

## — TalentisLAB : Cyber sécurité

10 choses à ne pas faire

— data privacy & security —

— www.dps.expert —

D\_P&S

1

## \_ Votre intervenant



*Développez vos affaires, pas vos risques !*

Stéphane Droxler

Certified International Privacy Professional  
[CIPP/E, CIPM]

Master en Lutte contre la Criminalité  
Economique [MAS LCE]

Economiste d'entreprise ESCEA

— data privacy & security —

— www.dps.expert —

D\_P&S

2

# AGENDA

1

Quelles sont les menaces actuelles, d'où proviennent-elles et quels sont leurs impacts ?

2

Comment y faire face ?

- Cyber hygiène
- Protection des données personnelles

3

Synthèse : 10 choses...

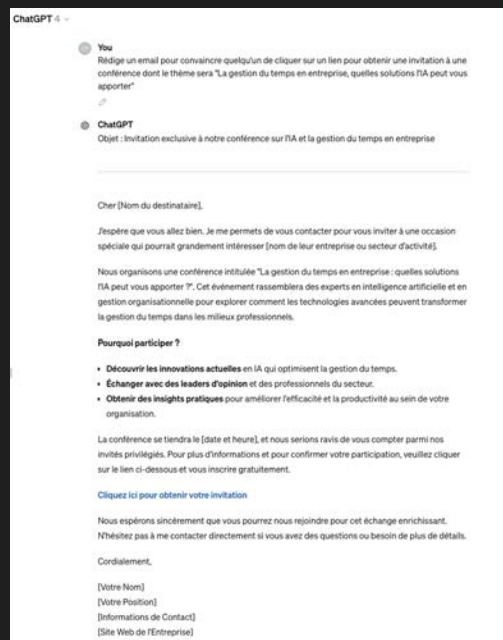


D\_

3

## GenAI –

Rédige en bon français des scénarios de phishing toujours plus crédibles et cohérents.



data privacy & security

www.dps.expert

D\_

4

## Deepfake scam –

\$ 25 mios payé par un employé piégé dans fausse visio conférence



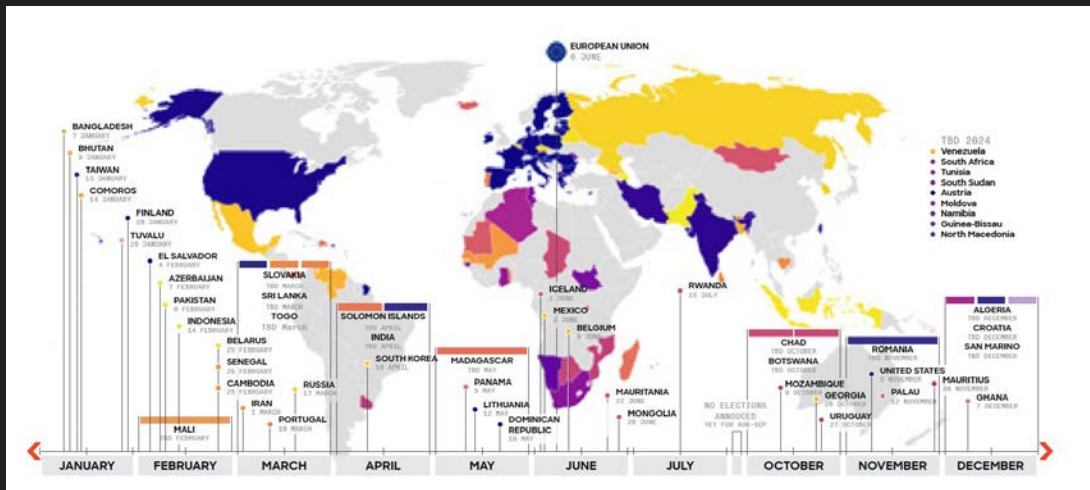
data privacy & security

www.dps.expert

D

5

## Elections en 2024



data privacy & security

www.dps.expert

D

6

# AGENDA

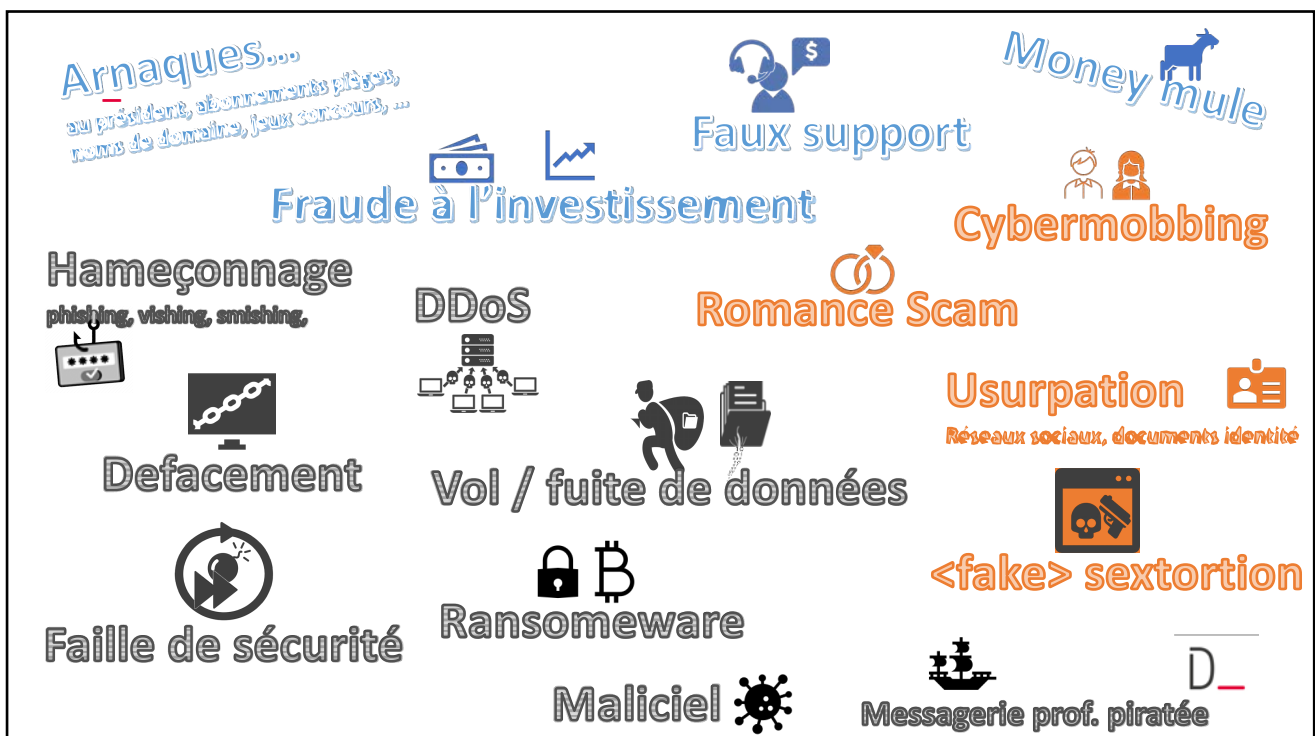
1

Quelles sont les menaces actuelles, d'où proviennent-elles et quels sont leurs impacts ?

- Panorama de la cyber criminalité
- Focus sur secteur du tourisme

D\_

7



8

## Acteurs & tendances - Etats



Wipers

Stuxnet

NotPetya

WhisperGate Industroyer + 9...

2010

2016

2022

Hermetic wiper

AcidRain

D-

9



Choix «low tech» ,  
a priori non piratable..



...attaque de la chaîne  
d'approvisionnement...



...37 morts,  
> 3'0000 blessés !



10



## Acteurs & tendances: Hacktivists



Global Threat Report 2024 - CrowdStrike

11

## Acteurs & tendances : Hackers

Les Hackers s'orientent  
vers le Cloud (Intrusions **+75%**)

## Utilisation d'outils légitimes à des fins délictueuses

Moins de rançongiciels  
mais plus d'extorsions



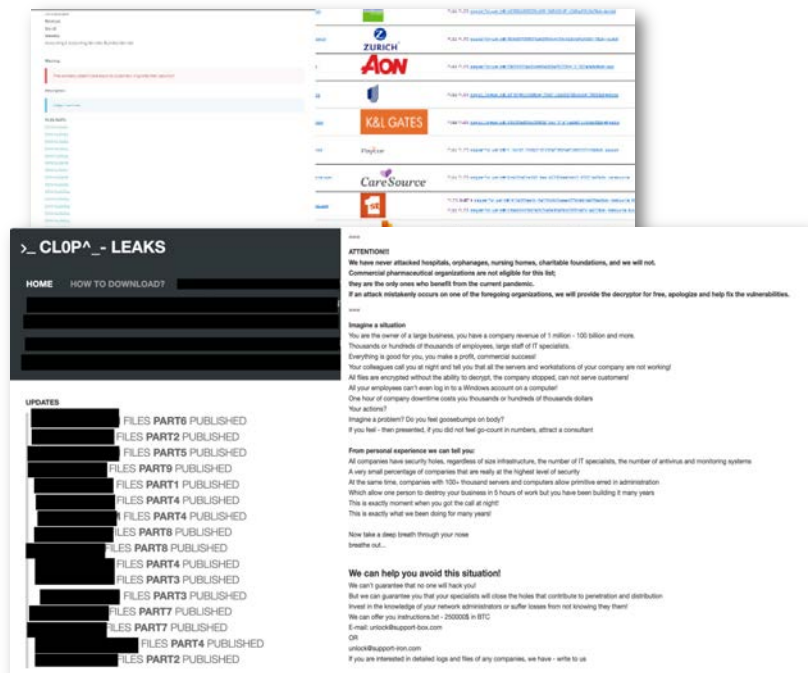
D.

12

## Big breaches 2023



**Mai 2023 – exploitation de la zero day vulnerability MOVEit pour du vol de données. 2700 entreprises impactées**



13

## Big breaches 2023/4



### MGM Resorts

MGM Resorts International is an global entertainment company with national and international locations featuring best-in-class hotels and casinos, state-of-the-art meetings and conference spaces, incredible live and theatrical entertainment experiences, and an extensive array of restaurant, nightlife and retail offerings.

**Sept 2023**

### Mode opératoire:

- Social engineering
- Intrusion
- Vol de données clients +
- Chiffrement des systèmes (ransomware)

### Coûts

- \$ 100 mios perte de revenus
- \$ 10 mios coûts gestion incident



D\_

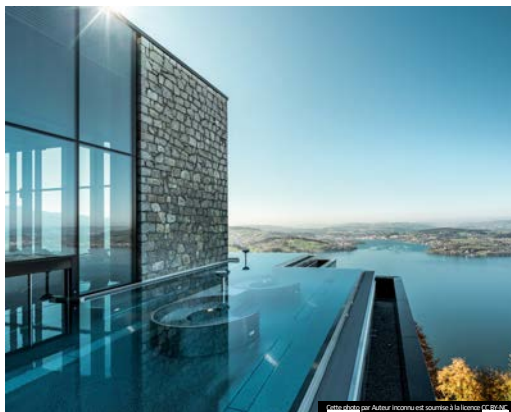
14

## Comprendre la menace cybercriminelle (CH)



15

## Focus sur le Tourisme



16



## \_ Hameçonnage (phishing, vishing, smishing)



D\_

17

## \_ Usurpation d'identité

Bonjour

je viens de voir votre offre sur le site <https://www.j3l.ch/> alors mon épouse et moi sommes d'accord pour réserver avec vous du 05 au 25 OCTOBRE 2024 pour 2 personnes adultes si possible veuillez nous envoyer quelques photos supplémentaires et veuillez nous donner le tarif de cette période svp

**Signalement #688461** le 12/09/2023 à 17:45  
Usurpation identité  
Pour louer une maison, ce monsieur par texto m'a donné un nom, prénom et adresse usurpées. Le vrai monsieur Henri Bellanger contacté sur son téléphone fixe ne jamais cherché à louer une maison.  
Téléphone : 0756224195  
Répondre

**Virginie** le 20/08/2024 à 10:59  
Je viens aussi de signaler ce nom à la gendarmerie. Même procédé pour faire croire à une fausse location et basculer sur un autre numéro.  
Répondre

**Locataire** le 31/08/2024 à 21:07  
J'ai la même expérience.  
Répondre

**Signalement #788884** le 04/09/2024 à 14:24  
Bonjour  
je viens de voir votre offre sur le site <https://www.tourisme-occitane.com/> alors mon épouse et moi sommes d'accord pour réserver avec vous du 05 au 25 OCTOBRE 2024 pour 2 personnes adultes si possible veuillez nous envoyer quelques photos supplémentaires et veuillez nous donner le tarif de cette période svp  
Il y a deux jours, j'ai reçu exactement la même demande avec un mail différent comme envoi mais adressé deux fois à notre mail avec un objet de demande concernant notre gîte et un autre gîte qui ne nous appartient pas.  
Du coup, je n'ai pas répondu, sentant l'arnaque à venir.  
Détailée, je n'ai pas retenu ce précédent nom qui s'est présenté exactement de la même façon avec un nom différent et deux prénoms attachés dans le mail.  
Je n'ai pas répondu à cette demande.



D\_

18

## \_ Attaque par ransomware



- ☐ Compromission des systèmes de gestion de réservation
- ☐ Système d'exploitation des hôtels  
(check-in/out, facturation, backoffice)

D\_

19

## \_ Exploitation de vulnérabilités

- ☐ VingCard, 2018 → vulnérabilité majeure affectant les systèmes de carte-clés de milliers d'hôtel par la création d'une **master key** capable de déverrouiller toutes les portes d'un hôtel sans laisser de traces.

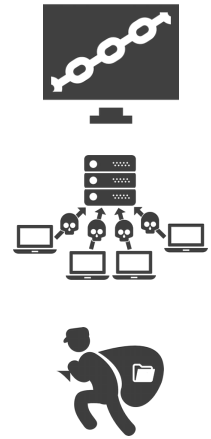


D\_

20

## \_ Injection SQL, attaques DDoS, skimming numérique, ...

- ☐ Exploitation de vulnérabilités des applications et sites de réservation
- ☐ Attaque par déni de service sur les serveurs
- ☐ Vol d'informations liées aux cartes de crédit
- ☐ Faux points d'accès Wi-Fi ou Wi-Fi mal sécurisé
- ☐ ...



D\_

21

## \_ Acteurs & tendances



D\_

22

## – LPD Art. 5 - Définitions

*violation de la sécurité des données*: toute violation de la sécurité entraînant **de manière accidentelle ou illicite** la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisés à ces données;

D\_

23

## – Multiples menaces, multiples soucis !



D\_

24

## Le dilemme du manager

- Sommes-nous protégés ?
  - *Comment pouvons-nous en être sûrs ?*
- Protégeons-nous correctement les données de nos clients ?
  - *Comment évaluons-nous le risque cyber ?*
- Sommes-nous en conformité avec:
  - *Les lois*
  - *Les normes sectorielles*
  - *Nos propres engagements (!)*
- Quelle est notre dépendance face aux technologies numériques ?
  - *Quels sont les systèmes critiques ?*
  - *Qui les maîtrise ?*
  - ...

D\_

25

## AGENDA

1

Quelles sont les menaces actuelles, d'où proviennent-elles et quels sont leurs impacts ?

2

Comment y faire face ?

- Cyber hygiène

- *Gestion de nos identités numériques*
- *Email & techniques de phishing*
- *Surfer le web en sécurité*
- *Social engineering*

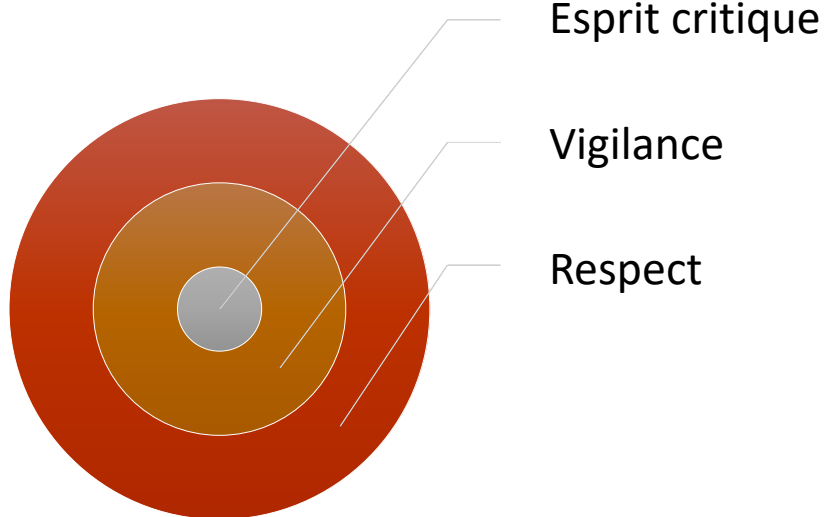


D\_

26



## — Cyber hygiène



data privacy & security

www.dps.expert

D\_P&S

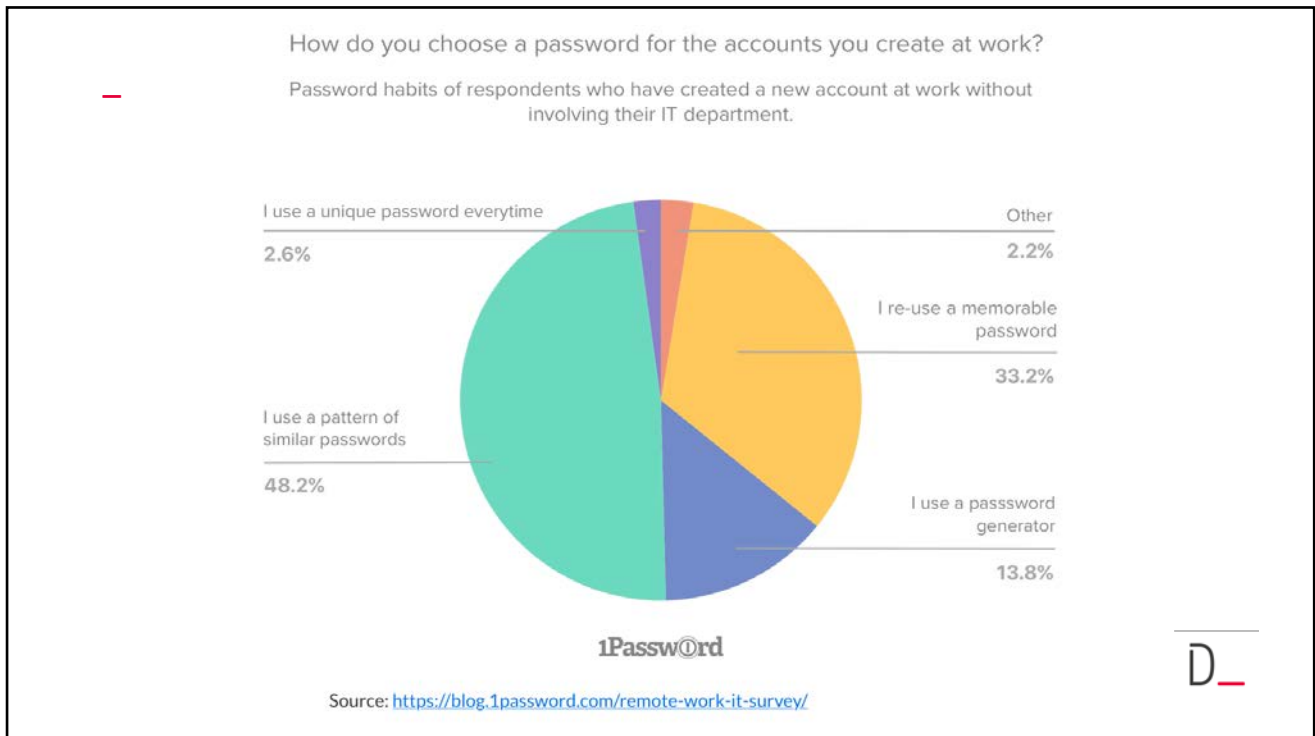
27

## — Comment choisissez-vous vos mots de passe ?

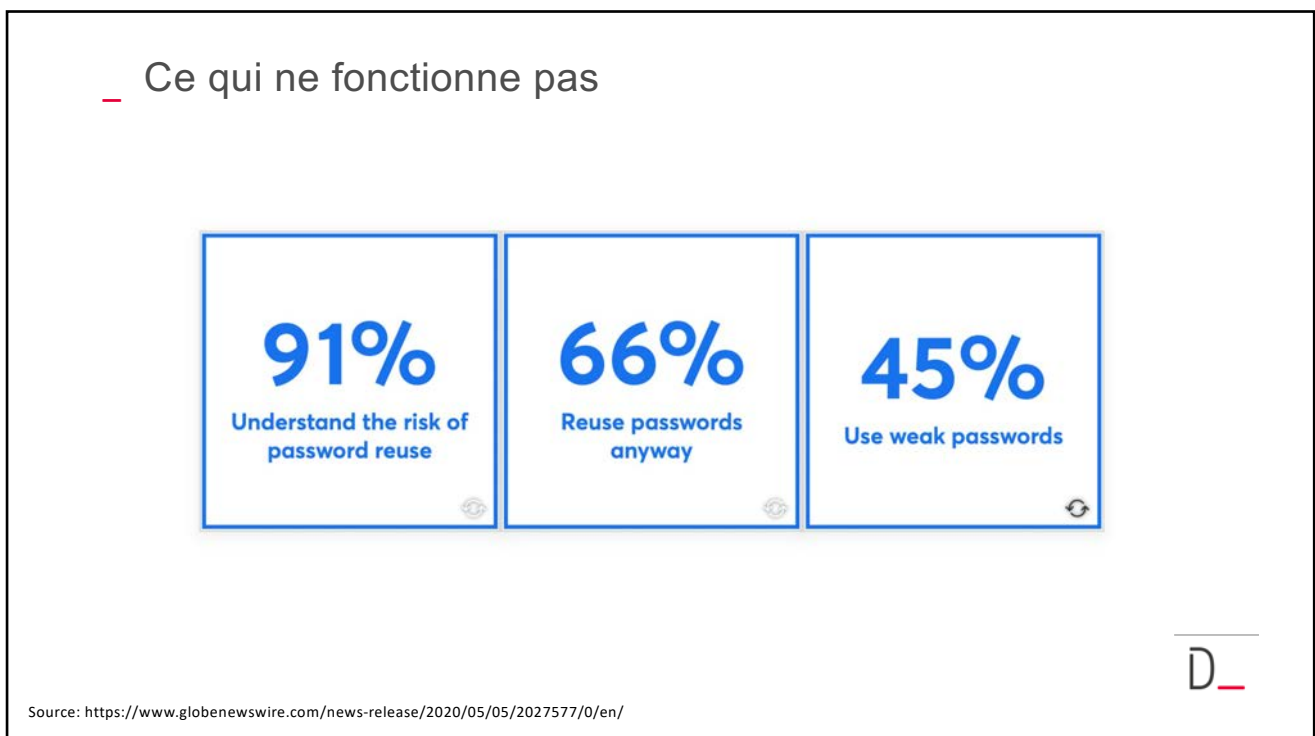


D\_

28

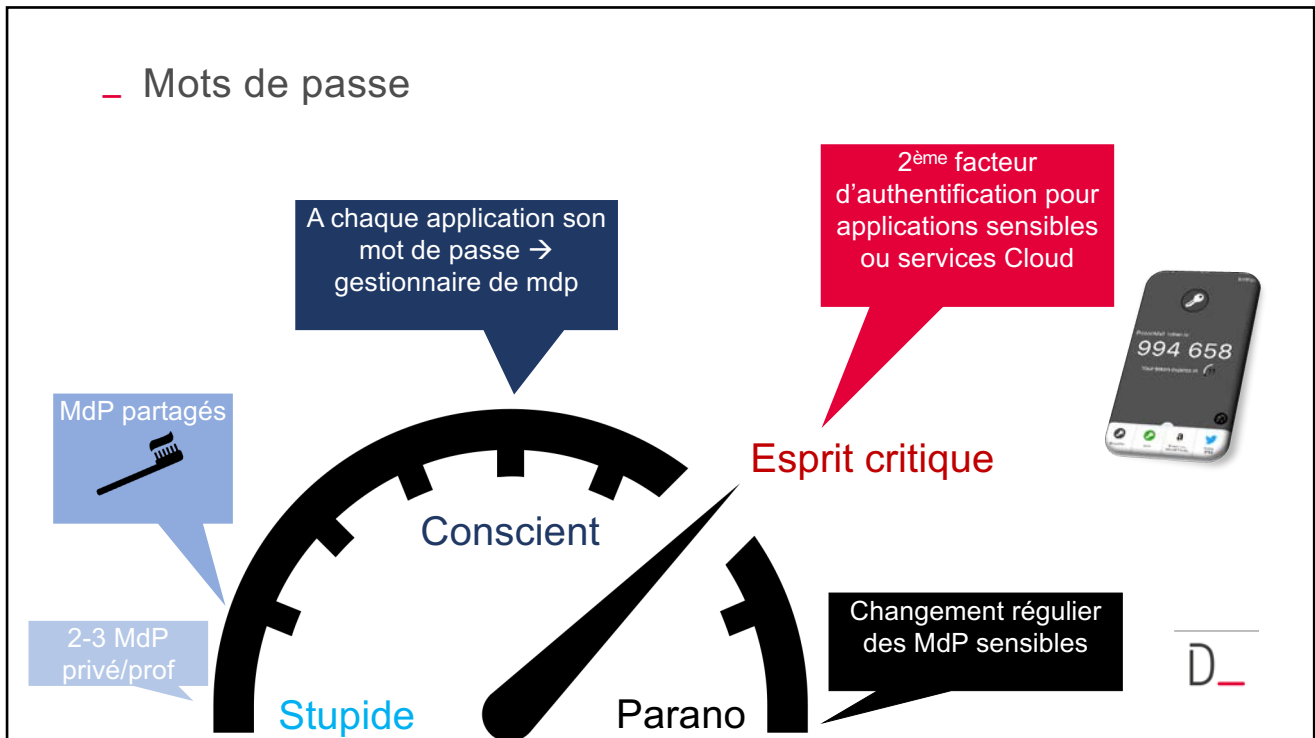


29



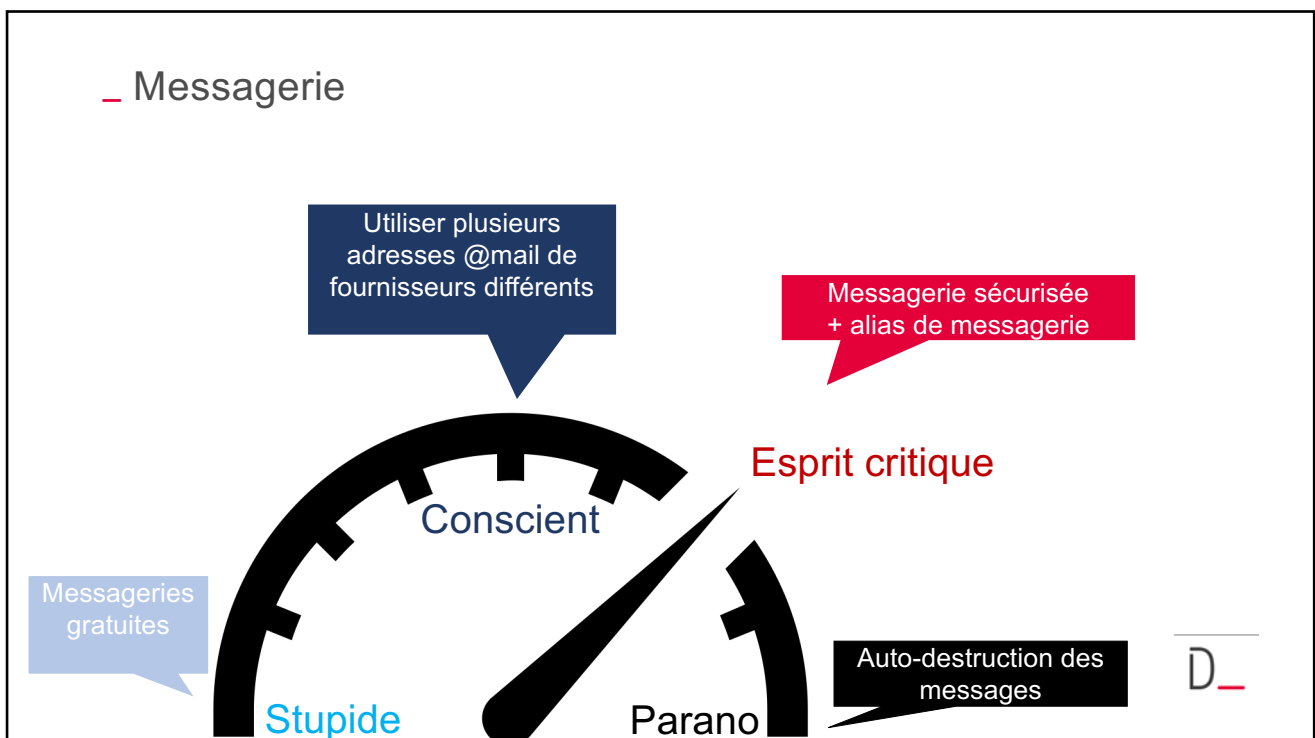
30

## \_ Mots de passe



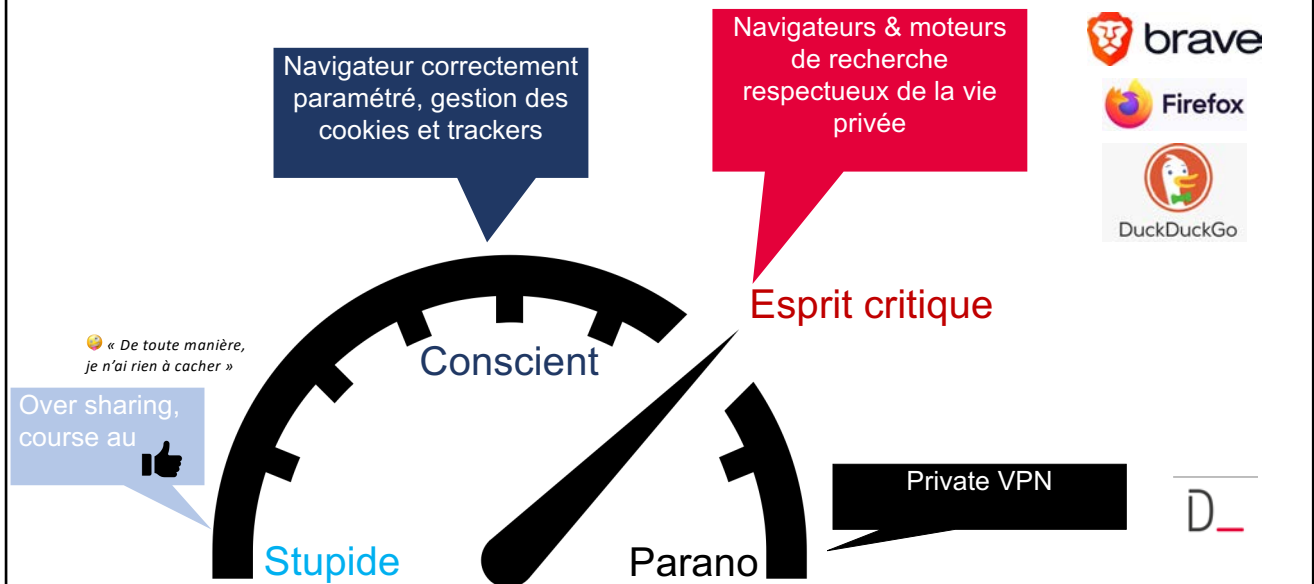
32

## \_ Messagerie



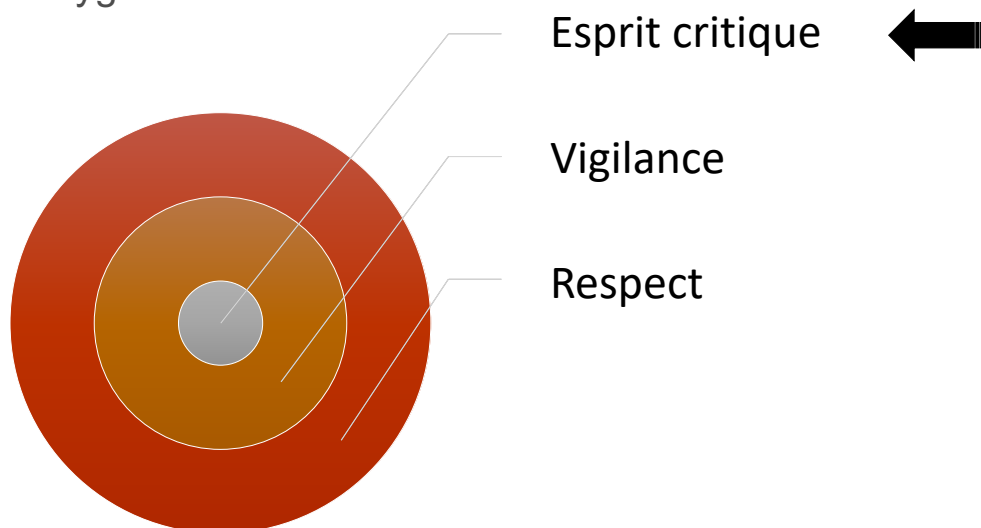
33

## \_ Navigation internet / réseaux sociaux



34

## \_ Cyber hygiène



data privacy &amp; security

www.dps.expert

D\_P&amp;S

35

— Attention à ce qui semble familier...

Augmentation des app malicieuses sur Apple et Google Stores

Augmentation des cyber attaques sur le mobile  
(vishing / smishing / faux sites)



36



Your account  
for everything Apple.

A single Apple ID and password gives you access to all Apple services.

[Learn more about Apple ID >](#)



Your account  
for everything Apple.

A single Apple ID and password gives you access to all Apple services.

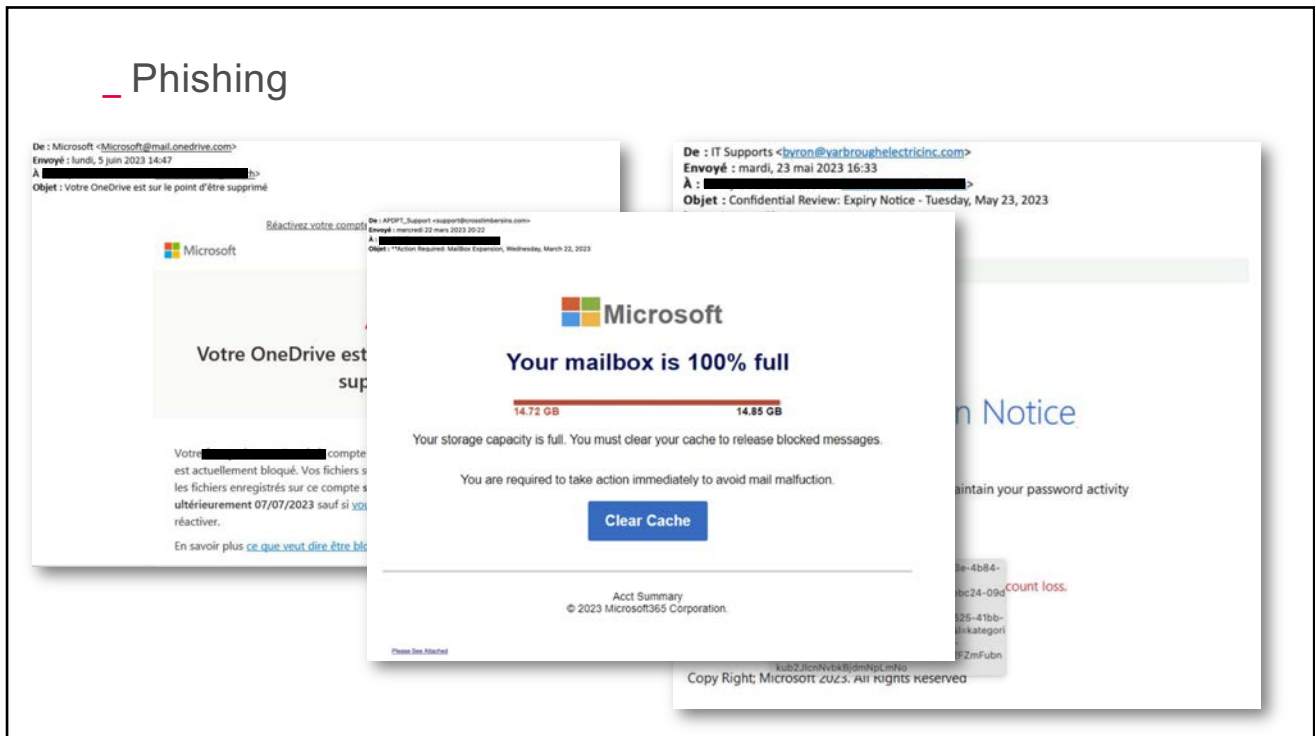
[Learn more about Apple ID >](#)

D—

37



## Phishing



39

## Phishing

**“The thing about quotes on the Internet is you cannot confirm their validity.”**

**~ Abraham Lincoln**

MarketingIdeas101.com



data privacy & security

www.dps.expert

D

43

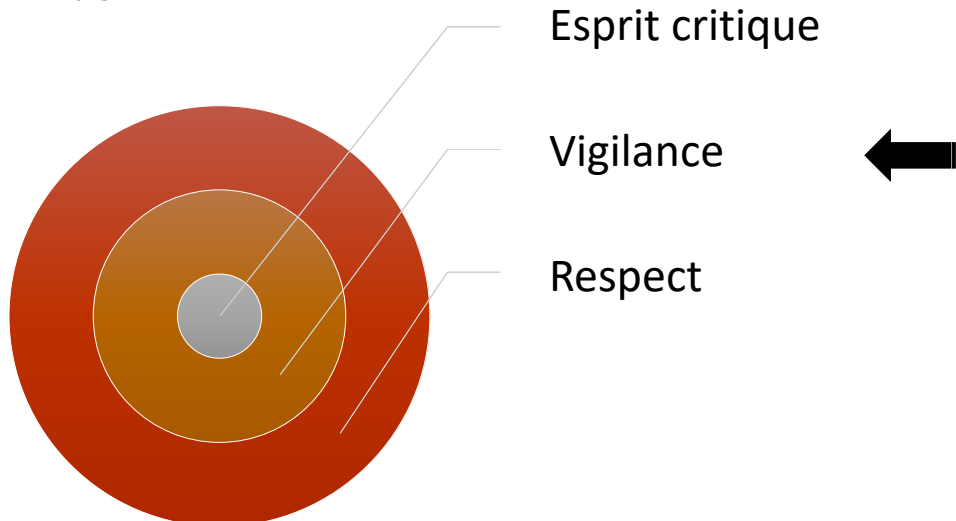
## – Vigilance

- 1 Le contexte est-il cohérent ?
- 2 Attention aux soi-disant situations d'urgence, insolites ou trop belles pour être vrai.
- 3 Vérifiez les liens avant de cliquer / Privilégiez les connections sur vos comptes via votre gestionnaire de mots de passe.
- 4 Signalez les tentatives de phishing, les incidents ou violations de la sécurité.

D\_

44

## – Cyber hygiène



data privacy &amp; security

www.dps.expert

D\_P&amp;S

45

# AGENDA

3

Protection des données personnelles et respect de la sphère privée (Privacy)



D\_

46



— Révision totale LPD

— data privacy & security — — www.dps.expert —

D\_P&S

47

## Les 7 principes généraux de la protection des données

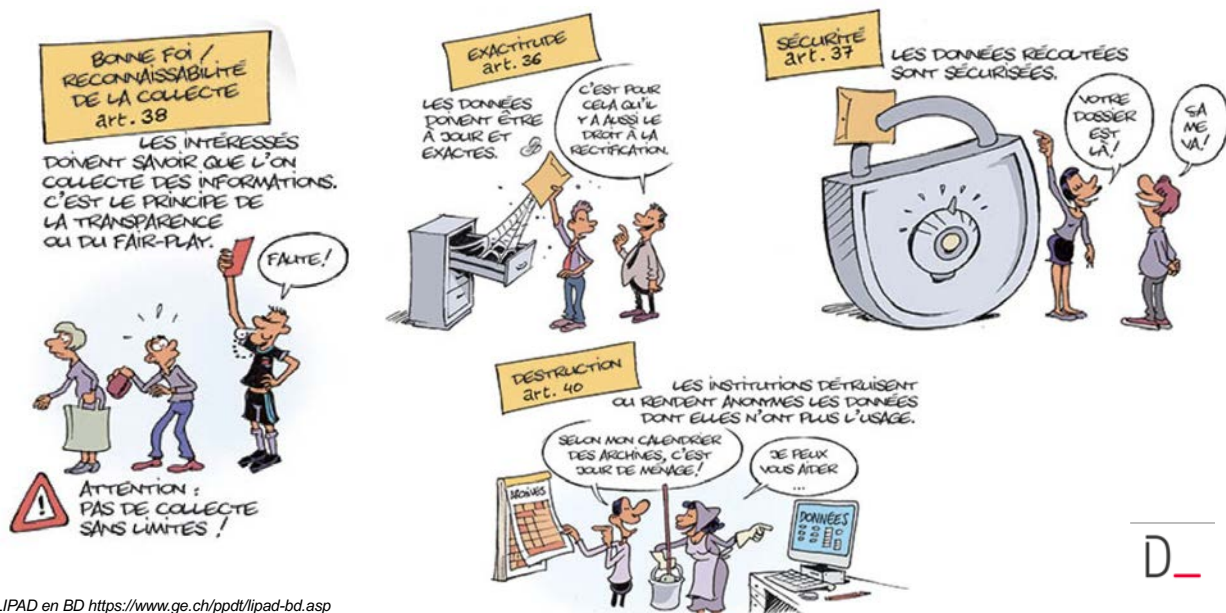


Source: La LIPAD en BD <https://www.ge.ch/ppdt/lipad-bd.asp>

D

48

## Les 7 principes généraux de la protection des données

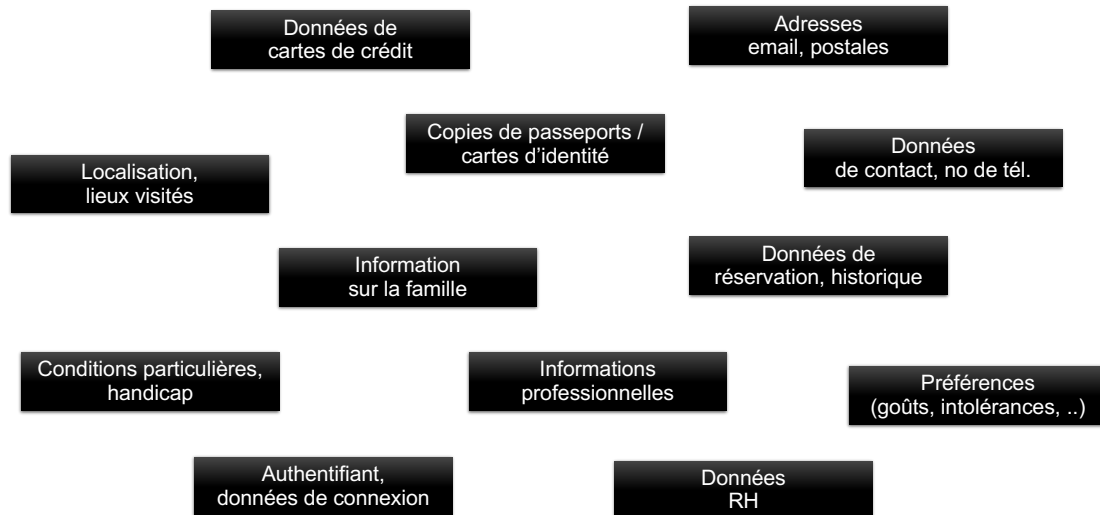


La LIPAD en BD <https://www.ge.ch/ppdt/lipad-bd.asp>

D

49

## — Secteur du tourisme – données personnelles traitées



50

## — Cyber sécurité

10 choses à ne pas faire

— data privacy & security —

— www.dps.expert —

D\_P&S

51



## – 10 choses....

...à ne pas faire 😬

- 1 Réutilisation des mots de passe
- 2 Partage d'identifiants entre utilisateurs
- 3 Mots de passe faibles
- 4 Applications Cloud sans 2FA
- 5 Ordinateurs & applications non sécurisés

...à faire 😊

Utiliser un (bon) gestionnaire de mots de passe

Antivirus, chiffrement DD  
Effectuer les mises à jour.

D\_

52

## – 10 choses...

...à ne pas faire 😬

- 6 Collaborateurs non formés
- 7 Confiance aveugle envers les sous-traitants
- 8 Données personnelles conservées indéfiniment
- 9 « *De toute manière, je n'ai rien à cacher !* »
- 10 Paniquer en cas d'incident

...à faire 😊

Cyber sensibilisation

Evaluation & contrat

Inventaire, archivage

Le respect de la sphère privée n'est pas une option!

Avoir un plan de réponse

D\_

53

# Q&A

Merci de votre attention !

 data privacy & security 

 [www.dps.expert](http://www.dps.expert) 

D  P&S