

Hacker n'est pas jouer

conférence & démos

Présentation by
@Michel & Benzo

25.05.2024



SQ
Tiers d'innovations
Médiathèque
DU CANAL





L'association Root66





L'association Root66

- Depuis 1999



L'association Root66

- Depuis 1999
- Les logiciels libres



L'association Root66

- Depuis 1999
- Les logiciels libres
- Conférences



L'association Root66

- Depuis 1999
- Les logiciels libres
- Conférences
- Permanences & ateliers



L'association Root66

- Depuis 1999
- Les logiciels libres
- Conférences
- Permanences & ateliers
- Install Party & smartphone Party



L'association Root66

- Depuis 1999
- Les logiciels libres
- Conférences
- Permanences & ateliers
- Install Party & smartphone Party
- Ciné Débat

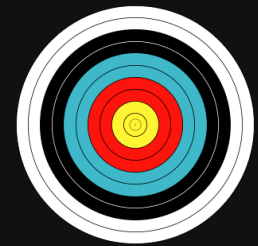


L'association Root66

- Depuis 1999
- Les logiciels libres
- Conférences
- Permanences & ateliers
- Install Party & smartphone Party
- Ciné Débat
- Formation

Disclaimer

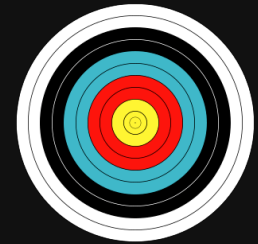
Contexte



Disclaimer

Contexte

Toutes nos activités sont numérisées

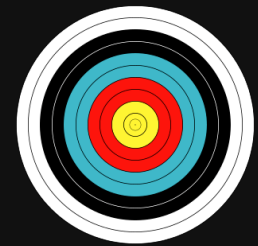


Disclaimer

Contexte

Toutes nos activités sont numérisées

Nos données sont convoitées



Disclaimer

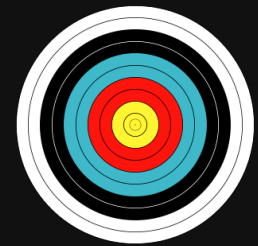
Contexte

Toutes nos activités sont numérisées

Nos données sont convoitées

piratage :

multitude d'acteurs avides de nos
datas : état, entreprises, d'autres
malveillants, cybercriminels, kevin...



Disclaimer

Contexte

Toutes nos activités sont numérisées

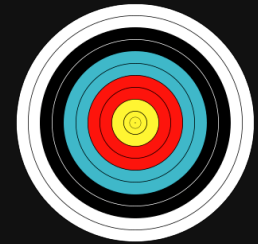
Nos données sont convoitées

piratage :

multitude d'acteurs avides de nos
datas : état, entreprises, d'autres
malveillants, cybercriminels, kevin...



-> menaces escroquerie, arnaques ,
vols de données , espionnage,
surveillance généralisée ...



Disclaimer

conférence participative

1. démos (x4) - crescendo
2. conseils
3. questions - échanges

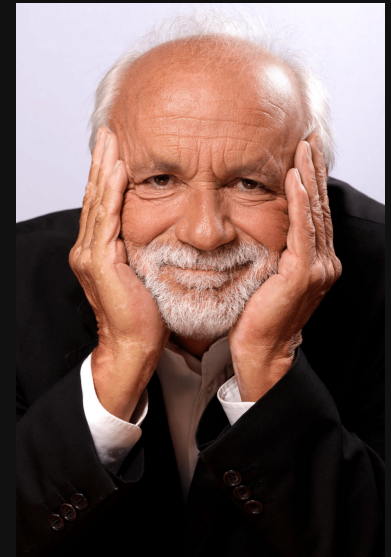
Disclaimer

effet Bonaldi

Disclaimer

Disclaimer

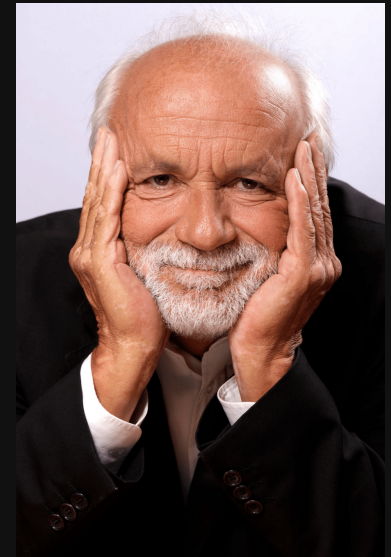
effet Bonaldi



Disclaimer

effet Bonaldi

« Toute démonstration d'un produit quelconque qui fonctionnait parfaitement aux répétitions échouera lamentablement lors de la démonstration publique. »



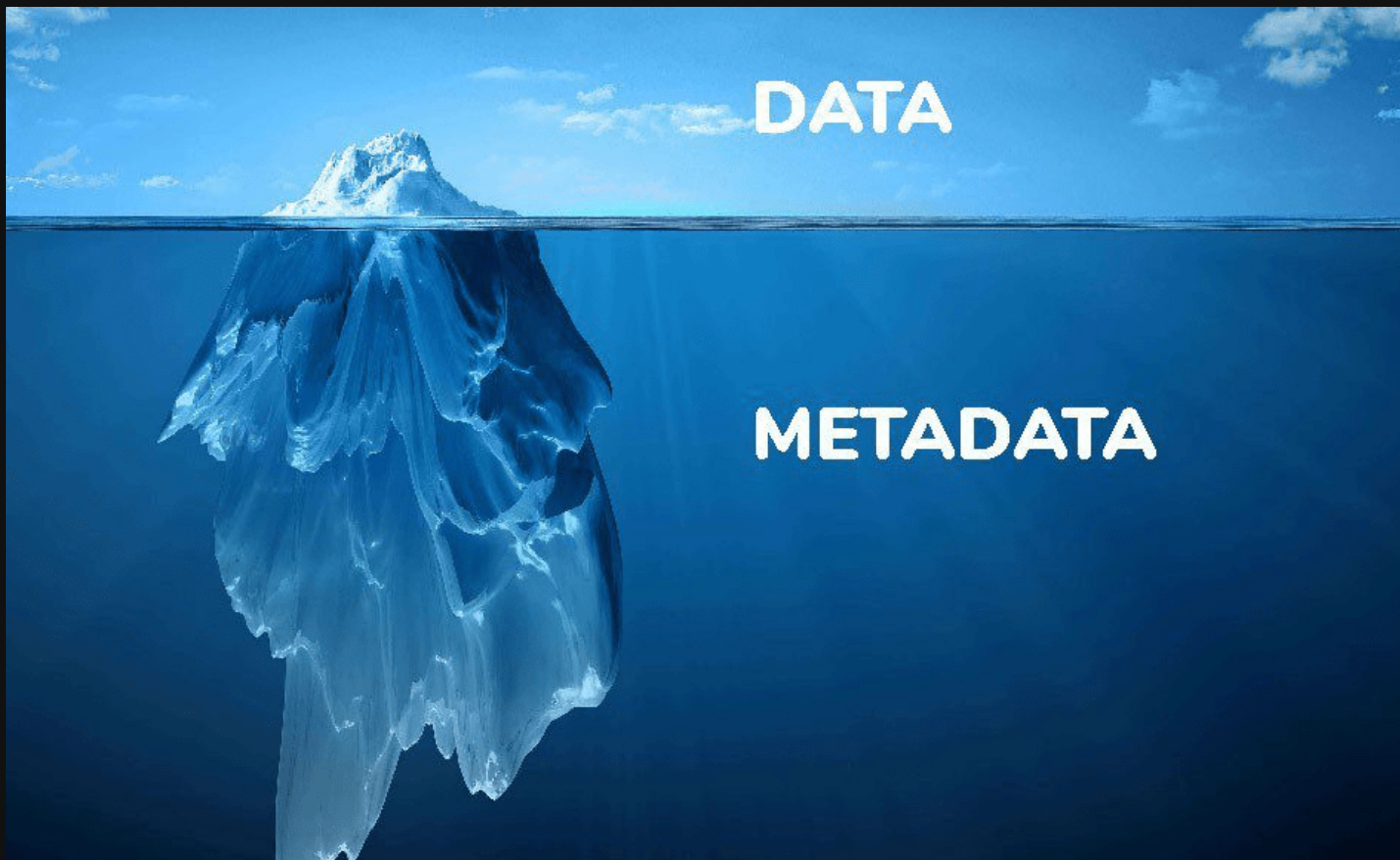
Démo 1

Derrière les apparences ...



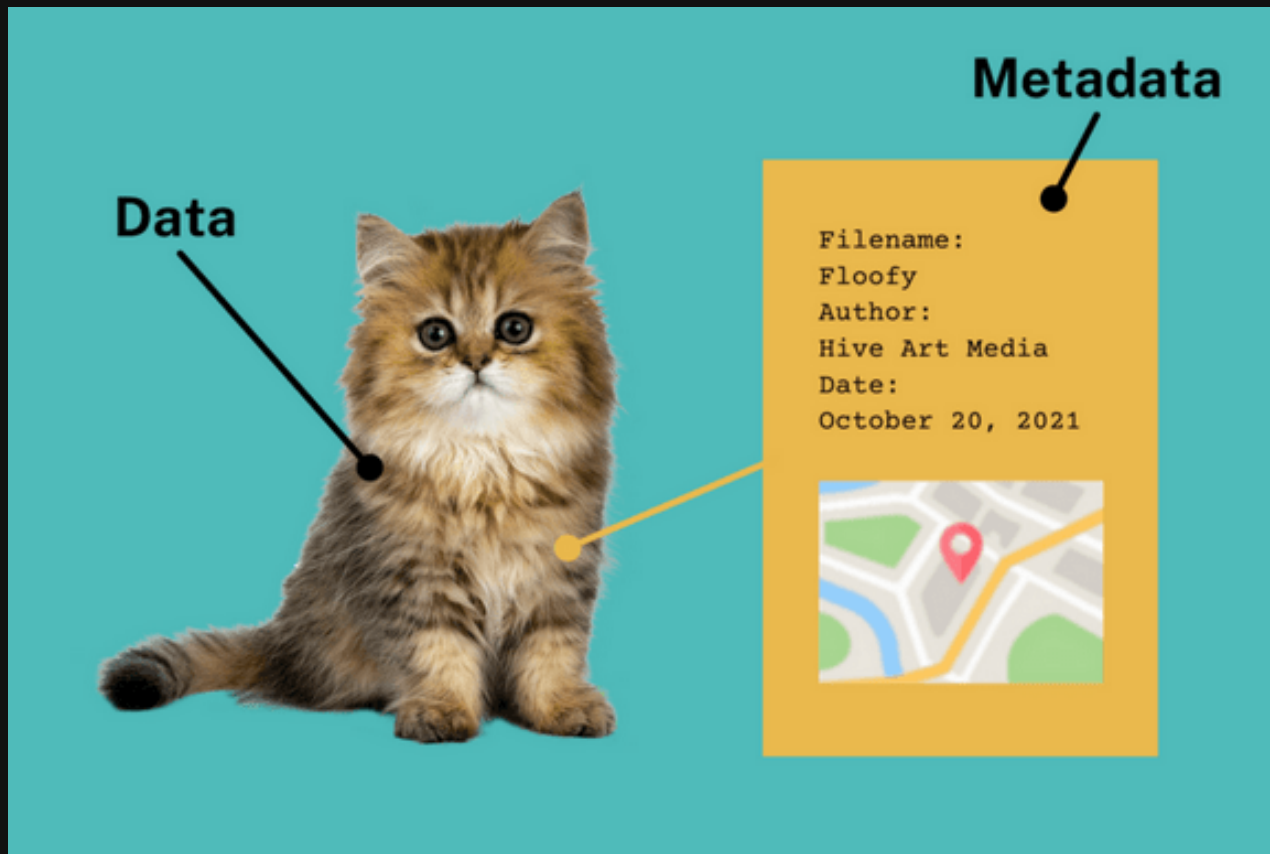
Derrière les apparences...

Les traces qu'on laisse sur le Web



Derrière les apparences...

Les traces numériques



Derrière les apparences...

Mesures - conseils pour limiter le risque:

**Supprimer metadatas avant de partager
les fichiers**

- sous windows : 
clic droit sur doc - propriétés - détails -
supprimer
- sous Linux : exiftool 

Derrière les apparences...

Mesures - conseils

Limiter la production de metadatas

- en **configurant** ses logiciels
d'édition de docs bureautiques , pao
etc

Menus préférences - options

pdf , docx, Photoshop, Gimp ...

Derrière les apparences...

Mesures - conseils pour limiter le risque:



Derrière les apparences...

Mesures - conseils pour limiter le risque:

Android :

Sur l'Appareil Photo

- ouvrir l'application - aller dans les Réglages
- désactiver l'option Enregistrer le lieu.



Derrière les apparences...

Mesures - conseils pour limiter le risque:

Android :

Sur l'Appareil Photo

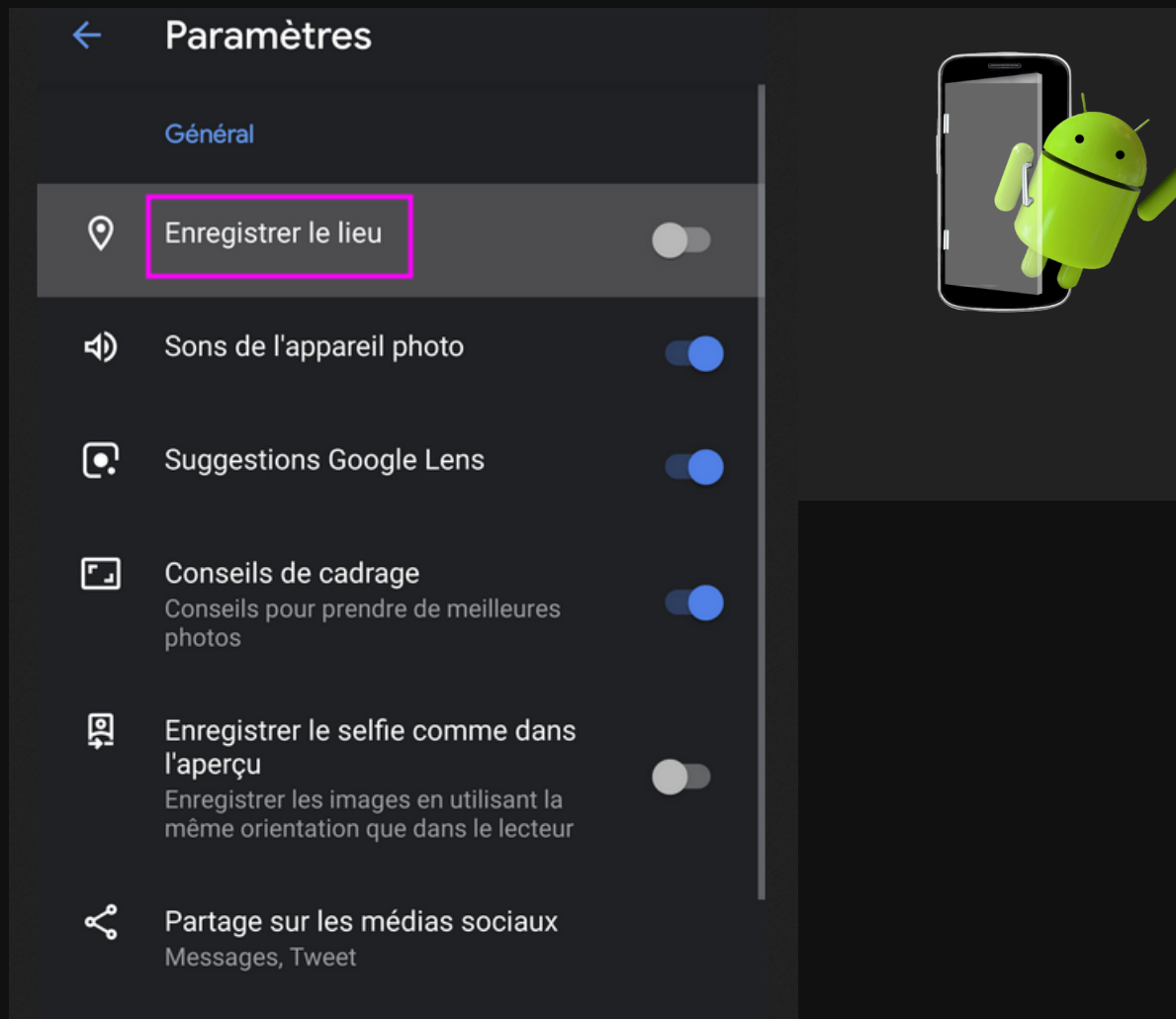
- ouvrir l'application - aller dans les Réglages
- désactiver l'option Enregistrer le lieu.



Les photos prises par la suite ne pourront plus avoir les données GPS dans ses métadonnées.

Derrière les apparences...

Mesures - conseils pour limiter le risque:




The image shows a screenshot of the Android camera settings menu. The title is 'Paramètres' with a back arrow. Under the 'Général' section, the option 'Enregistrer le lieu' is highlighted with a red rectangle and has its toggle switch turned off. Other options include 'Sons de l'appareil photo' (on), 'Suggestions Google Lens' (on), 'Conseils de cadrage' (on), 'Enregistrer le selfie comme dans l'aperçu' (off), and 'Partage sur les médias sociaux' (Messages, Tweet).

← Paramètres

Général

- 📍 Enregistrer le lieu
- 🔊 Sons de l'appareil photo
- 📷 Suggestions Google Lens
- 📐 Conseils de cadrage
Conseils pour prendre de meilleures photos
- 📱 Enregistrer le selfie comme dans l'aperçu
Enregistrer les images en utilisant la même orientation que dans le lecteur
- 🔗 Partage sur les médias sociaux
Messages, Tweet



Derrière les apparences...

Mesures - conseils pour limiter le risque:

Configurer ses appareils et ses applications pour ne pas produire de metadatas

Applications bureautiques :
ex: Libre-office

Derrière les apparences...

Mesures - conseils pour limiter le risque:

Options - LibreOffice - Données d'identité

LibreOffice

- Données d'identité
- Général
- Affichage
- Impression
- Chemins
- Polices
- Sécurité
- Personnalisation
- Couleurs de l'interface
- Accessibilité
- Avancé
- OpenCL
- Chargement/enregistrement
- Paramètres linguistiques
- LibreOffice Writer

Adresse

Société : Syndicat

Prénom/Nom/Initiales : benzo b

Rue : 31 rue victor hugo

Code postal/ville : 75300

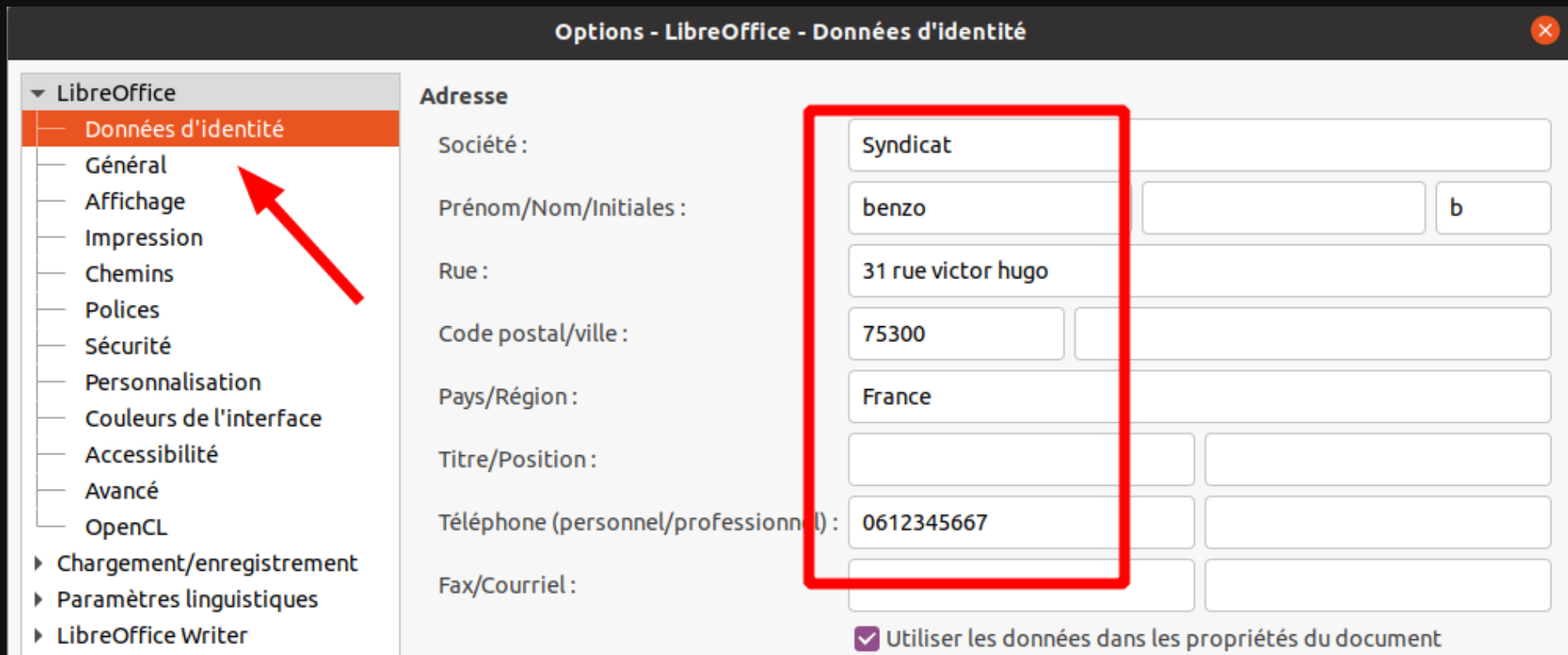
Pays/Région : France

Titre/Position :

Téléphone (personnel/professionnel) : 0612345667

Fax/Courriel :

Utiliser les données dans les propriétés du document



Démo 2

A la pêche de vos infos



Le phishing par SMS



Le phishing par mail

Sujet : Votre Abonnement a EXpiré.
De : supportnetfli x<ajarro.d.patfield@realgarrafeira.com>
Date : 27/02/2024 08:25
Pour : <michel.shriqui@free.fr>

[renouveLez voTre compte graTuiTement](#)

NETFLIX

Attention !
Abonnement Netflix



Cher client,
Votre abonnement a expire !
Toutefois, notre programme de fidelite
vous permet desormais de le
prolonger gratuitement de 90 jours.

Prolongation gratuite

Démo 2

Mesures - conseils pour détecter un phishing:



Démo 2

Mesures - conseils pour détecter un phishing:

1 - Soyez sceptique



Démo 2

Mesures - conseils pour détecter un phishing:

1 - Soyez sceptique

Ne répondez jamais :

- à **l'urgence** d'un message, surtout s'il vous demande infos sensibles
- aux promesses d'enrichissement , de remboursement , de bonheur,...



Démo 2

Mesures - conseils pour détecter un phishing:

Démo 2

Mesures - conseils pour détecter un phishing:

2 - vérifier les URL

Démo 2

Mesures - conseils pour détecter un phishing:

2 - vérifier les URL

Au survol de la souris , l'URL complète apparaît :

- nom de domaine légitime ?

Démo 2

Mesures - conseils pour détecter un phishing:



France
Connect

Bonjour,

Une connexion a eu lieu grâce à FranceConnect :

Merci d'avoir utilisé notre service.

Si ce n'était pas vous, **cliquez ici.**

<http://fo.79qp14.com/d>

Pour plus d'informations, consultez notre FAQ Usagers à l'adresse suivante :

<http://franceconnect.gouv.fr/faq>

url suspecte

Démo 2

Mesures - conseils pour détecter un phishing:

2 - vérifier les URL



France
Connect

Bonjour,

Une connexion a eu lieu grâce à FranceConnect :

Merci d'avoir utilisé notre service.

Si ce n'était pas vous, **cliquez ici.**

Pour plus d'informations, consultez notre FAQ Usagers à l'adresse suivante :
<http://fo.79qp14.com/d>

url suspecte

Le phishing par mail

TYPOSQUATTING

AKA URL Hijacking — the practice of registering domains of known brands with the intent of tricking users into believing they are legitimate sites



COMMON TECHNIQUES

**DROPPING THE DOT
AFTER 'WWW'**

wwwaa.com

DROPPING ONE LETTER

apple.om

**SWITCHING TWO
LETTERS**

faecbook.com

DOUBLING CHARACTERS

twiitter.com

**USING SIMILAR
LOOKING CHARACTERS**

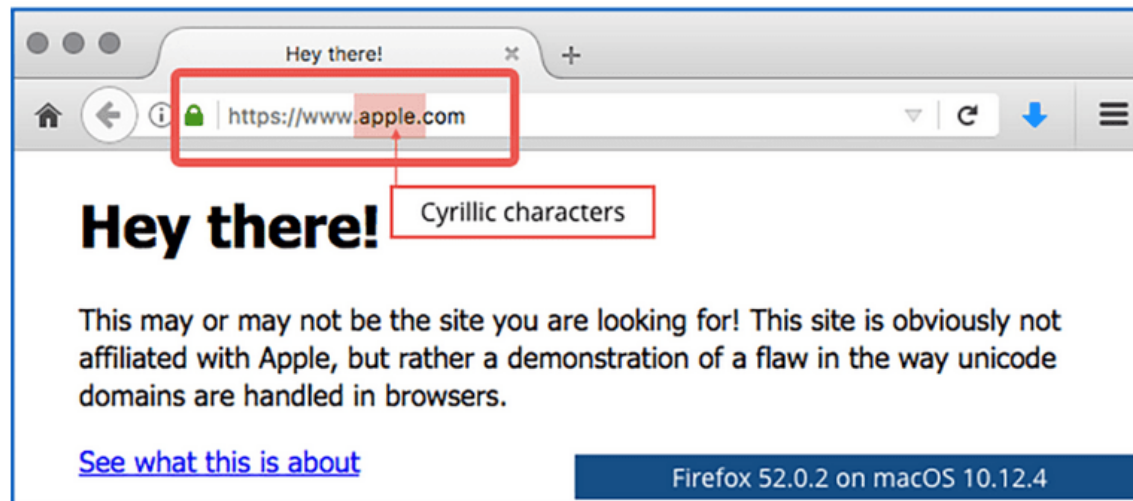
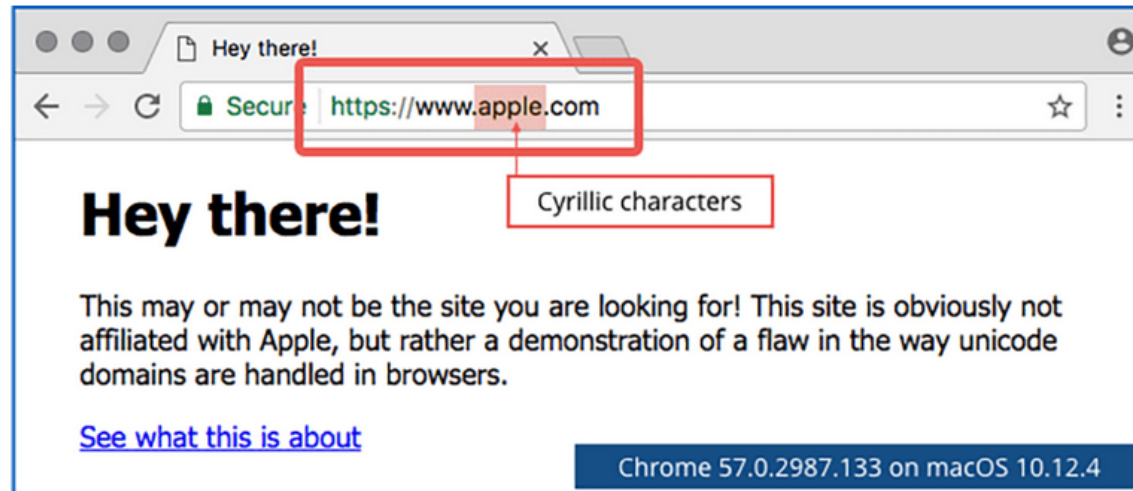
google.com (l vs l)

**PRESSING A WRONG
KEY**

costko.com

Le phishing par mail

attaque homographique



Démo 2

Mesures - conseils pour détecter un phishing:

3 - indices supplémentaires

Démo 2

Mesures - conseils pour détecter un phishing:

3 - indices supplémentaires

- vérifier l'expéditeur
- l'orthographe du mail
- charte graphique , logo

Démo 2

Mesures - conseils pour détecter un phishing:

3 - indices supplémentaires

- vérifier l'expéditeur
- l'orthographe du mail
- charte graphique , logo



Démo 2

Mesures - conseils pour détecter un phishing:

3 - indices supplémentaires

- vérifier l'expéditeur
- l'orthographe du mail
- charte graphique , logo



De nos jours, ces indices ne suffisent plus
Les outils pour générer mails de phishings se sont perfectionnés , professionnalisés, industrialisés (IA)

Démo 2

Mesures - conseils

4 - Règles de base

Démo 2

Mesures - conseils

4 - Règles de base

- Ne répondez jamais aux mails ou SMS vous demandant la saisie d'informations confidentielles (mots de passe, codes ...)
- Ne cliquez jamais sur les liens de mails ou SMS suspects
- idem pour PJ

Démo 2

Mesures - conseils

4 - Règles de base

- Ne répondez jamais aux mails ou SMS vous demandant la saisie d'informations confidentielles (mots de passe, codes ...)
- Ne cliquez jamais sur les liens de mails ou SMS suspects
- idem pour PJ

En cas de doute, contactez directement par téléphone ou sur votre espace en ligne les organismes concernés : EDF, impôts, CAF, banque...

Démo 2

Mesures - conseils

5 - Mesures de prévention

Démo 2

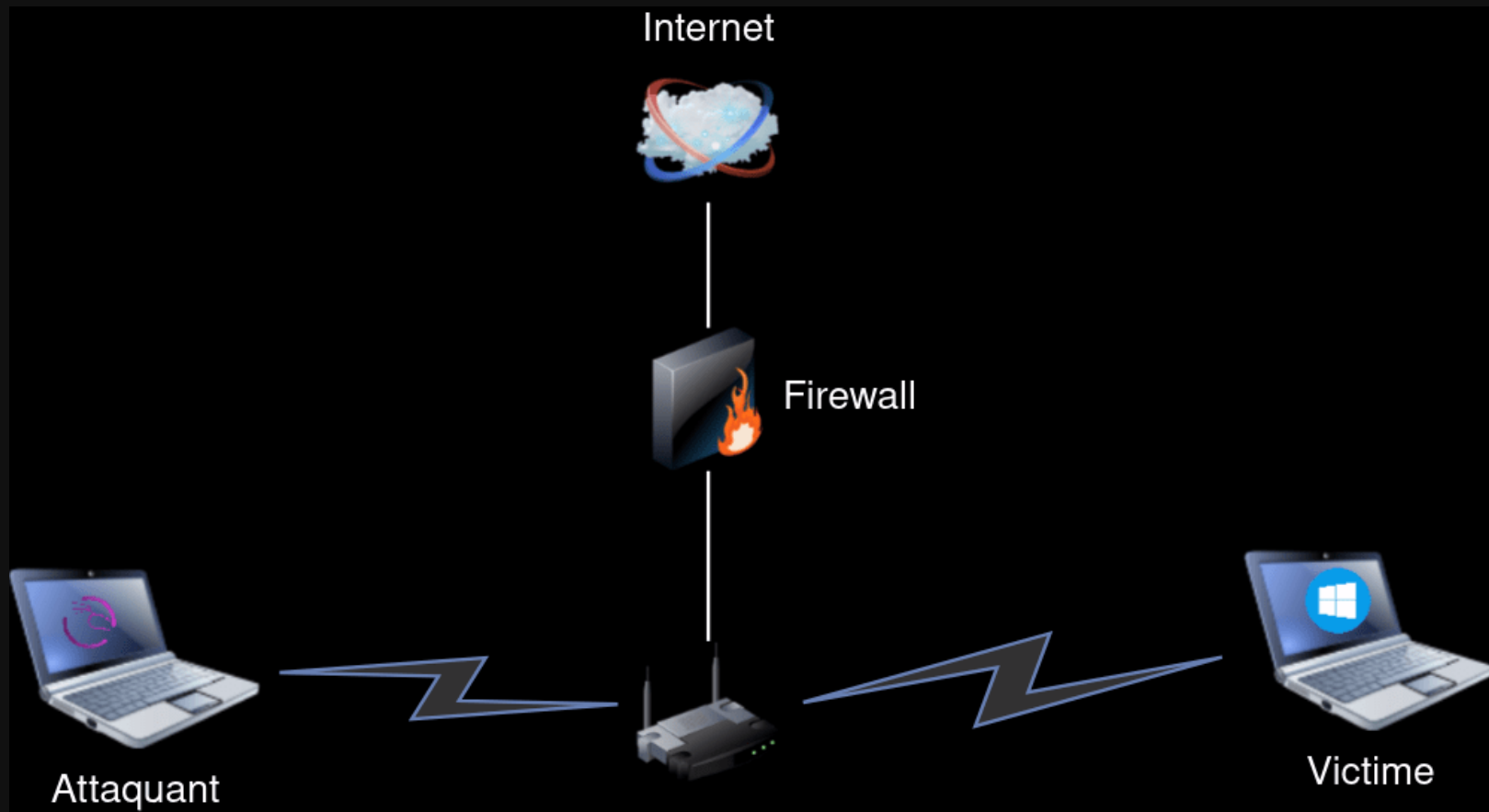
Mesures - conseils

5 - Mesures de prévention

- 1 seul mot de passe complexe et unique par appli / services
- Activer la double authentification (mails, services webs...)
- Faire mises à jour régulières système et applications

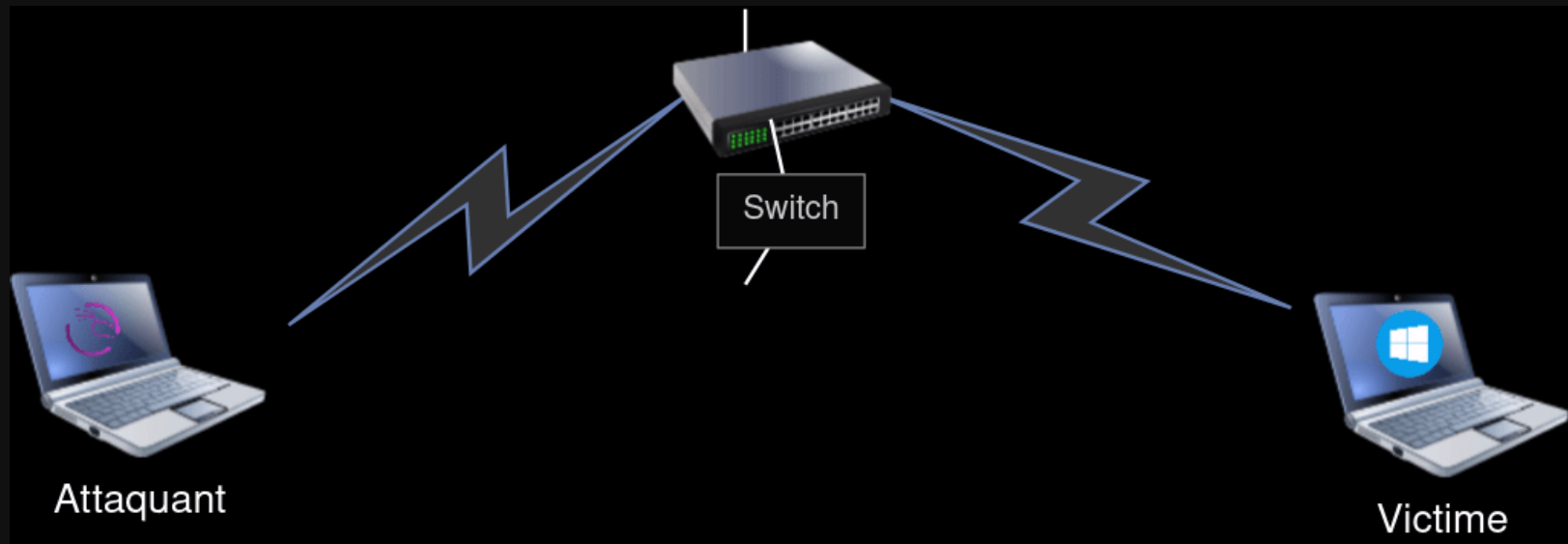
Démo 2

A la pêche de vos infos



Démo 2

A la pêche de vos infos



Démo 2

Mesures - conseils

Démo 2

Mesures - conseils

en cas de compromission par phishing:

Démo 2

Mesures - conseils

en cas de compromission par phishing:

- déconnecter pc du réseau
- contacter le service compromis (banque; impots ,edf, mails...)
- changer ses mots de passe
- signaler à PHAROS

Démo 3

Dans l'intimité de votre machine



Démo 3

Mesures - conseils



Démo 3

Mesures - conseils

Prévention



Démo 3

Mesures - conseils

Prévention

- Ne pas connecter à son pc clés USB inconnues



Démo 3

Mesures - conseils

Prévention

- Ne pas connecter à son pc clés USB inconnues
- Ne pas cliquer sur PJ mails inconnus



Démo 3

Mesures - conseils

Prévention

- Ne pas connecter à son pc clés USB inconnues
- Ne pas cliquer sur PJ mails inconnus
- Ne pas télécharger applis, films ..sur sites douteux



Démo 3

Mesures - conseils

Prévention

- Ne pas connecter à son pc clés USB inconnues
- Ne pas cliquer sur PJ mails inconnus
- Ne pas télécharger applis, films ..sur sites douteux
- Vérifier intégrité des programmes qu'on télécharge



Démo 3

Mesures - conseils

Prévention

- Ne pas connecter à son pc clés USB inconnues
- Ne pas cliquer sur PJ mails inconnus
- Ne pas télécharger applis, films ..sur sites douteux
- Vérifier intégrité des programmes qu'on télécharge
- Antivirus (windows)



Démo 3

Mesures - conseils

Prévention

- Ne pas connecter à son pc clés USB inconnues
- Ne pas cliquer sur PJ mails inconnus
- Ne pas télécharger applis, films ..sur sites douteux
- Vérifier intégrité des programmes qu'on télécharge
- Antivirus (windows)
- Utiliser logiciels libres si possibles



Démo 3

Mesures - conseils

Démo 3

Mesures - conseils

en cas de compromission :

Démo 3

Mesures - conseils

en cas de compromission :

- Déconnecter son pc du réseau
- Analyser fichiers AntiVirus
- Changer ses mots de passe + double auth
- Réinstaller /réinitialiser OS

Démo 4

Smartphone android



Démo 4

Smartphone android

L'espion qui m'aimait ?



Conseils généraux

Hygiène numérique



Conseils généraux

Hygiène numérique

En fonction du contexte



Conseils généraux

Hygiène numérique

En fonction du contexte

- Télécharger applis sur sites officiels



Conseils généraux

Hygiène numérique

En fonction du contexte

- Télécharger applis sur sites officiels
- Utiliser logiciels libres



Conseils généraux

Hygiène numérique

En fonction du contexte

- Télécharger applis sur sites officiels
- Utiliser logiciels libres
- Faire mises à jour régulières (syst, applis)



Conseils généraux

Hygiène numérique

En fonction du contexte

- Télécharger applis sur sites officiels
- Utiliser logiciels libres
- Faire mises à jour régulières (syst, applis)
- Antivirus



Conseils généraux

Hygiène numérique

En fonction du contexte

- Télécharger applis sur sites officiels
- Utiliser logiciels libres
- Faire mises à jour régulières (syst, applis)
- Antivirus
- Ne pas cliquer sur liens ou PJ douteuses



Conseils généraux

Hygiène numérique

En fonction du contexte

- Télécharger applis sur sites officiels
- Utiliser logiciels libres
- Faire mises à jour régulières (syst, applis)
- Antivirus
- Ne pas cliquer sur liens ou PJ douteuses
- mots de passe complexe (keepass)



Conseils généraux

Hygiène numérique

En fonction du contexte

- Télécharger applis sur sites officiels
- Utiliser logiciels libres
- Faire mises à jour régulières (syst, applis)
- Antivirus
- Ne pas cliquer sur liens ou PJ douteuses
- mots de passe complexe (keepass)
- Chiffrer vos communications



Conseils généraux

Hygiène numérique

En fonction du contexte

- Télécharger applis sur sites officiels
- Utiliser logiciels libres
- Faire mises à jour régulières (syst, applis)
- Antivirus
- Ne pas cliquer sur liens ou PJ douteuses
- mots de passe complexe (keepass)
- Chiffrer vos communications
- Chiffrer vos disques durs



Conseils généraux

Hygiène numérique

En fonction du contexte

- Télécharger applis sur sites officiels
- Utiliser logiciels libres
- Faire mises à jour régulières (syst, applis)
- Antivirus
- Ne pas cliquer sur liens ou PJ douteuses
- mots de passe complexe (keepass)
- Chiffrer vos communications
- Chiffrer vos disques durs
- Sauvegarder régulièrement ses données



Conseils récaps

Hygiène numérique

En fonction du contexte

Conseils récaps

Hygiène numérique

En fonction du contexte

- Supprimer traces : cookies , historiques , mots de passe préenregistrés

Conseils récaps

Hygiène numérique

En fonction du contexte

- Supprimer traces : cookies , historiques , mots de passe préenregistrés
- Nettoyer les métadonnées

Conseils récaps

Hygiène numérique

En fonction du contexte

- Supprimer traces : cookies , historiques , mots de passe préenregistrés
- Nettoyer les métadonnées
- Couper wifi , bluetooth si non utilisés

Conseils récaps

Hygiène numérique

En fonction du contexte

- Supprimer traces : cookies , historiques , mots de passe préenregistrés
- Nettoyer les métadonnées
- Couper wifi , bluetooth si non utilisés
- Utiliser un VPN sur hotspot wifi public

Conseils récaps

Hygiène numérique

En fonction du contexte

- Supprimer traces : cookies , historiques , mots de passe préenregistrés
- Nettoyer les métadonnées
- Couper wifi , bluetooth si non utilisés
- Utiliser un VPN sur hotspot wifi public
- Ne pas laisser son smartphone ou pc sans surveillance s'il n'est pas éteint

Conseils récaps

Hygiène numérique

En fonction du contexte

- Supprimer traces : cookies , historiques , mots de passe préenregistrés
- Nettoyer les métadonnées
- Couper wifi , bluetooth si non utilisés
- Utiliser un VPN sur hotspot wifi public
- Ne pas laisser son smartphone ou pc sans surveillance s'il n'est pas éteint
- Éviter d'utiliser comptes admin comme compte utilisateur principal

Conseils récaps

Hygiène numérique

En fonction du contexte

- Supprimer traces : cookies , historiques , mots de passe préenregistrés
- Nettoyer les métadonnées
- Couper wifi , bluetooth si non utilisés
- Utiliser un VPN sur hotspot wifi public
- Ne pas laisser son smartphone ou pc sans surveillance s'il n'est pas éteint
- Éviter d'utiliser comptes admin comme compte utilisateur principal
- Utiliser la double authentification quand c'est possible

Hygiène numérique

GUIDE DE SURVIE DES AVENTURES SUR INTERNET v.3

ou comment protéger ses libertés
en milieu numérique "hostile"



Octobre 2023

Ligue
des droits de
l'Homme



Le CECIL
Comité d'Action sur le Contrôle de
l'Informatique et les Libertés
www.lececil.org
contact@lececil.org

ritimo
le changement par l'Info !

Questions

