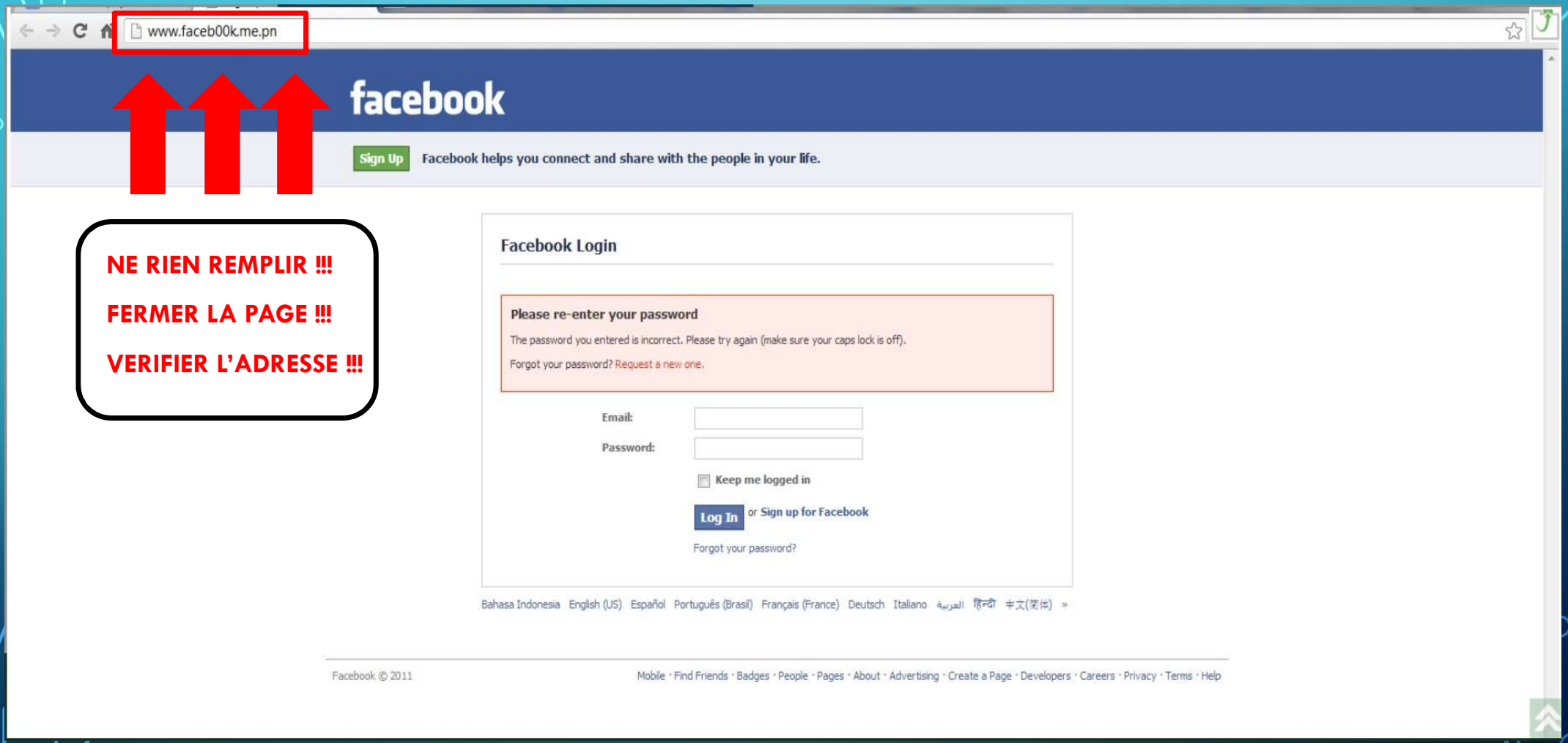
2°) Appuyer simultanément sur :
Ctrl + Alt + Suprr

3°) Sélectionner :
Gestionnaire de tâches

4°) Chercher votre navigateur (dans lequel la fausse alerte s'est ouverte)
Positionner la souris sur le nom du navigateur puis faite « clic droit »
Puis sélectionner « Fin de tâche »

GUERIR

LES MAUVAIS LIENS : LE PHISHING (FAUX SITE WEB)



NE RIEN REMPLIR !!!

FERMER LA PAGE !!!

VERIFIER L'ADRESSE !!!

SURFEZ EN SÉCURITE !

PARTIE 2 : JE ME SUIS FAIT PIRATÉ, QUE FAIRE ?

ON A PIRATE UN COMPTE (MAIL OU SITE)

COMMENT EST-CE ARRIVE ?

J'ai été par erreur sur un faux site où j'ai rentré mes informations de connexion

Phishing, arnaque

Un logiciel espion est installé sur mon appareil sans que je le sache

Infection virale, piratage

Le site web contenant mes informations de connexions a été piraté

Hacking/Piratage de site web

QUE FAIRE ?

Je change tous les mots de passes liés à l'identifiant de connexion

Phishing, arnaque

Je mets à jour l'antivirus, je lance un scan antivirus de mon appareil, je met à jour windows

Infection virale, piratage

Je change tous les mots de passes liés à l'identifiant de connexion lorsqu'ils sont identiques

Hacking/Piratage de site web

EXEMPLE DE FRAUDE TELEPHONIQUE

- La fraude au service bancaire : https://www.youtube.com/watch?v=urQ1QMyapAk

  De 46:50 à 51:00

Ce qu'il faut faire :

1°) Garder son sang froid et son bon sens
2°) Se renseigner ailleurs et conforter l'information
3°) S'abstenir d'agir, prendre son temps
4°) Ne jamais donner ses codes d'accès par téléphone, ne jamais rien valider sur le téléphone si vous n'en êtes pas à l'origine, même si on vous le demande !

JE PENSE ETRE VICTIME D'UNE FRAUDE BANCAIRE

COMMENT EST-CE ARRIVE ?

J'ai répondu à un appel téléphonique ou j'ai donné mes codes.
J'ai validé une notification sur mon téléphone alors que je n'en étais pas à l'origine.

Un logiciel espion est installé sur mon appareil sans que je le sache et récupère mes informations tapées.

Le site web avec lequel j'ai fais une transaction a été piraté, j'ai pu constater des anomalies sur le relevé de compte bancaire

Faites preuve de vigilance

Garder ses systèmes bien à jour (OS, Antivirus)

Inévitable

QUE FAIRE ?

1°) JE CONTACTE TOUT DE SUITE MA BANQUE !!

2°) Je fais opposition à ma carte bancaire

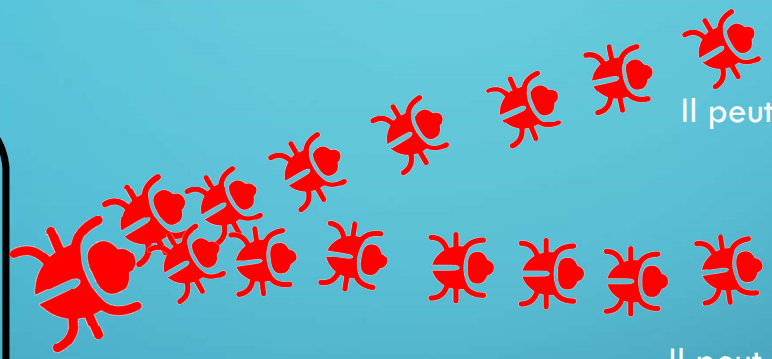
3°) Je porte plainte et fait la déclaration de fraude en ligne THESEE/PERCEVAL

LES MOTS DE PASSES

France Connect

Identifiant : rodolphe@gmail.com
Mot de passe : a1b2c3d4

Le pirate veut vos informations France Connect pour y récupérer des informations.



Ex : Ransomware, exploitation des failles de sécurité des serveurs, des pages web, piratage des BDD

Il peut pirater le site de l'administration

Ex : Virus, Keylogger, logiciel tiers, par téléchargement de pieces jointes, ou accès à des pages web infectées

Il peut pirater mon ordinateur

Appelée « attaque brute force »

Il peut essayer de deviner le mot de passe.

LES MOTS DE PASSES

Temps requis pour trouver un mot de passe par attaque « brute force »

NOMBRE DE CARACTÈRES	CHIFFRES SEULEMENT	LETTRES MINUSCULES	LETTRES MINUSCULES ET MAJUSCULES	CHIFFRES, LETTRES MINUSCULES ET MAJUSCULES	SYMBOLES, CHIFFRES, LETTRES MINUSCULES ET MAJUSCULES
4	Instantanément	Instantanément	Instantanément	Instantanément	Instantanément
5	Instantanément	Instantanément	Instantanément	Instantanément	Instantanément
6	Instantanément	Instantanément	Instantanément	1 seconde	5 secondes
7	Instantanément	Instantanément	25 secondes	1 minute	6 minutes
8	Instantanément	5 secondes	22 minutes	1 heure	8 heures
9	Instantanément	2 minutes	19 heures	3 jours	3 semaines
10	Instantanément	58 minutes	1 mois	7 mois	5 ans
11	2 secondes	1 jour	5 ans	41 ans	400 ans
12	25 secondes	3 semaines	300 ans	2000 ans	34k ans
13	4 minutes	1 an	16k années	100k ans	2M ans
14	41 minutes	51 ans	800k années	9M ans	200M ans
15	6 heures	1k ans	43M ans	600M ans	15G ans
16	2 jours	34k ans	2G ans	37G ans	1T ans
17	4 semaines	800k ans	100G ans	2T ans	93T ans
18	9 mois	23M ans	2T ans	100T ans	7(10^{48}) ans

= 1h !!!

France Connect

Identifiant : rodolphe@gmail.com
Mot de passe : a1b2c3d4

8 caractères
Minuscules
Chiffres

Préférez des mots de passes de 12 caractères minimum, avec des majuscule, minuscules, chiffres et caractères spéciaux !

LES MOTS DE PASSES

Limiter les risques

QUELS SONT LES COMPTES IMPACTES

France Connect

Identifiant : rodolphe@gmail.com
Mot de passe : a1b2c3d4

Compte CAF

Identifiant : rodolphe@gmail.com
Mot de passe : Caf2023Rodolphe

Compte Facebook

Identifiant : rodolphe@gmail.com
Mot de passe : a1b2c3d4

Compte Instagram

Identifiant : lafritedu@gmail.com
Mot de passe : a1b2c3d4

Compte Leboncoin

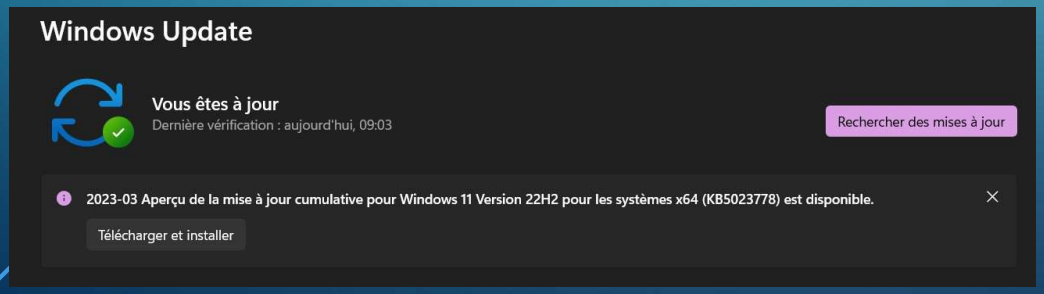
Identifiant : rodolphe@gmail.com
Mot de passe : Leboncoin2023

Changer tous les mots de passes lorsque identifiant et mdp identique + compte connectés

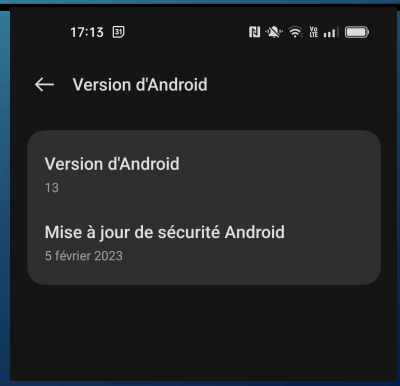
MAIS COMMENT JE SAIS SI JE SUIS EN SECURITÉ ?

QUESTION 1 : MES APPAREILS ONT-ILS LEUR SYSTÈME A JOUR ?

Pour savoir cliquer sur :
- Windows (le menu démarrer) en bas à gauche
- Cliquez ensuite sur paramètre (la roue dentée)
- Choisissez ensuite « Sécurité »
- Localisez la mention tout en haut qui indique si l'ordinateur est à jour :



Pour savoir aller dans :
- Paramètres
- A propos de l'appareil / Mises à jour
- Version d'Android
- Puis regarder les mentions de sécurité Android



MAIS COMMENT JE SAIS SI JE SUIS EN SECURITÉ ?

QUESTION 2 : AIS-JE BESOIN D'AUTRE CHOSE ?

OUI !

NON

ANTIVIRUS

norton

Avast One

Facultatif mais commun aux deux : Bloqueur de publicité

ABP

EN RÉSUMÉ

1°) JE FAIS LES MISE À JOURS DE MON MATÉRIEL ET ANITIVIRUS SUR ORDINATEUR

2°) JE RESTE VIGILANT ET « SUSPICIEUX », JE RECROISE LES INFORMATIONS

3°) JE DEMANDE CONSEIL (PROCHES, PROFESSIONNELS)