Bienvenue chez abicom

Imagine IT

Entreprise de Services du Numérique

Imaginons ensemble
la meilleure solution technologique
pour **votre système d'information**
et de **communication**

abicom
Imagine IT

30 millions
Chiffre d'affaires

1 000
Clients fidèles

125
Collaborateurs
75% technique

4 Business Unit

abicom Modern IT
abicom Human IT
abicom Connect IT
abicom Secure IT

75
certifications
techniques

3 CERTIFICATIONS QUALITÉ
ISO 9001 – 27 001 - HDS

MALVEILLANCE & CYBERSÉCURITÉ

Session de sensibilisation

Centre de Gestion de la Fonction Publique Territoriale du Puy-de-Dôme (CDG 63)

Juin 2023

cdg 63 Centre de Gestion de la Fonction Publique Territoriale du Puy-de-Dôme

abicom Secure IT

SOMMAIRE

01 INTRODUCTION

Un sujet d'actualité omniprésent :

MÉTÉO-FRANCE ANNONCE AVOIR ÉTÉ VICTIME D'UNE CYBERATTAQUE

BFM 14/04/2023

Cyberattaque : trois établissements de santé touchés à Lyon et Bourg-en-Bresse

France Info 30/01/2023

Le site de la Poste victime d'une cyberattaque revendiquée par un groupe de hackers du Bangladesh

Ouest France 31/05/2023

«RESPECTEZ LA RUSSIE» : PLUSIEURS MAIRIES FRANÇAISES VISÉES PAR DES CYBERATTAQUES PRO-RUSSES

CNEWS 04/05/2023

LILLE: LA MAIRIE VICTIME D'UNE CYBERATTAQUE, PLUSIEURS SERVICES MUNICIPAUX PERTURBÉS

BFM 01/03/2023

Cyberattaques en série en Île-de-France et dans l'Oise : face à la menace fantôme, la riposte s'organise

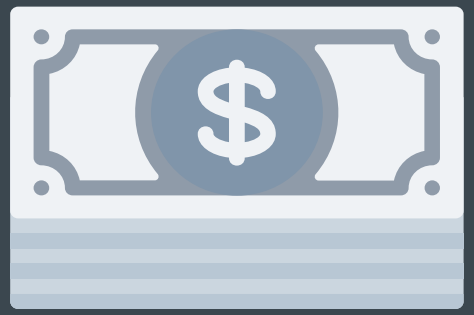
Des mairies, des hôpitaux, des institutions... Tandis que les pirates informatiques multiplient les actions, les victimes pansent leurs plaies numériques. Un fléau considéré comme « une priorité absolue » par la région Île-de-France.

Le Parisien 08/05/2023

Les sources de cybermenaces

Nuisance quotidienne

De nombreux acteurs malveillants réalisent de manière automatisée des actions pouvant nuire au fonctionnement du système d'information.



Menace cybercriminelle

A but essentiellement lucratif, ces attaques visent à générer du profit au travers d'un acte malveillant sur un système d'information.

Menace étatique

Opérées par des attaquants soutenus par des Etats et particulièrement sophistiquées, ces attaques ciblent précisément des entités.

02 LES MENACES

abicom
Secure IT

HAMEÇONNAGE : POINT D'ENTRÉE ET DE PROPAGATION

Technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données ou agir en sa faveur, en se faisant passer pour un tiers de confiance.

Exemple : *faux message, SMS ou appel téléphonique de banque, de réseau social, d'opérateur de téléphonie, de fournisseur d'énergie, de site de commerce en ligne, d'administrations, etc.*

Le *phishing* par courriel

Le *vishing* (appel vocal)

Le Smishing (SMS)

Le *phishing* sur les réseaux sociaux

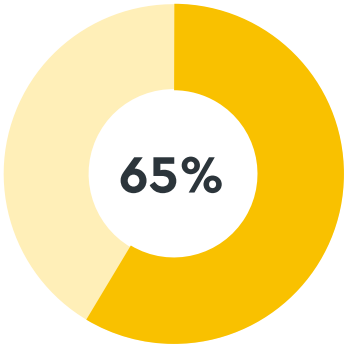
Le *spear phishing*

But recherché : Récupérer des informations (*comptes, mots de passe, données bancaires*...) pour en faire un usage frauduleux ou pousser le destinataire à télécharger & exécuter un fichier porteur d'un virus.

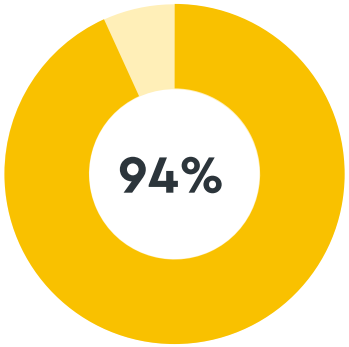
CONSÉQUENCES DE L'HAMEÇONNAGE

Rançongiciel : programme malveillant bloquant l'accès aux données du système contre le paiement d'une rançon pour obtenir le déchirement

Fraude au président : obtention frauduleuse d'informations ou d'argent, où l'attaquant se fait passer pour une personne importante demandant le traitement urgent de sa demande.



Des attaques débutent par un simple hameçonnage



Des logiciels malveillants sont propagés par courriel

abicom

LE PIRATAGE DE COMPTE EN LIGNE, LA FAIBLESSE DES MOTS DE PASSE

Vecteur d'attaque répandu car simple à réaliser.

Les **conséquences** : *vol de données, transactions frauduleuses, usurpations d'identités, etc.*

Vise les **comptes bancaires en ligne**, les **comptes de réseaux sociaux**, mais aussi et surtout les **comptes de messageries électroniques**.

Origine(s) :

1. **Mot de passe simple à deviner**
2. **Mot de passe transmis (in)volontairement**
3. **Suite d'un hameçonnage**
4. **Utilisation du même mot de passe sur un site piraté**
5. **Equipement infecté par un virus voleur de mot de passe**

Ressource utile : **haveibeenpwned.com**

LES SUPPORTS AMOVIBLES, VECTEUR D'ATTAQUE PAR DU MATÉRIEL PIÉGÉ

Fourniture d'un support amovible (ex : clé USB) ou d'un périphérique (ex : souris, borne de recharge de téléphone...) contenant un moyen d'attaque infectant l'équipement lors de la connexion.

Code malveillant

Lien vers un site malveillant

Rubber Ducky

USB Killer

03 LES SOLUTIONS

abicom
Secure IT

L'IDENTIFICATION DES MESSAGES SUSPECTS

- **L'orthographe approximative**
- **Adresse mail suspecte**
- **Interlocuteur inconnu**
- **Numéro surtaxé**
- **Lien ne correspondant pas au site d'origine**
- **Demande d'informations personnelles**

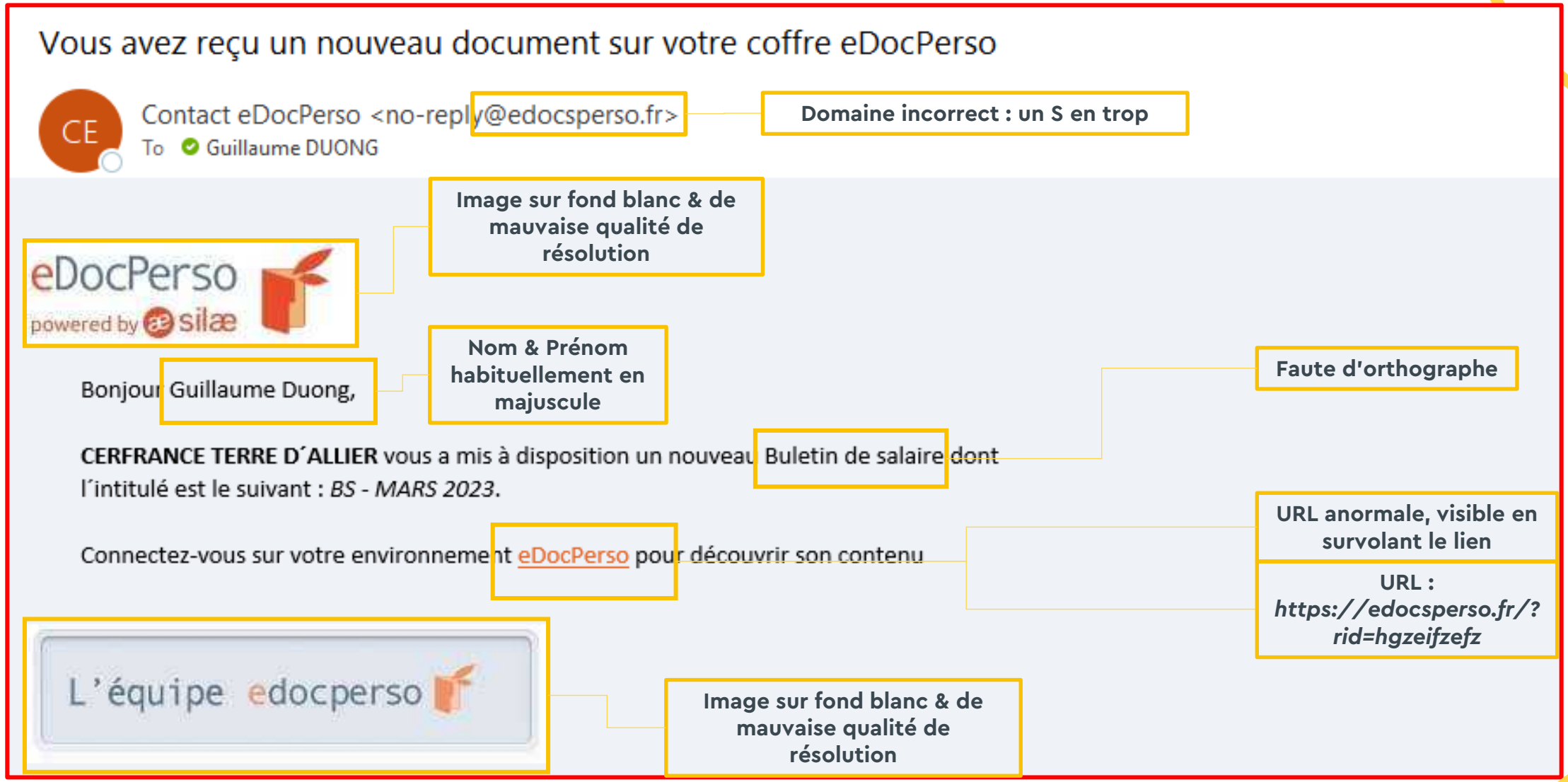
Que faire en cas d'attaque par hameçonnage ?

- **Ne pas cliquer sur des liens suspects ou inconnus.** (Accéder aux sites via un moteur de recherche par exemple)
- **Prévenir l'équipe sécurité et informer tous les collègues.**

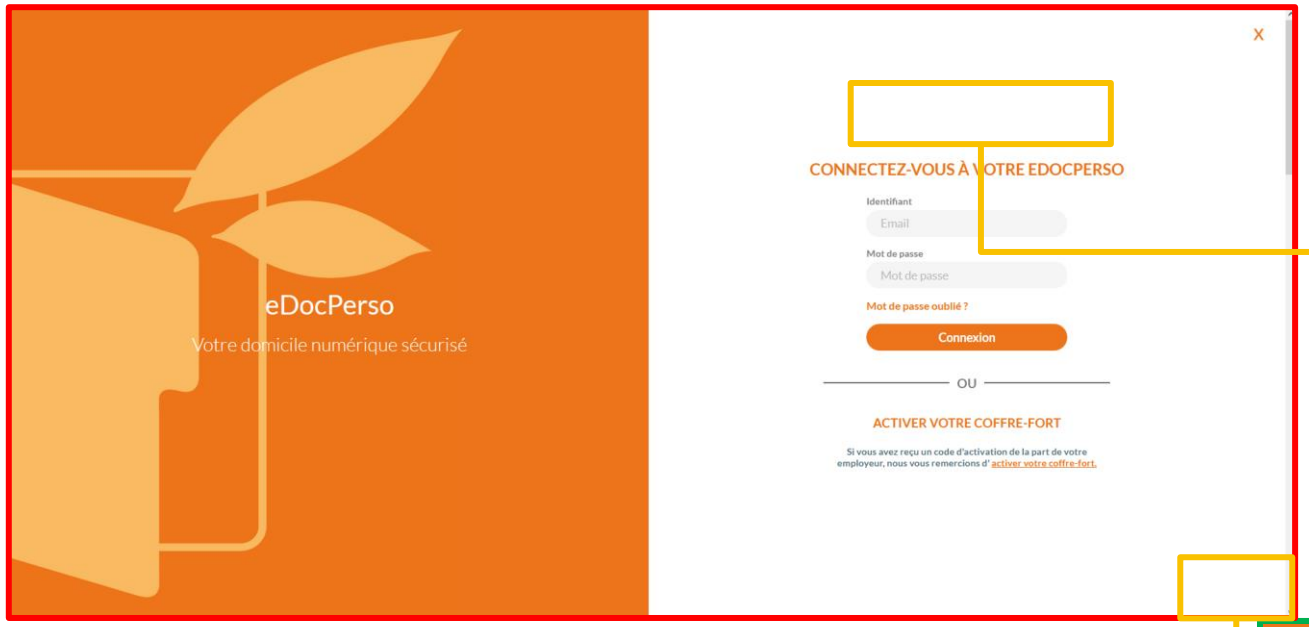
Ressource utile : **www.virustotal.com**

abicom

Un exemple de mail d'hameçonnage :

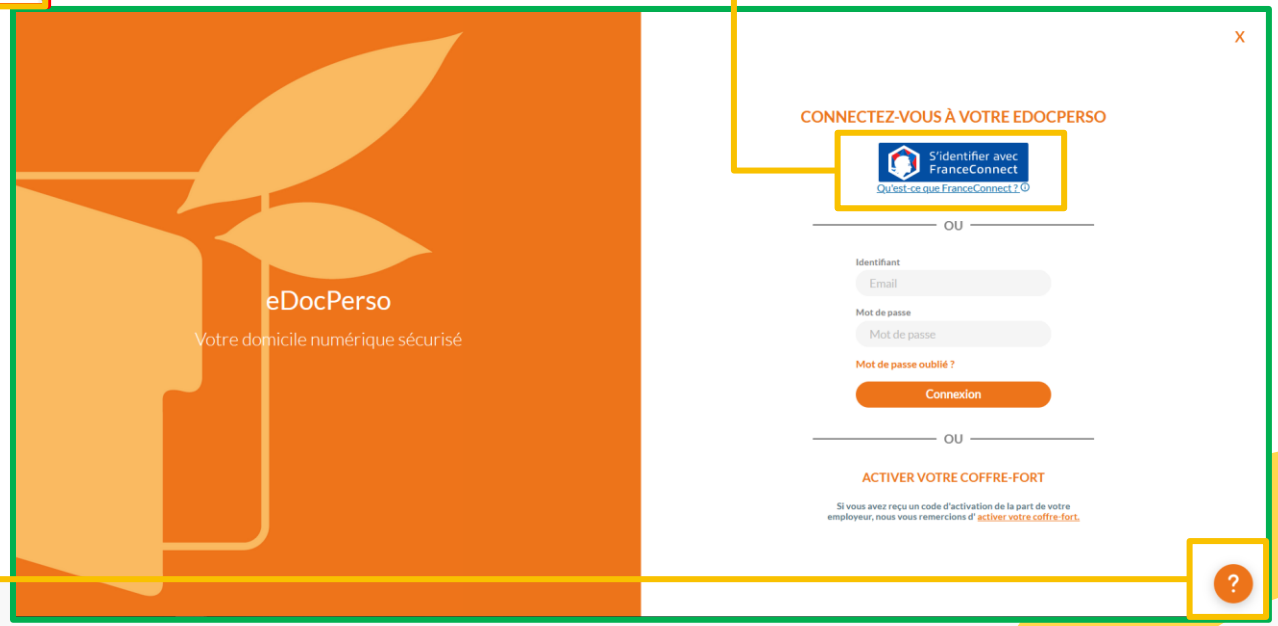


Concernant la page d'identification :



Icône de connexion avec France Connect manquante

Icône d'aide absente



abicom

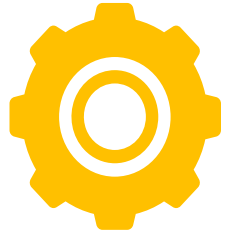
LE RENFORCEMENT DES MOTS DE PASSE

Force brute

Utiliser des mots de passe longs combinant plusieurs types de caractères (*chiffre*, *majuscule*, *minuscule*, *caractère spécial*)

Par dictionnaire

Ne jamais réutiliser un mot de passe piraté.
Ne pas utiliser de mot de passe commun (*ex : 123456789*, *password*, *qwerty*...).



Ingénierie sociale

Ne pas utiliser d'informations en lien avec vous, par exemple : *prénoms*, *noms*, *dates de naissance de vos enfants*, *nom de votre entreprise*, *animaux*...

abicom

Ressource utile : **le gestionnaire de mot de passe**

LA PROTECTION DES DONNÉES

Vigilance aux supports amovibles :

- Limiter au minimum l'usage de supports amovibles
- Analyser tout support amovible avant de le connecter sur son poste

Protéger matériellement les données :

- Mettre en veille/verrouiller son poste de travail lors des pauses
- Ne pas laisser de documents en libre accès
- Faire attention à l'accès aux locaux

Faire attention pendant les déplacements et en télétravail :

- Ne pas utiliser de réseau non maitrisé ou de borne électrique en libre service
- Se comporter chez soi comme l'on se comporte au bureau
- Séparer le domaine professionnel du domaine personnel

04 VOS RÉFLEXES

VOS BONS RÉFLEXES À AVOIR AU QUOTIDIEN :

- Savoir identifier tout mail douteux
- Bien choisir et ne jamais communiquer son authentification
- Savoir protéger les données

MERCI POUR VOTRE ATTENTION, MAINTENANT C'EST À VOUS DE JOUER !

Marc ANSELMINI
Ingénieur en conformité &
Juriste en droit du numérique
manselmini@abicom.fr _ 04.73.37.01.69. _ 06.10.04.98.54.

abicom
Secure IT