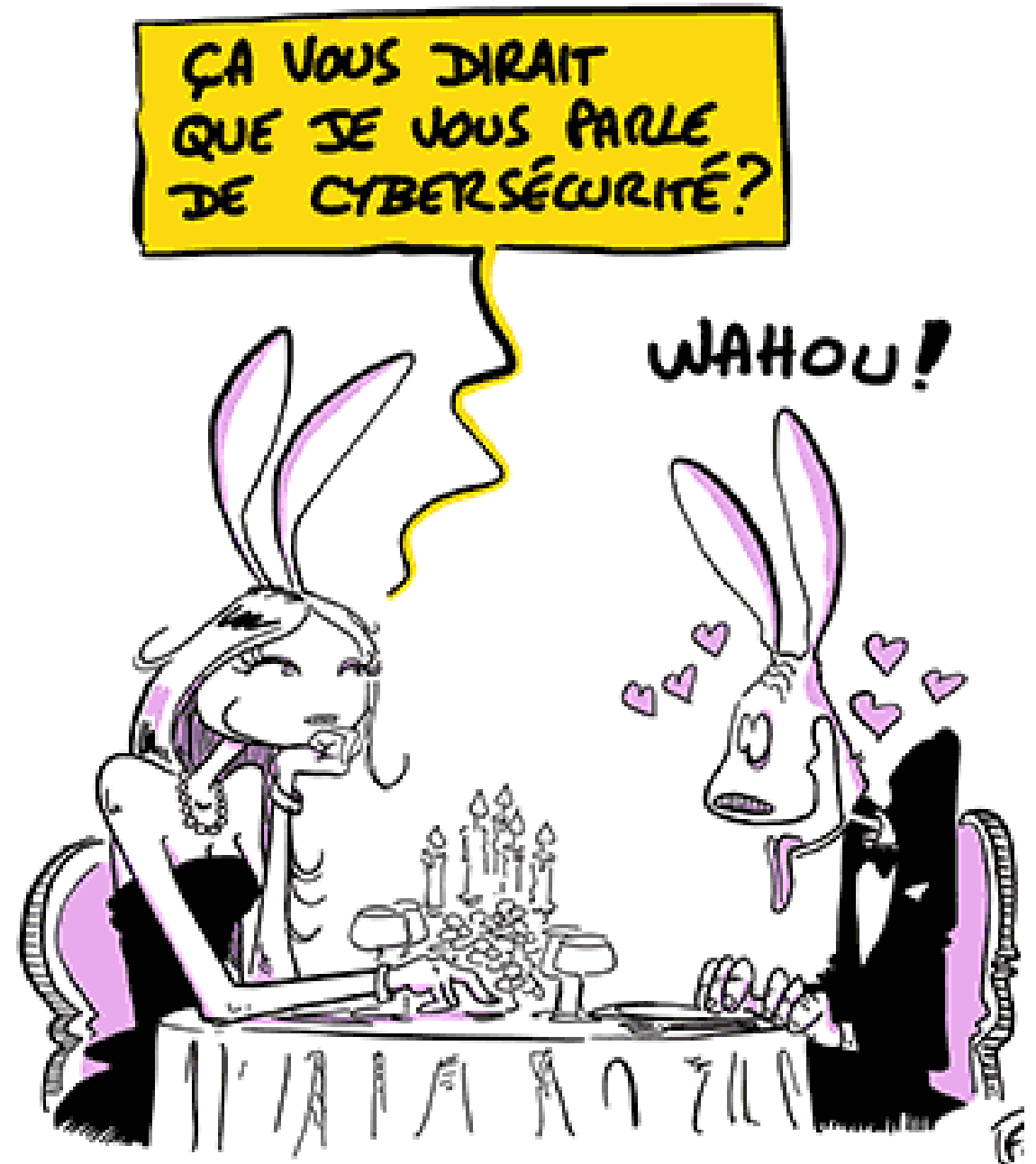


Cybermois

Les Cyber rencontres





...
TU N'UTILISES
QUAND MÊME PAS
LA MÊME CLÉ
POUR TOUTES
LES SERRURES ?

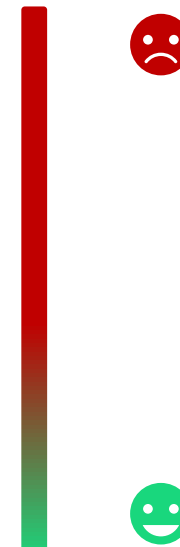
**LES MOTS DE PASSE
C'EST COMME LES
CLÉS : C'EST MIEUX
D'EN AVOIR PLUSIEURS**

CHAPITRE 3

Les mots de passe, comment
vivre avec ?

L'importance d'avoir un mot de passe robuste

Type de mot de passe	Temps machine pour trouver un MdP
Un mot facile à saisir, ex: <i>azerty</i> ou <i>654321</i>	2 millisecondes
Le nom de votre chien, ex : <i>rex</i>	15 millisecondes
Un nom commun, ex : <i>novembre</i>	23 millisecondes
Un mot avec une substitution triviale de lettre par chiffre, ex: <i>L4sVeg4s</i>	920 millisecondes
Une suite de chiffres usuelle pour vous : <i>une date</i> ou <i>un code postal</i>	2 secondes
Une suite de caractères au hasard : <i>p%9y#k&yFm?</i>	90 millions de siècles
4 mots choisis au hasard : <i>location immeuble jardin parking</i>	3 700 milliards de siècles



- ➔ **Eviter** d'y inclure : votre nom, prénom, code postal, date et année de naissance
- ➔ **Privilégier l'utilisation de phrases secrètes** au lieu de simples mots de passe
 - **Exemple 1** : CeciEst1MotdeP4sseDeTest!
 - **Exemple 2** : JeMange5fruits&légumes/jour

Mot de passe – Les bonnes pratiques

- 1 On évite la suite numérique, même à 10 chiffres ! : 0123456789
- 2 Sur mobile aussi on muscle son mot de passe (6 caractères min.) avec ou sans biométrie et on met un verrouillage auto
- 3 Dans le doute, on ne s'abstient pas, on change de MdP
- 4 On évite le recyclage ! On s'interdit d'utiliser le même mot de passe pour tous nos comptes
- 5 Un mot de passe, c'est comme sa brosse à dent, c'est personnel !
- 6 Activer la double authentification, pour être doublement confiant
- 7 Quand on a plein de lingots (ou de Bitcoins), on les met au coffre, les MdP c'est pareil

PFFF,
CHANGER DE
MOT DE PASSE ...
JE METS QUOI
POUR REMPLACER
GEORGETTE ?

... PAS
DOUÉ LE GARS,
IL SUFFIT DE METTRE :
GEORGETTE07_EST_LE_
CERVEAU_DU_COUPLE

...
AU HASARD

LA PHRASE DE PASSE :
**C'EST LOURD MAIS
ÇA MARCHE**



WWW.CYBERMOIS.FR
OCTOBRE 2021

CHAPITRE 4

Gestionnaire de mot de passe

Gestionnaire de mots de passe



Pourquoi faire ?

- **Stockez** tous **vos mots de passe professionnels** à un **seul endroit** et ne retenez qu'un seul mot de passe

Les avantages

- Ne plus **mémoriser** tous vos mots de passe
- Possibilité de générer des **mots de passe très compliqués**
- Garder un **inventaire** de toutes vos **identités en ligne**
- Plus besoin de **saisir** vos mots de passe

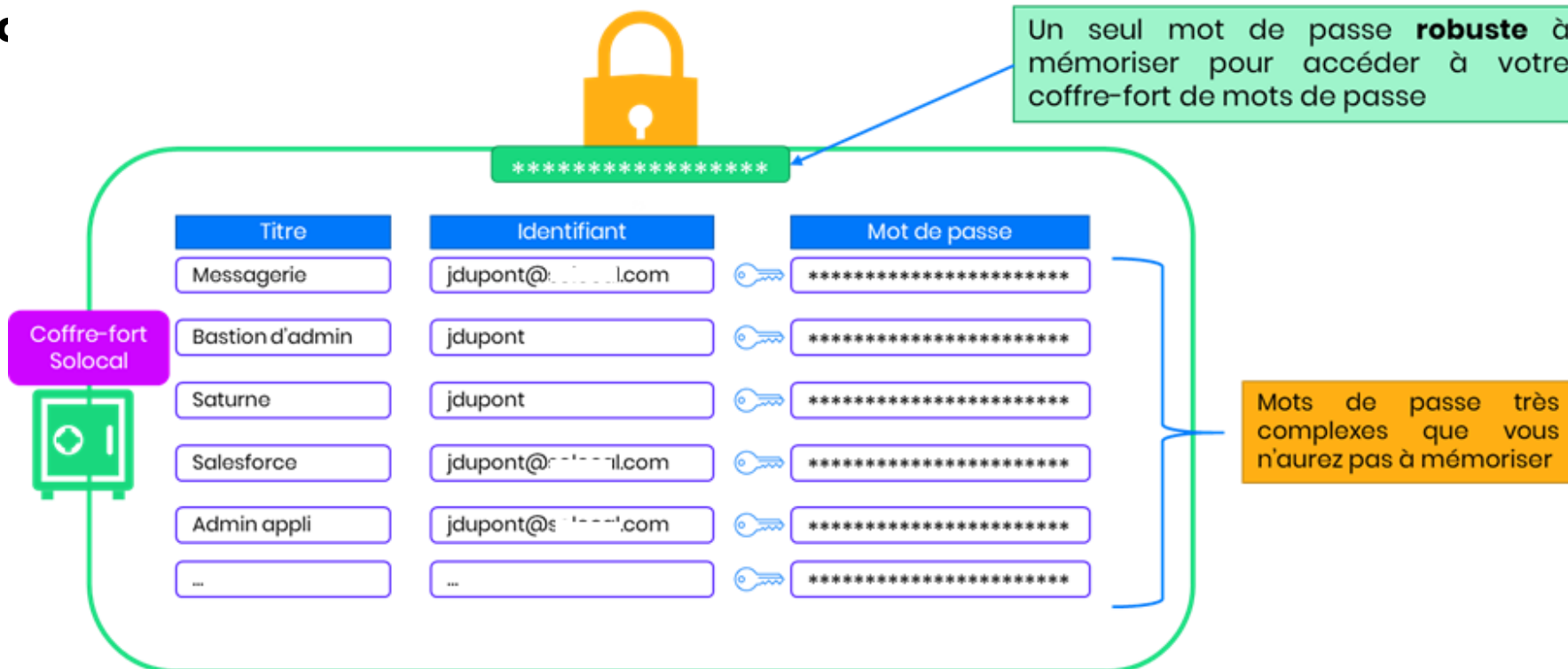


Procédure bientôt disponible dans l'espace « Sécurité de l'Information » sur l'intranet

Gestionnaire de mot de passe

Cc

Un seul mot de passe **robuste** à mémoriser pour accéder à votre coffre-fort de mots de passe



Recommandation de l'outil KeePass :

- Gratuit
- Certifié par l'ANSSI
- Procédure d'utilisation bientôt sur l'intranet



Comment ça marche ?

Pour saisir son mot de passe sur son compte applicatif, M. Dupont procède comme suit :

- Il ouvre son coffre fort de mot de passe
- Clique droit -> Copie du mot de passe nécessaire dans son coffre-fort
- Colle le mot de passe au niveau du champ de l'application utilisée

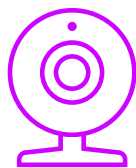
Privilégier l'utilisation de **deux coffres-forts distincts** entre usage **pro** et **perso**

Passwordless – Une évolution logique



→ **Ne plus avoir à utiliser des mots de passe** et être plus sécurisé

→ **Reconnaissance faciale :**



La caméra de l'ordinateur/smartphone est capable de vous reconnaître pour être déverrouillé et pour vous connecter à divers services

→ **Empreinte digitale :**

Si votre terminal dispose d'un lecteur d'empreintes, un simple toucher vous permettra de vous authentifier sur votre session



→ **Code** associé à votre ordinateur



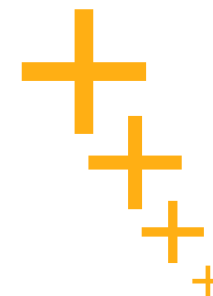
Les avantages

C'est (très) rapide !

Cela répond à de grands standards de sécurité (NIST 800-63)




Vous devenez invincibles aux attaques par phishing

Vous n'aurez plus à mémoriser plusieurs mots de passe



Disponible chez ENTREPRISE sur certains portables / pilote en cours

Passwordless – Windows Hello for Business

- Les grands du numérique (Google, Microsoft, Apple) sont alignés sur l'adoption de l'authentification passwordless qui permettrait une réduction drastique du risque de vol de mot de passe.
- Cette mesure de protection serait à mettre en place en parallèle de l'authentification forte (utilisation du double facteur d'authentification).
- **Chez ENTREPRISE, l'approche passwordless se fera avec « Microsoft Hello for Business »** qui se base sur :
 - Un PIN défini par l'utilisateur 
 - L'empreinte digitale (*) 
 - La reconnaissance faciale (*) 

(*) : Uniquement sur les appareils supportés

PRESS RELEASE

May 5, 2022

Apple, Google, and Microsoft commit to expanded support for FIDO standard to accelerate availability of passwordless sign-ins

Faster, easier, and more secure sign-ins will be available to consumers across leading devices and platforms



MOUNTAIN VIEW, CALIFORNIA – In a joint effort to make the web more secure and usable for all, Apple, Google, and Microsoft today announced plans to expand support for a common passwordless sign-in standard created by the FIDO Alliance and the World Wide Web Consortium. The new capability will allow websites and apps to offer consistent, secure, and easy passwordless sign-ins to consumers across devices and platforms.

<https://www.apple.com/newsroom/2022/05/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard/>



CYBERPIRATES :
NE LEUR OUVREZ
PAS LA VOIE



WWW.CYBERMOIS.FR
OCTOBRE 2021

CHAPITRE 5

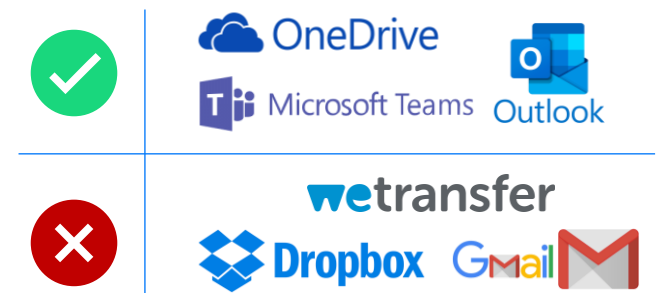
Les bonnes pratiques

Filtrage des fichiers manipulés

→ Depuis l'attaque de février, certains types de fichiers sont bloqués systématiquement lors d'envoi de mail ou téléchargement comme les anciennes extensions Office :



- Privilégiez l'échange de fichiers par des solutions fournies par l'entreprise comme **Outlook/OneDrive** et la mise en place de **groupes Teams temporaires**
- N'utilisez pas des solutions telles que **Dropbox** ou **WeTransfer** et l'utilisation de **boîtes de messagerie personnelles** pour des besoins professionnels



Un doute, une question ? => ?

Les bonnes pratiques en entreprise



- Prenez l'habitude de **verrouiller** votre ordinateur au cours de chaque absence (même pour un bref instant)



- Synchroniser continuellement les **documents importants et critiques** sur OneDrive

- N'utilisez pas des ordinateurs **à disposition** dans les **cybercafés ou en libre service**

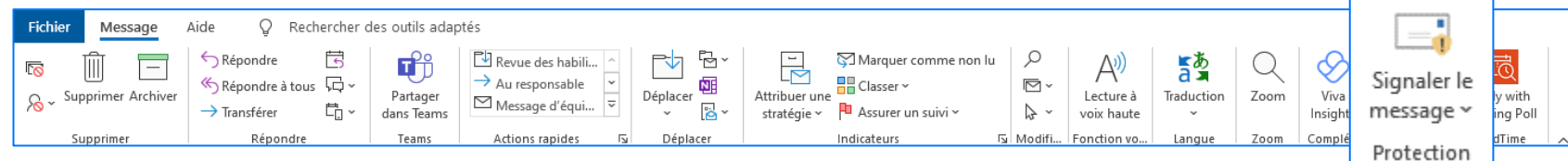


- Utilisez votre adresse électronique ENTREPRISE **uniquement** pour un usage professionnel

- Evitez l'utilisation de **clés USB** ou de **disques de stockage externes**



- **Installez les mises à jour** dès réception de la notification de leur disponibilité sur votre poste de travail



Un doute, une question ? ==> ?

Les attaques par phishing



- Malgré les multiples briques de protection mises en place, **certaines attaques arrivent toujours à passer** pour atteindre vos boîtes de messagerie.

33 millions d'euros, une arnaque au président record en France

Sécurité : *Un promoteur immobilier parisien a été victime d'une arnaque au président basée sur des e-mails contrefaits. Les escrocs sont parvenus à extorquer 33 millions d'euros à la société victime.*



Par Louis Adam | Mardi 04 Janvier 2022

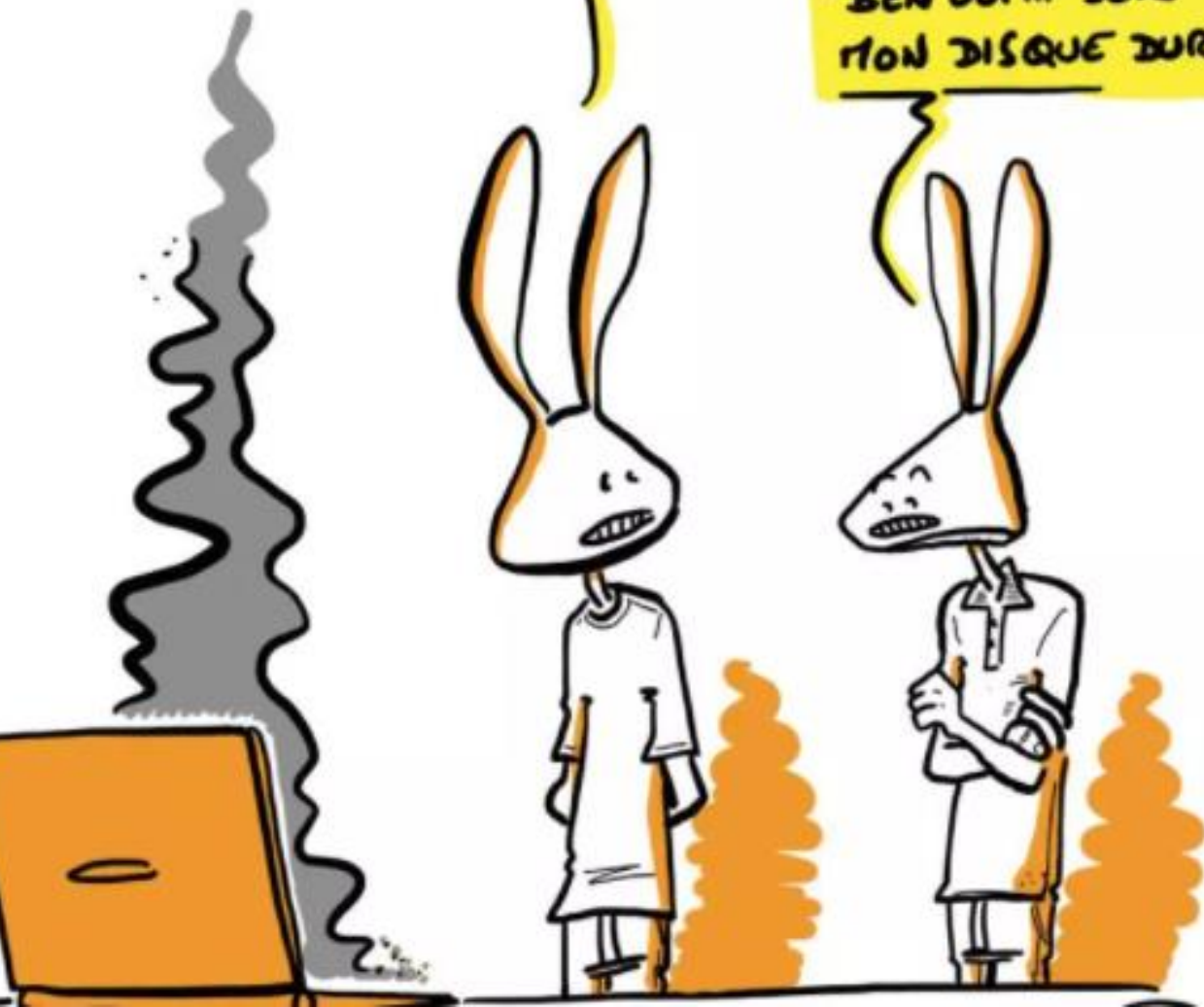
<https://www.zdnet.fr/actualites/33-millions-d-euros-une-arnaque-au-president-record-en-france-39934933.htm>

- **La solution :** A travers cette session ainsi que les **communications/formations cybersécurité**, nous visons à vous apporter quelques réflexes qui pourraient vous permettre d'éviter de vous faire piéger.

Un doute, une question ? => ?

FLÛTE... T'AVAIS FAIT
UNE SAUVEGARDE DE
TON DISQUE DUR ?

BEN OUI... SUR
MON DISQUE DUR...



Exercice

Phishing Game

Exemples de mail

Phishing ou légitime?



Phishing

De : Messagerie Outlook <outlook-noreply@micro-soft.com>

Envoyé : jeudi 1 juillet 2021 10:31

À : [redacted] <[\[redacted\]@l.com](mailto:[redacted]@l.com)>

Objet : Messages non délivrés



[redacted], vous avez des messages en suspens.

Message pour : [redacted]@[\[redacted\]@l.com](mailto:[redacted]@l.com)

Pour lire vos message, veuillez suivre le lien ci-dessous :

[Lire les messages](#)

Tous les messages en suspens vont être automatiquement supprimés après 48 heures



[Privacy Statement](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052



<https://sharepointen.com/dkim/ljgzdf...>

Exemples de mail

Phishing ou légitime?



Légitime

De : quarantine@messaging.microsoft.com <quarantine@messaging.microsoft.com>
Envoyé : mardi 5 octobre 2021 03:16
À : [redacted] <[redacted]@[redacted].com>
Objet : Notification de courrier indésirable : nouveaux messages 8



Examiner ces messages

8 les messages sont conservés afin de vous permettre de passer en revue à **05/10/2021 00:00:00 (UTC)** .

Réviser-les dans les **30 jours de la date de réception** by going to the [Page de quarantaine](#) dans le centre de conformité & de sécurité.

Original URL:
<https://protection.office.com/quarantine>
Click or tap to follow link.

Bloquer l'expéditeur

Diffuser

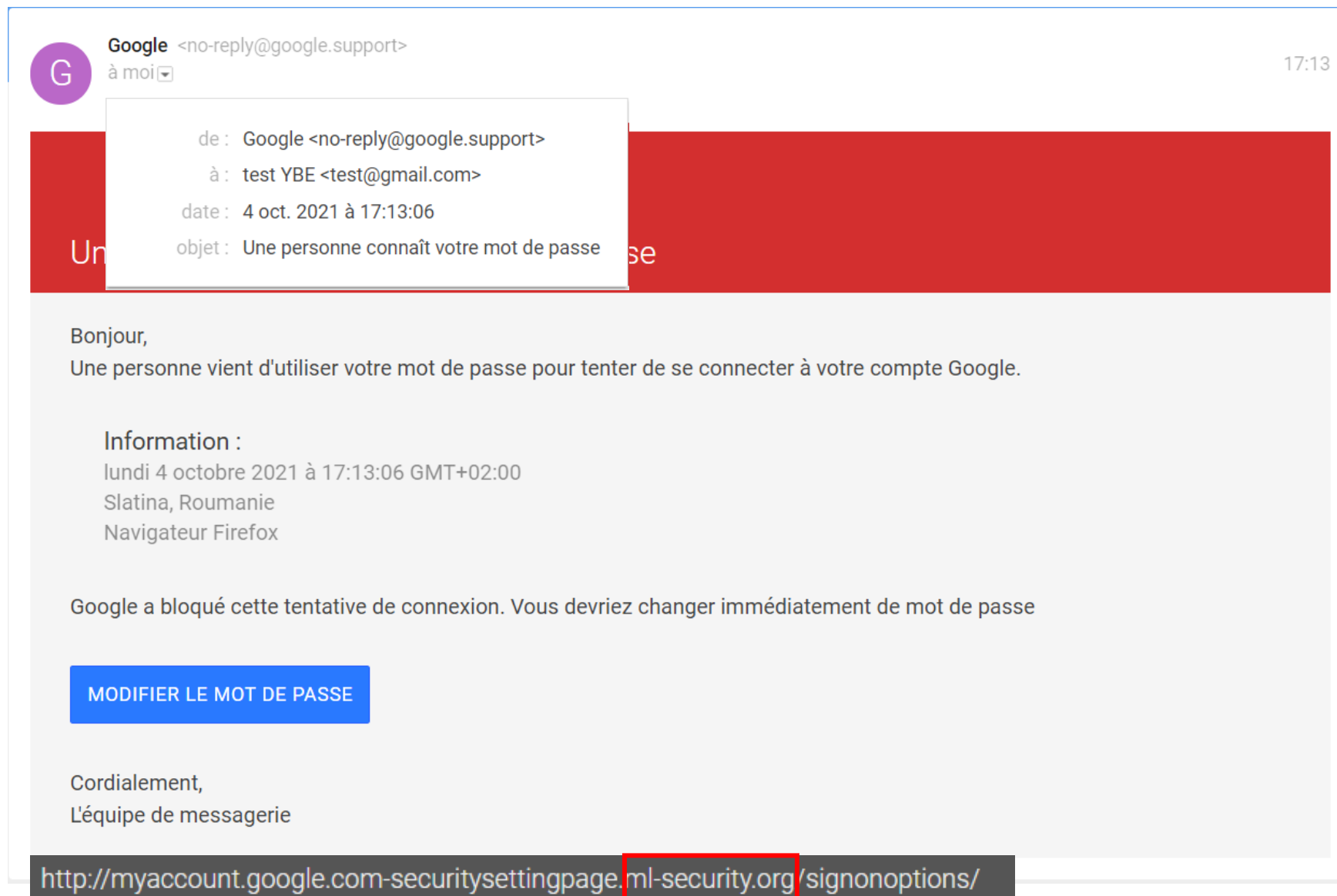
Réviser

Exemples de mail

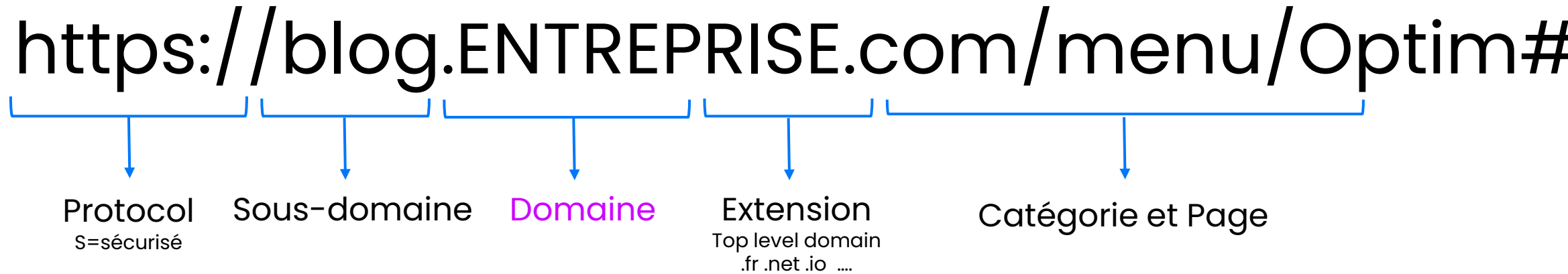
Phishing ou légitime?



Phishing



Explication d'une URL



Exemples de mail

Phishing ou légitime?



Phishing



Luke Johnson <luke.json8000@gmail.com>

à moi

17:25

de : Luke Johnson <luke.json8000@gmail.com>

à : test YBE <hello@mail.com>

date : 4 oct. 2021 à 17:25:44

objet : Budget départemental 2021

document suivant :

 Budget département 2021.docx



Bonjour. Voici le document demandé. N'hésitez pas à me contacter si vous avez besoin d'autre chose !

Ouvrir dans Docs

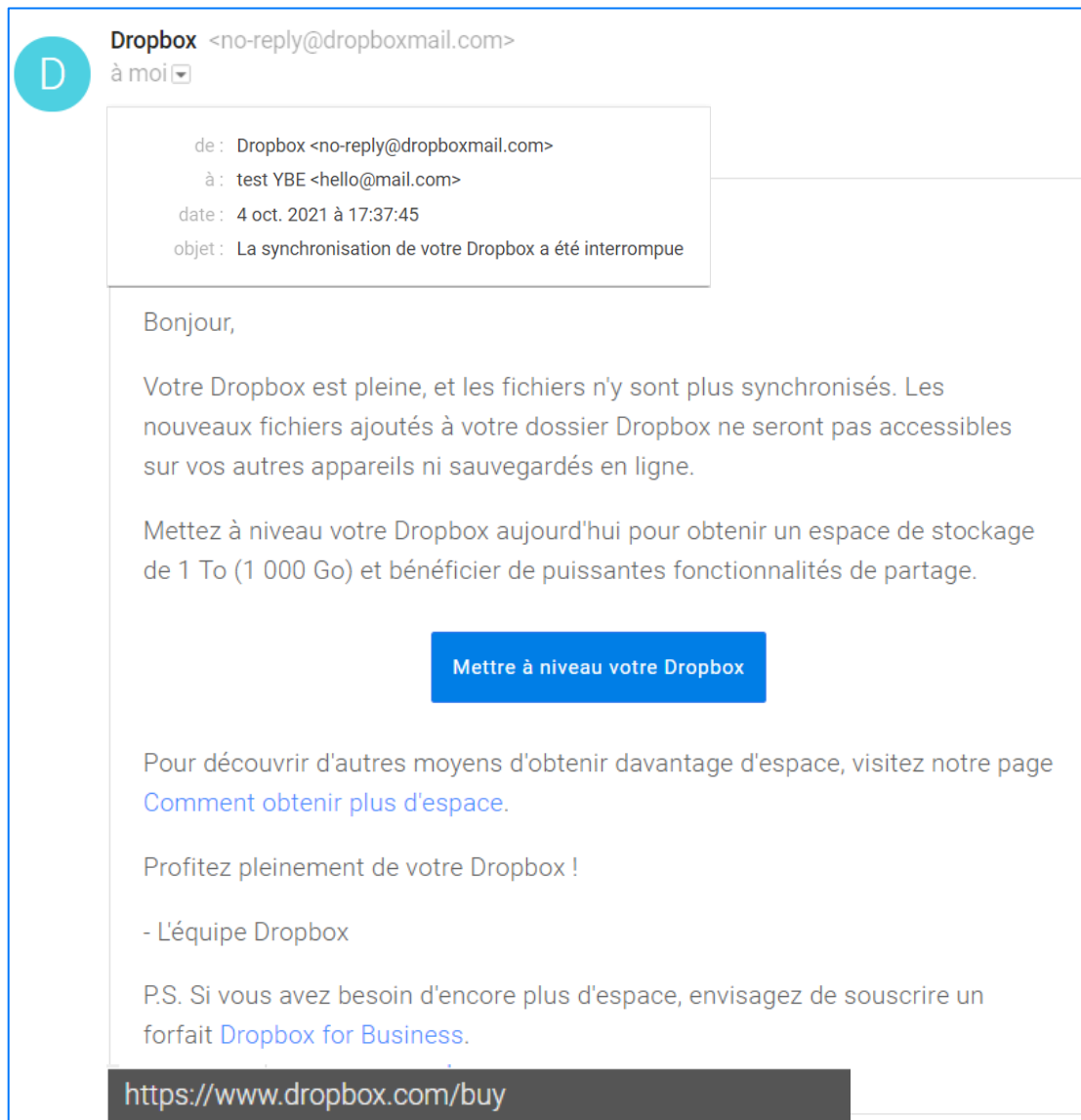
<http://drive-google.com/luke.johnson>

Exemples de mail

Phishing ou légitime?



Légitime



Exemples de mail

Phishing ou légitime?



Phishing

From: Credit_agricole.fr <Agricol@like4card.com>

Sent on: Friday, June 17, 2022 5:12:42 PM

To: [redacted].fr

Subject: (2) message important

Vous ne recevez pas souvent de courriers de la part de agricol@like4card.com. [Découvrez pourquoi cela est important](#)

(1) message important..! Si ce message ne s'affiche pas correctement, [Banque & Assurances](#)
Pour vous désabonner de la newsletter Femme Actuelle Quotidienne [Crédit Agricole](#)

Crédit Agricole

Cher Client,

NOTIFICATION : CONSEILLER BANCAIRE CREDIT AGRICOL.

Vous avez **(1) message important** sur votre boîte de messagerie sécurisée.

Pour le consulter veuillez cliquer sur le lien ci-dessous:

- [ACCÉDER À MES COMPTES](#)

Merci de nous soutenir dans cette démarche responsable.

Très cordialement.

©Crédit Agricole Message de Sécurité.

www.mgu.edu.in/ssh1.php

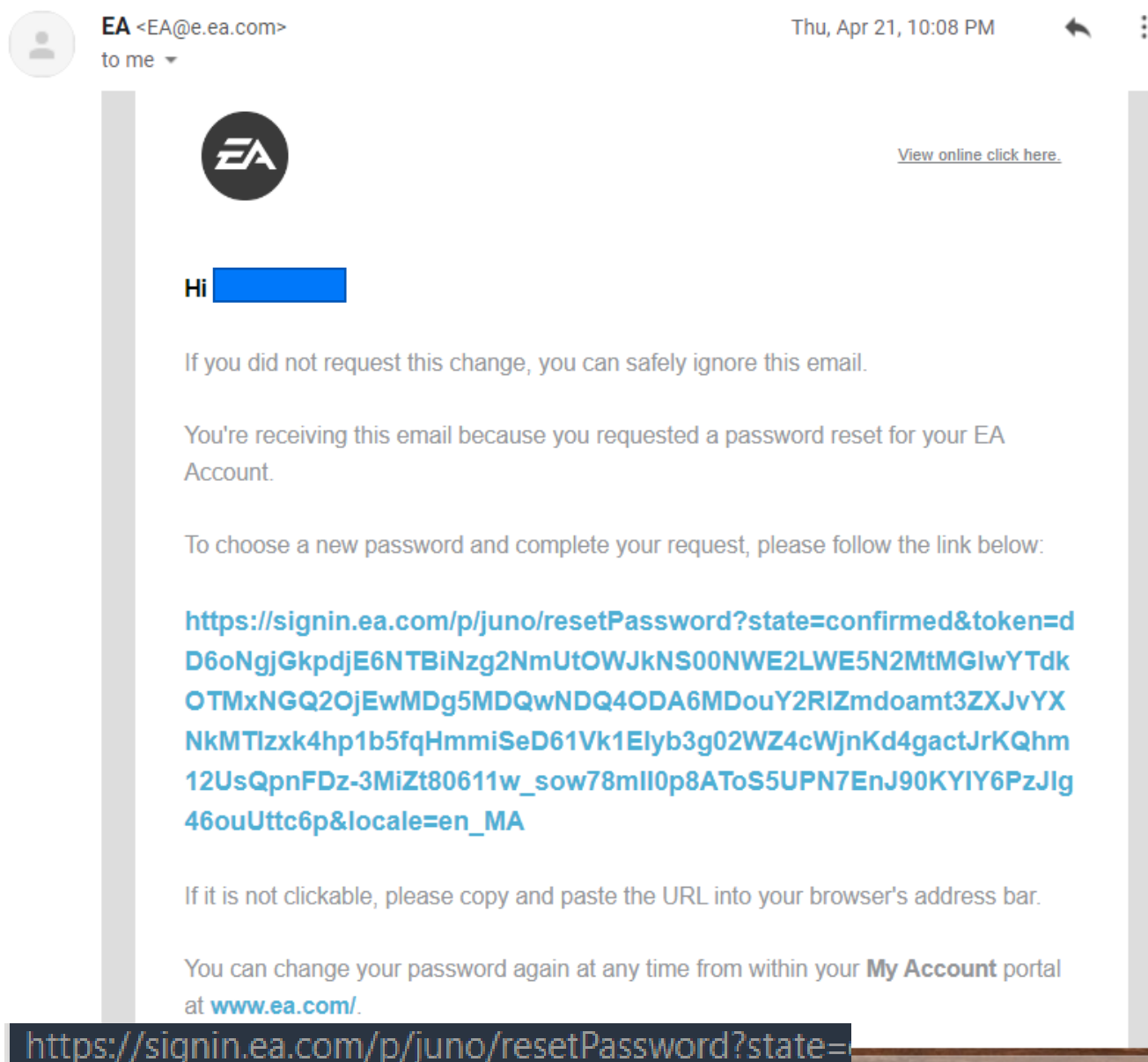


Exemples de mail

Phishing ou légitime?



Légitime



Exemples de mail


Phishing ou légitime?

Netflix <info@netflix.com> [Unsubscribe](#)
to [REDACTED]



Phishing

NETFLIX

 Your account is on hold.

Please update your payment details

Dear User,

We're having some trouble with your current billing information. Would you like to retry running your card again? Your card information is below.

RETRY PAYMENT

<https://account.netflix.com.account.websec-websayt.com>

Quiz

Question 2

- **Parmi les mots de passe suivants, lequel est le plus sécurisé ?**
 - ☐ Caroline
 - ☐ 24031988
 - ☐ UV67!rv@O
 - ☐ je pars au travail à 9H par train

Question 3

- **Parmi les types de fichiers suivants, quels sont ceux qui sont susceptibles de contenir des virus?**
 - ☐ Zip
 - ☐ exe
 - ☐ jpg
 - ☐ xls
 - ☐ docx

Question 4

- **Parmi les affirmations suivantes à propos d'un virus informatique, lesquelles sont vraies ?**
 - ☐ Il ne pourra jamais s'installer si l'ordinateur possède un anti-virus
 - ☐ Il peut utiliser le réseau pour se propager
 - ☐ Il ne s'attrape que par la messagerie électronique
 - ☐ Il détruit systématiquement tous les fichiers du disque dur
 - ☐ Il peut prendre le contrôle de l'ordinateur

Question 5

- **Lorsque je suis en déplacement à l'extérieur de l'entreprise, comment puis-je continuer à participer à la sécurité de mon entreprise (choisissez la réponse la plus précise) ?**
 - ☐ En désactivant l'anti-virus, pour ne pas consommer
 - ☐ En installant un antivirus plus efficace
 - ☐ En réalisant moi-même des « scan antivirus » sur mon poste
 - ☐ En utilisant mon poste de travail à l'abri des regards indiscrets, et en n'installant aucun logiciel non autorisé sur mon poste

Question 6

- **Vous recevez un e-mail en anglais d'une personne que vous ne connaissez pas...**
 - ☐ Vous le lisez, vous n'ouvrez pas la pièce jointe mais vous cliquez sur un lien
 - ☐ Vous le lisez et vous ouvrez la pièce jointe (y'a pas de risque!)
 - ☐ Vous le supprimez directement
 - ☐ Vous le signaler immédiatement à l'équipe sécurité ou via le plugin Outlook