Formation au numérique - Sécurité

Yves AGOSTINI «yves@yvesago.net»

janvier. 2023

Plan

Sécurité

Un usage sécurisé des réseaux

Les connaissances minimales pour ne pas se faire escroquer

1. Les risques
   ☞ *fantasme vs réalité*
2. Se protéger
   ☞ *avec seulement 4 bonnes pratiques*
3. **À retenir**

Les risques

1. Quelques exemples médiatisés depuis 2014
2. "Mes données n'ont pas d'importance"
3. Vols de données
4. Buts et motivations des attaquants

Les risques

En évolution constante

...

En 2023 :

- phishing
- logiciels malveillants
- désinformation
- vol de données personnelles

⇒ Pour les escrocs les données de n'importe qui ont de l'importance

Buts et motivations

1 ⇒ Financiers

2 ⇒ Idéologiques

3 ⇒ Curiosité

✖ visibilité de l'incident = f(motivation)
✔ mêmes protections, ∀ motivation

Se protéger

Pas de panique, la protection est facile :

1. Mot de passe
2. Machines
3. Le bon sens
4. Sauvegardes

Mot de passe

Rappel risques :

```
Accès à la boite mail:
 - changement de mots de passe sur sites avec payement : amazon, paypal, ↩
     banque, impôts, ...
 - escroquerie des contacts : "j'ai un problème, envoie moi un coupon ... "
 - réutilisation d ancien mails crédibles, modification de fichiers attachés

Accès aux applications internes:
 - vol d'information professionnelles
 - accès privilégiés

Usurpation d'identité: avantages sociaux, numéro de mobile, ...

Atteinte à la réputation: non conservation de secrets

Marché noir de la revente d'identifiants
```

1. Mot de passe ✔

- Mots de passe robustes
  - longs, MAJ./min., chiffres, + - _ *, ...
  - "J'ai acheté 5 CD pour cent euros cet après-midi" ⇒ `ght5CD%E7am`
  - "Les sanglots longs des violons de l'automne blessent mon cœur" ⇒ `Lsldv2lbmc`
- Secrets :
  - ni assistance, ni famille, ni responsable, ...
- **Différents pour chaque site**
- Savoir changer rapidement de mot de passe
  ☞ *l'erreur est humaine*
- Protection des accès :
  - domicile, portable, smartphone
    ☞ mot de passe, schéma, PIN

1. Mot de passe> les pièges ✖

- Usage de machine inconnue :
  - amis, famille *(infectés ?)*
  - voyage à l'étranger : douanes, cybercafé
- Wifi :
  - portail captif, wifi gratuit, aéroport, ...
    ☞ erreur de certificat
- VPN, proxy :
  - quelle identification ? quelle protection ?
    ≠ VPN d'entreprise ✖
  - qui gère ? comment ? toujours compétents ?
  - quelle assistance ?
    (les youtubeurs sont payés pour faire de la promotion)

1. Mot de passe> mauvaises idées ✖

- "Agrégateur" de comptes mails :
  - myMail, CloudMagic, BlueMail, Spark, ...
- Interface unique :
  - Gmail, Yahoo, Hotmail
- "Service" Blackberry
- Synchro centralisée de mot de passe :
  - LastPass, Opéra, ...
- "Découvrir / Importer ses contacts"

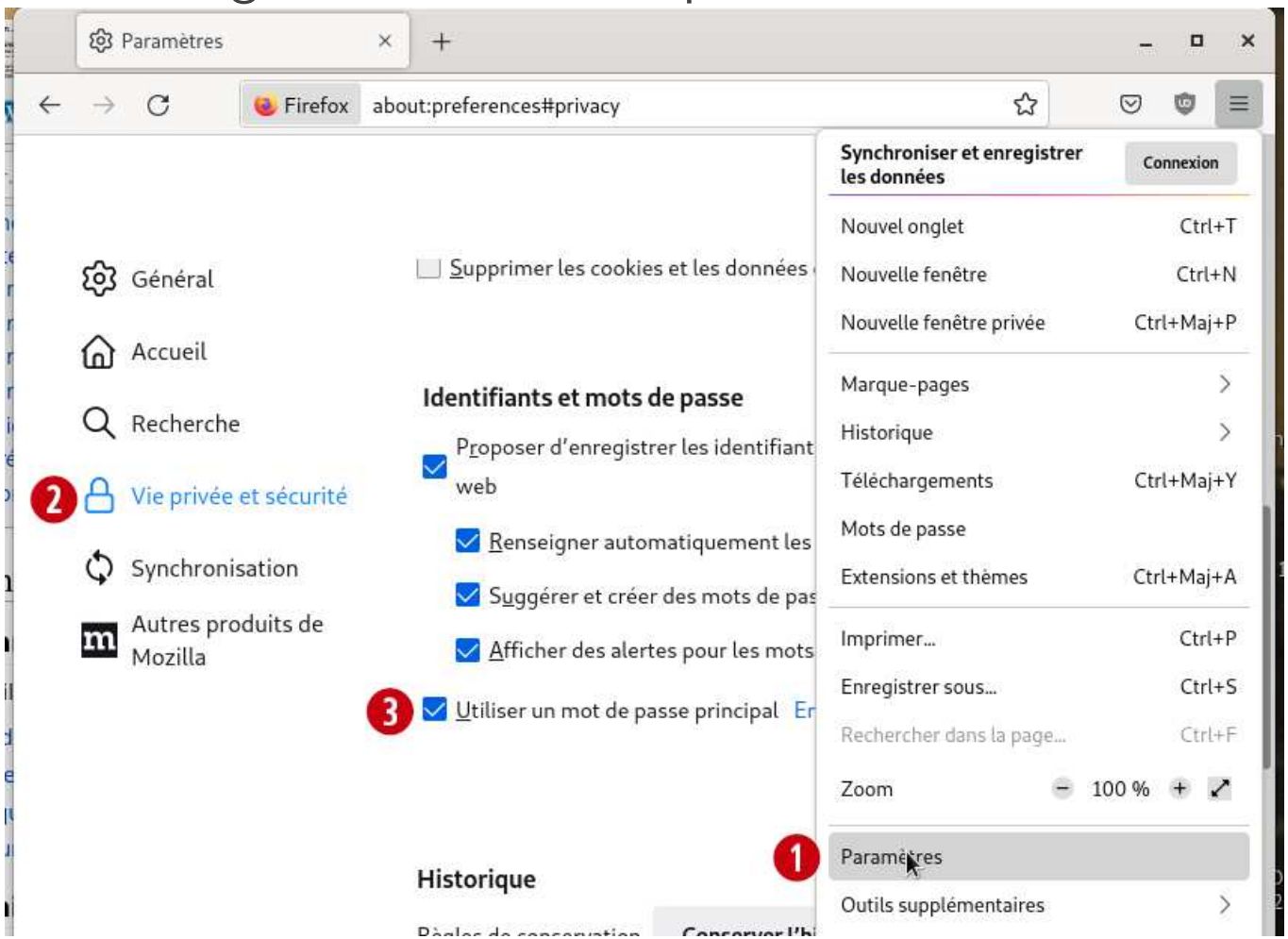
☞ **Ne pas confier ses mots de passe à des tiers**

1. Mot de passe> les solutions ✔

- Séparer identités **professionnelle** / **personnelle(s)**
  ☞ Mots de passe uniques

1. Mot de passe> les solutions ✔

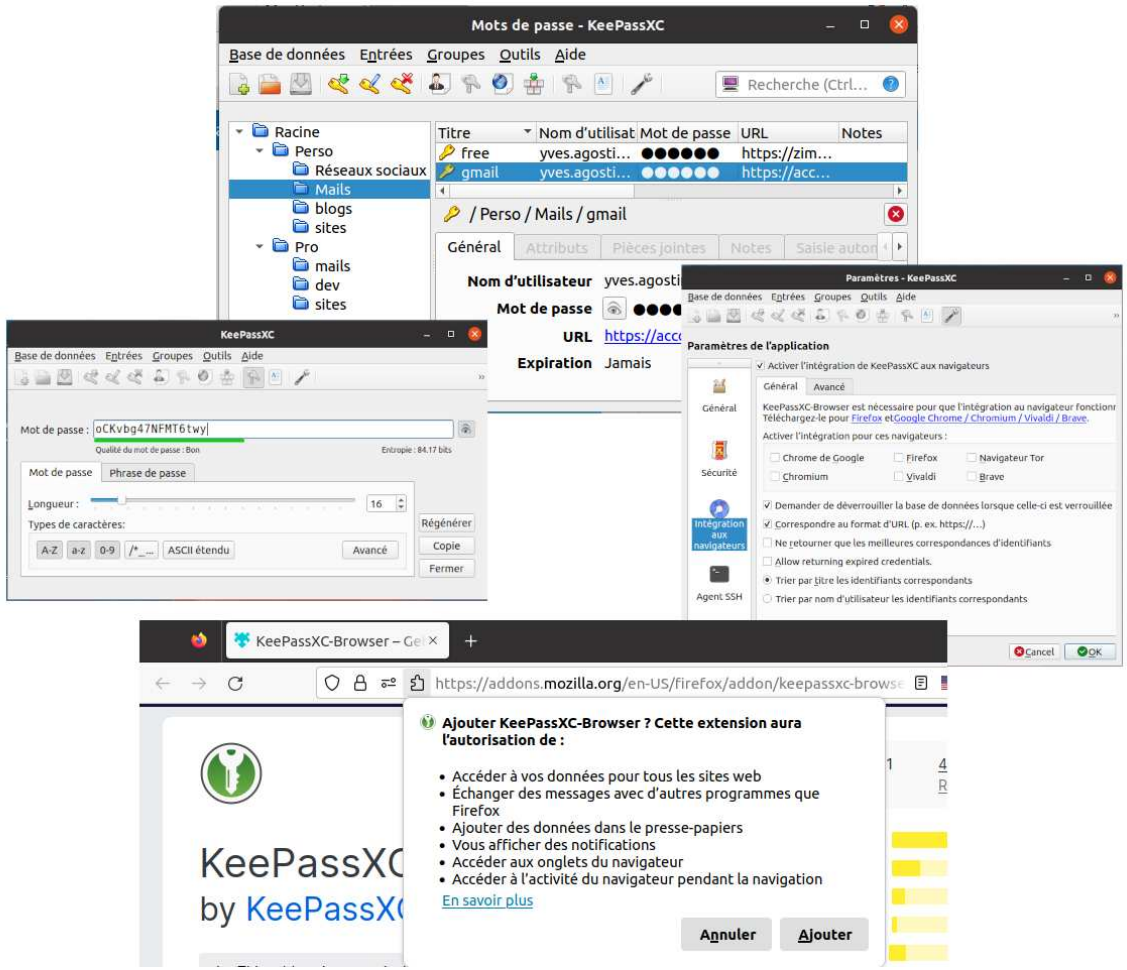
- Séparer identités **professionnelle** / **personnelle(s)**
- Outils de gestion de mots de passe :



Firefox : Mots de passe protégés par mot de passe principal

1. Mot de passe> les solutions ✔

- Séparer identités **professionnelle** / **personnelle(s)**
- Outils de gestion de mots de passe :

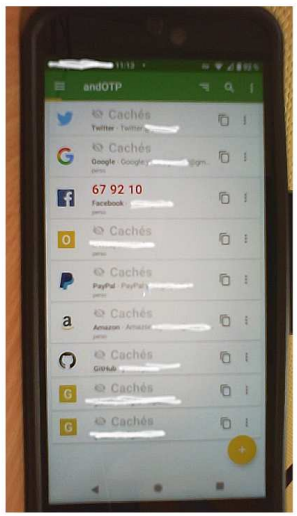


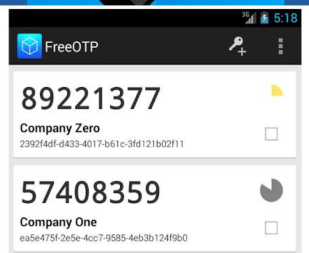
KeepassXC : Base de mots de passe dans un fichier partageable ✔

1. Mot de passe> les solutions ✔

- Séparer identités **professionnelle / personnelle(s)**
- Outils de gestion de mots de passe :
  Firefox : Mots de passe protégés par mot de passe principal
  KeepassXC : Base de mots de passe dans un fichier partagé ✔
- Application mail → plusieurs comptes
- Authentification double facteurs :
  - Google, Facebook, Twitter, ...

AndOTP, Aegis, freeOTP, ...





Mises à jours

Rappels risques :

```
Virus = logiciel malveillant

Failles logiciels
  - installation de logiciel sans contrôle de l'utilisateur
  - accès à distance (attention aux mots de passe par défaut)
  - augmentation des privilèges
  - maintient sur le système compromis
  - destruction des traces d'accès


Conséquences:
  - vol de données personnelles, professionnelles
  - destruction des équipements
  - relai d'attaques
```

2. Des machines à jour

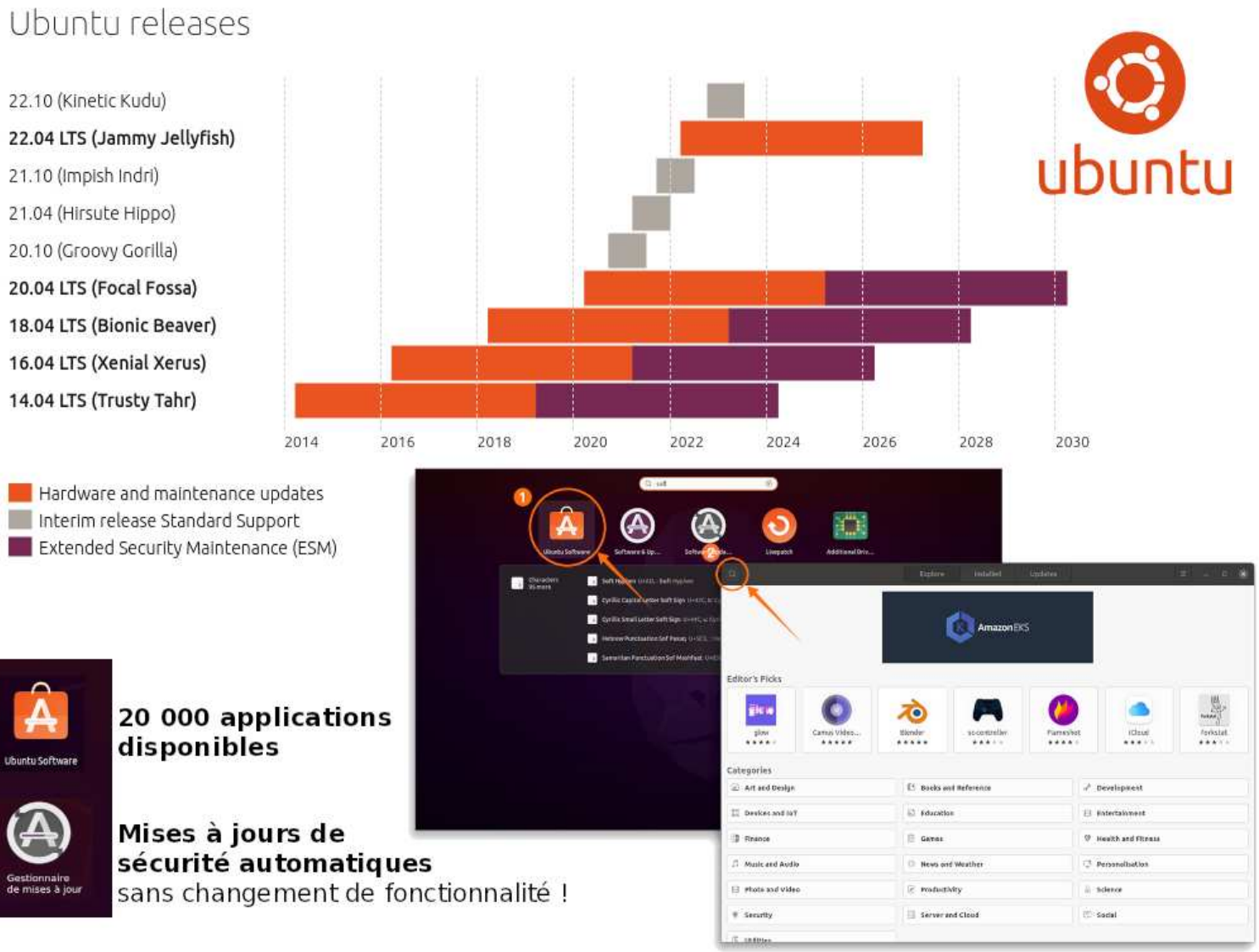
Protection contre les virus :

1. Mises à jour système
   - Windows, MacOS, Linux, Smartphones, ...
2. Mises à jour de toutes les applications
   - ! Choix et téléchargement des applications !
     ✖ Clubic, ✖ Telecharger.com, ✖ ...
3. Mises à jour antivirus et signatures

Optionnels :

- Firewall personnel
- Proxys, VPNs (de confiance)

2. Des machines à jour



☞ sources sûres de téléchargement corrigées par des équipes de sécurité

2. Des machines à jour

☞ Un système obsolète est dangereux

Obsolètes :

- Windows XP, Vista ⇒ EOL Windows 7 : janvier 2020 server 2008
- OS X : actuels 11, 12 (Big Sur : 2020-2023, Monterey : 2024)
  ⇒ EOL 10.15 (Catalina : 2019 - sept. 2022)

- Smartphone
  - Opérateurs ? ⇒ IOS, Android

Objets connectés ? gadgets, caméra, télévision, frigo, chauffage, ...

Connaissances minimales

Rappels risques :

```
Phishing :
 - faux site d'identification: vol de mot de passe
 - faux site de payement: vol des moyens de payements

Faux logiciels : installation de virus

Escroqueries financières :
 - faux virus
 - fausses solutions de protections
 - fausse assistance
 - faux contacts
 - faux virements
 - romances
 - ... [imagination des escrocs] ...


Désinformation
```

3. Une valeur sure : le bon sens !

Phishing = usurpe l'identité de l'émetteur

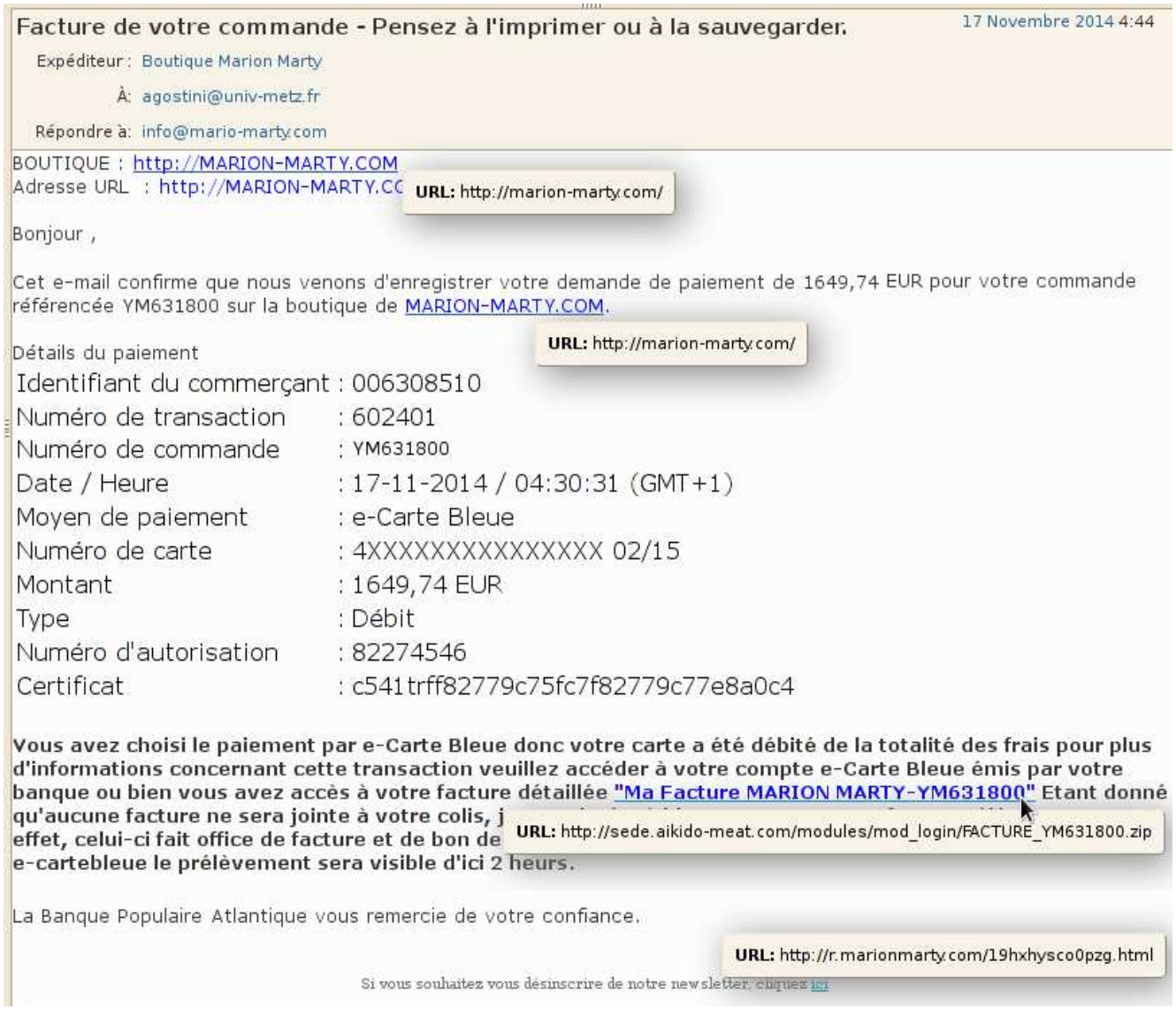
- Mail (réseaux sociaux) ⇒ nom et adresse de l'expéditeur non garantis
  - lien vers site malicieux
  - escroquerie au président

- Téléphone ⇒ numéro affiché non garanti
  - swating
  - escroquerie au président
  - rappel vers numéro surtaxé

- SMS ⇒ numéro affiché non garanti
  - numéro surtaxé
  - téléchargement d'application malicieuse

☞ **L'assistance n'a pas besoin de votre mot de passe**
(comme votre code de carte bleue)

3. Bon sens> Phishing



Facture de votre commande - Pensez à l'imprimer ou à la sauvegarder. 17 Novembre 2014 4:44

Expéditeur : Boutique Marion Marty
À: agostini@univ-metz.fr
Répondre à: info@mario-marty.com

BOUTIQUE : http://MARION-MARTY.COM
Adresse URL : http://MARION-MARTY.CC

URL: http://marion-marty.com/

Bonjour ,

Cet e-mail confirme que nous venons d'enregistrer votre demande de paiement de 1649,74 EUR pour votre commande référencée YM631800 sur la boutique de MARION-MARTY.COM.

URL: http://marion-marty.com/

Détails du paiement

Identifiant du commerçant	: 006308510
Numéro de transaction	: 602401
Numéro de commande	: YM631800
Date / Heure	: 17-11-2014 / 04:30:31 (GMT+1)
Moyen de paiement	: e-Carte Bleue
Numéro de carte	: 4XXXXXXXXXXXXXX 02/15
Montant	: 1649,74 EUR
Type	: Débit
Numéro d'autorisation	: 82274546
Certificat	: c541trff82779c75fc7f82779c77e8a0c4

Vous avez choisi le paiement par e-Carte Bleue donc votre carte a été débité de la totalité des frais pour plus d'informations concernant cette transaction veuillez accéder à votre compte e-Carte Bleue émis par votre banque ou bien vous avez accès à votre facture détaillée "Ma Facture MARION MARTY-YM631800" Etant donné qu'aucune facture ne sera jointe à votre colis, j effet, celui-ci fait office de facture et de bon de e-cartebleue le prélèvement sera visible d'ici 2 heurs.

URL: http://sede.aikido-meat.com/modules/mod_login/FACTURE_YM631800.zip

La Banque Populaire Atlantique vous remercie de votre confiance.

URL: http://r.marionmarty.com/19hxhysco0pzg.html

Si vous souhaitez vous désinscrire de notre newsletter, cliquez ici

Premier réflexe : survol des liens

3. Bon sens> URL

Savoir lire une URL : *URL ≡ adresse postale de doc.*

URL

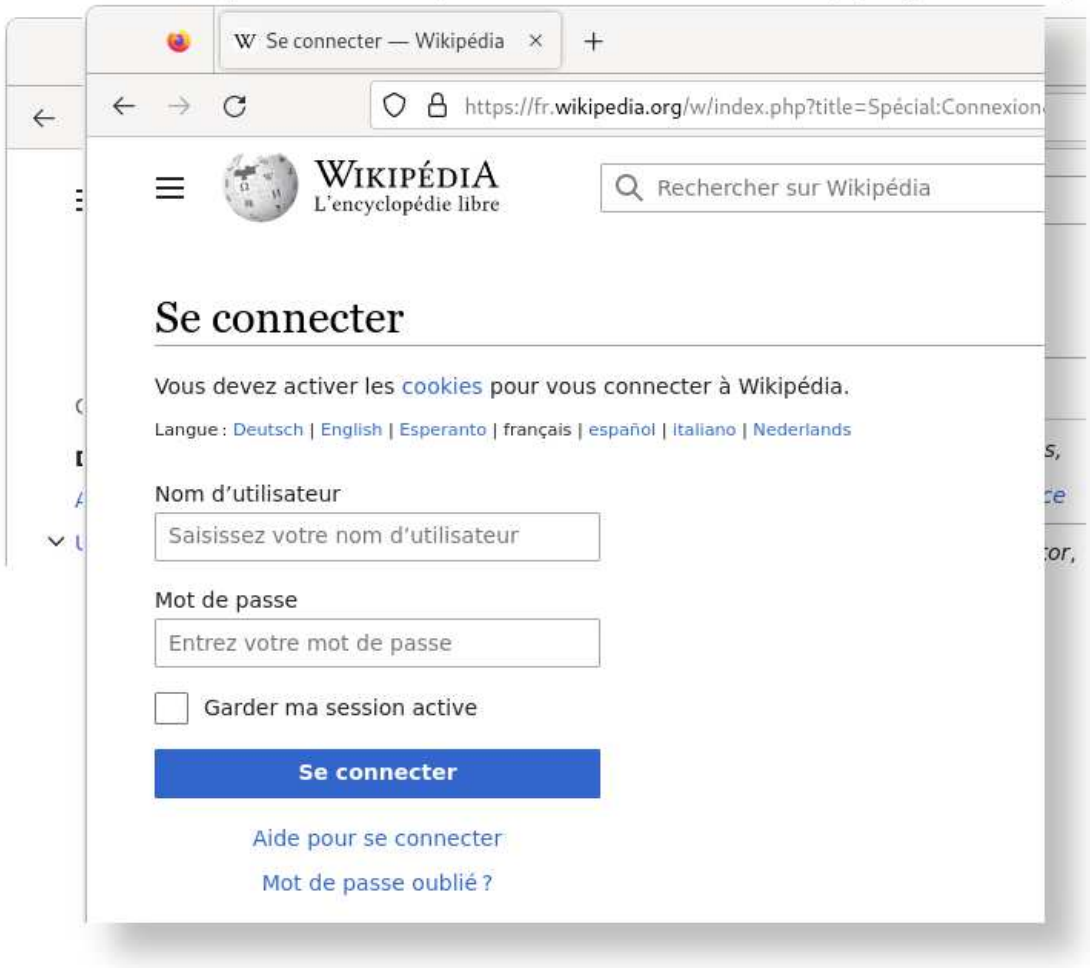
Localisation **unique** de chaque document: fichier, page HTML, image,...

3. Bon sens> URL

Savoir lire une URL : *URL ≡ adresse postale de doc.*

URL

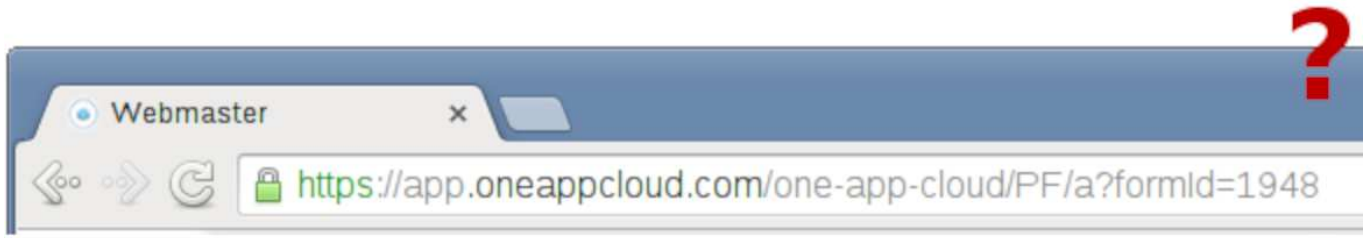
Localisation **unique** de chaque document: fichier, page HTML, image,...

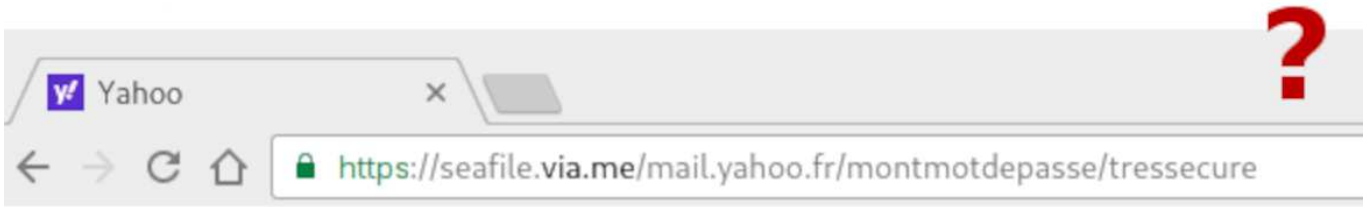


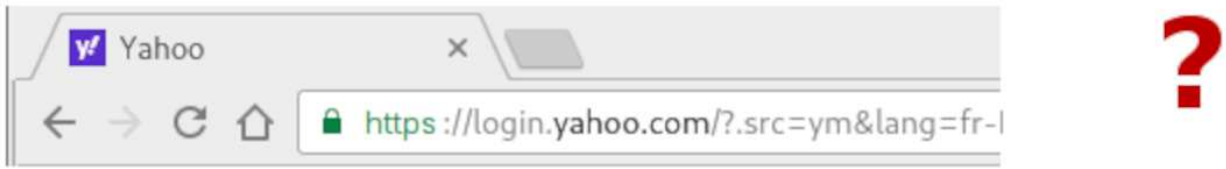
☞ **Surtout au moment de mettre ses identifiants !**

3. Bon sens> URL

Quelle URL est sûre ?







3. Bon sens

- **Lire l'URL**, l'adresse mail
- 99,999% des documents Excel, Word n'ont **pas de macro**
- Limiter l'accès à vos machines/smartphone (mot de passe, schéma)

- La curiosité est un vilain défaut
- Vous ne recevez ni colis, ni facture, ni aide inattendue
  - Vérifiez, rappelez vos correspondants
- La reine d'Angleterre ne vous a pas choisi comme héritier.e.
- On n'a pas enregistré votre webcam («sextorsion»)
- Les «romances» virtuelles sont des escroqueries à moyen et long terme

- Bulle d'information, Astroturfing ⇒ illusion de consensus
- «flood the zone with shit», Bannon 2018

Sauvegardes

Rappels risques :

```
Vol/perte des supports:
  - clés usb
  - disques durs
  - portables
  - smartphone


Ransomware:
  - chiffrement des données contre demande de rançon


Sabotage:
 - destruction malveillante des données et systèmes
```

Vos données ont de l'importance

- Utilisation des espaces mis à disposition pour les données
  - partage sur réseau local
  - cloud public (chiffrer les données)
- Éviter la perte de données (postes nomades, supports amovibles, . . .)
  - Chiffrement des équipements mobiles

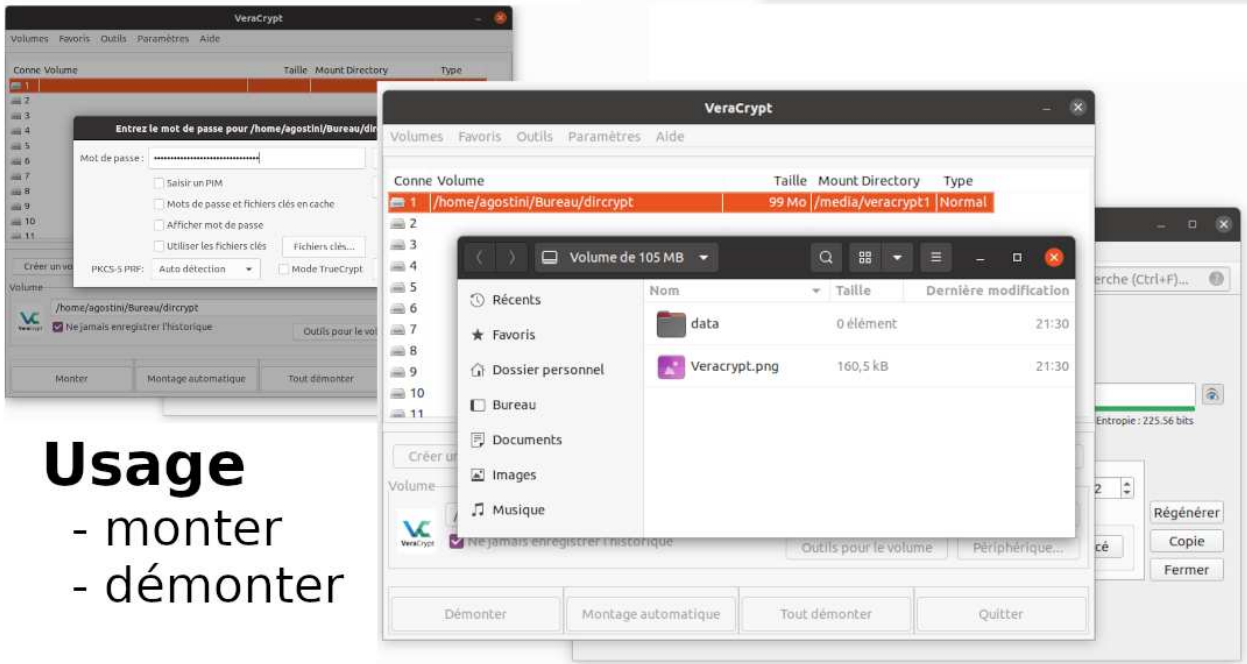
... et copies chiffrées régulières sur supports non connectés

4. Données > Chiffrement

Chiffrer les données dans des dossiers : VeraCrypt ✔

Création

Assistant :
- taille
- password (Keepass)



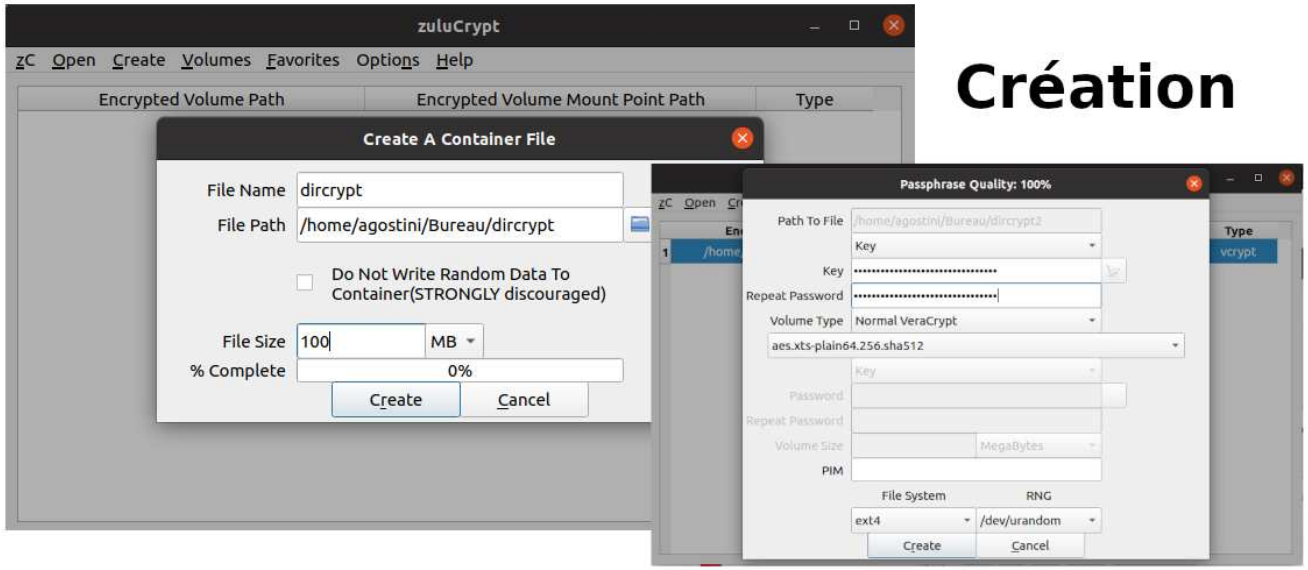
Usage

- monter
- démonter

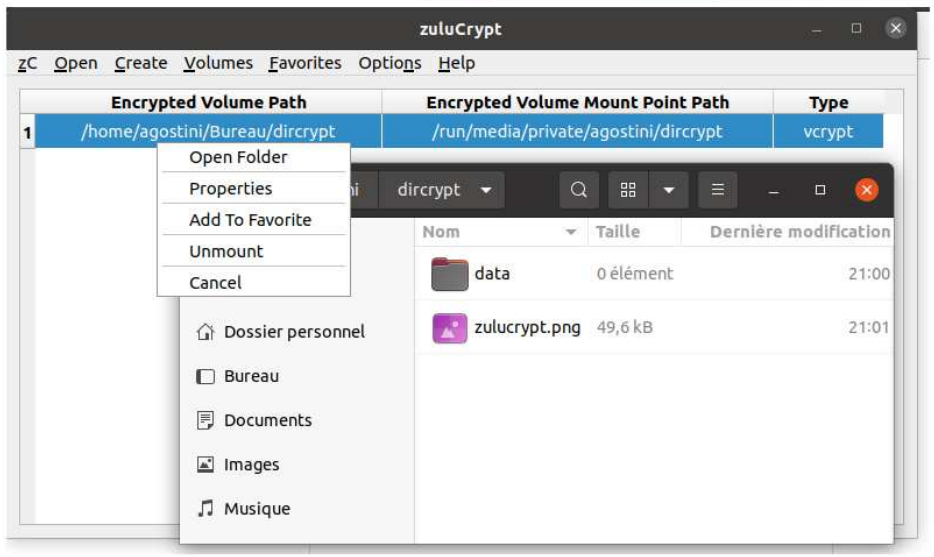
4. Données > Chiffrement

Chiffrer les données dans des dossiers : ZuluCrypt (packagé) ✔

Création



Usage

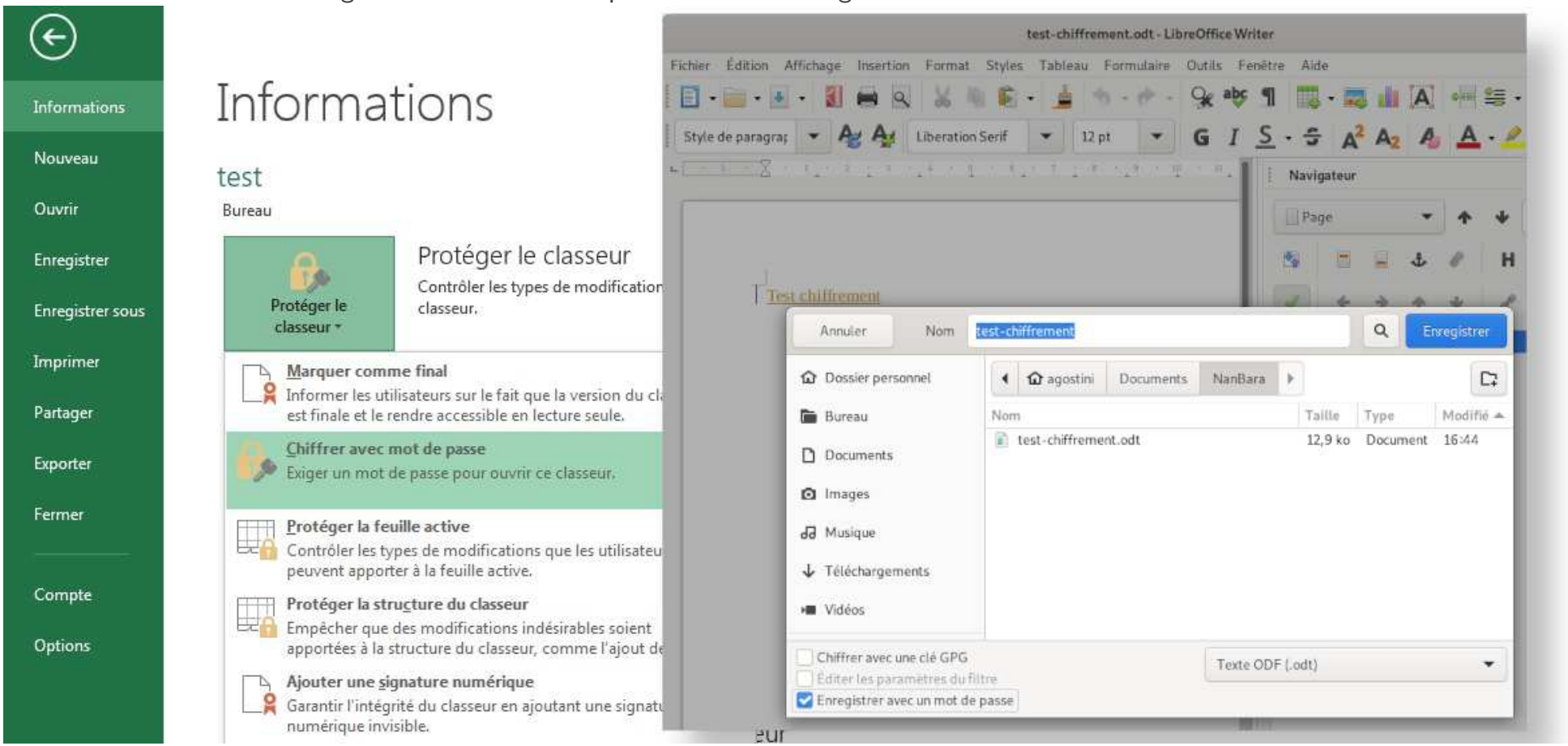


4. Données > Chiffrement

Chiffrer les données dans des dossiers : VeraCrypt ✔

Chiffrement simple avec mot de passe partageable :

Office : menu "Fichier" > "Informations"
LibreOffice : cochez "✔ Enregistrer avec un mot de passe" lors de l'enregistrement du fichier



À retenir

Risques :

- phishing
- logiciels malveillants
- désinformation
- vol de données personnelles

Mesures à prendre :

1. Mots de passe
2. Mises à jours
3. Bon sens avec connaissances minimales
4. Sauvegardes

☞ *Il n'y a pas de fatalité à se faire escroquer*