

## — 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  
[CIIPP/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

1

# 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.

ChatGPT-4 -

You  
Rédige un email pour convaincre quelqu'un de cliquer sur un lien pour obtenir une invitation à une conférence dont le thème sera "La gestion du temps en entreprise, quelles solutions l'IA peut vous apporter"

ChatGPT  
Objet : invitation exclusive à notre conférence sur l'IA et la gestion du temps en entreprise

Cher [Nom du destinataire],

J'espère que vous allez bien. Je me permets de vous contacter pour vous inviter à une occasion spéciale qui pourrait grandement intéresser [nom de leur entreprise ou secteur d'activité].

Nous organisons une conférence intitulée "La gestion du temps en entreprise : quelles solutions l'IA peut vous apporter". Cet événement rassemblera des experts en intelligence artificielle et en gestion organisationnelle pour explorer comment les technologies avancées peuvent transformer la gestion du temps dans les milieux professionnels.

Pourquoi participer ?

- Découvrir les innovations actuelles en IA qui optimisent la gestion du temps.
- Échanger avec des leaders d'opinion et des professionnels du secteur.
- Obtenir des insights pratiques pour améliorer l'efficacité et la productivité au sein de votre organisation.

La conférence se tiendra le [date et heure], et nous serions ravis de vous compter parmi nos invités privilégiés. Pour plus d'informations et pour confirmer votre participation, veuillez cliquer sur le lien ci-dessous et vous inscrire gratuitement.

[Cliquez ici pour obtenir votre invitation](#)

Nous espérons sincèrement que vous pourrez nous rejoindre pour cet échange enrichissant. N'hésitez pas à me contacter directement si vous avez des questions ou besoin de plus de détails.

Cordialement,

[Votre Nom]  
[Votre Position]  
[Informations de Contact]  
[Site Web de l'Entreprise]

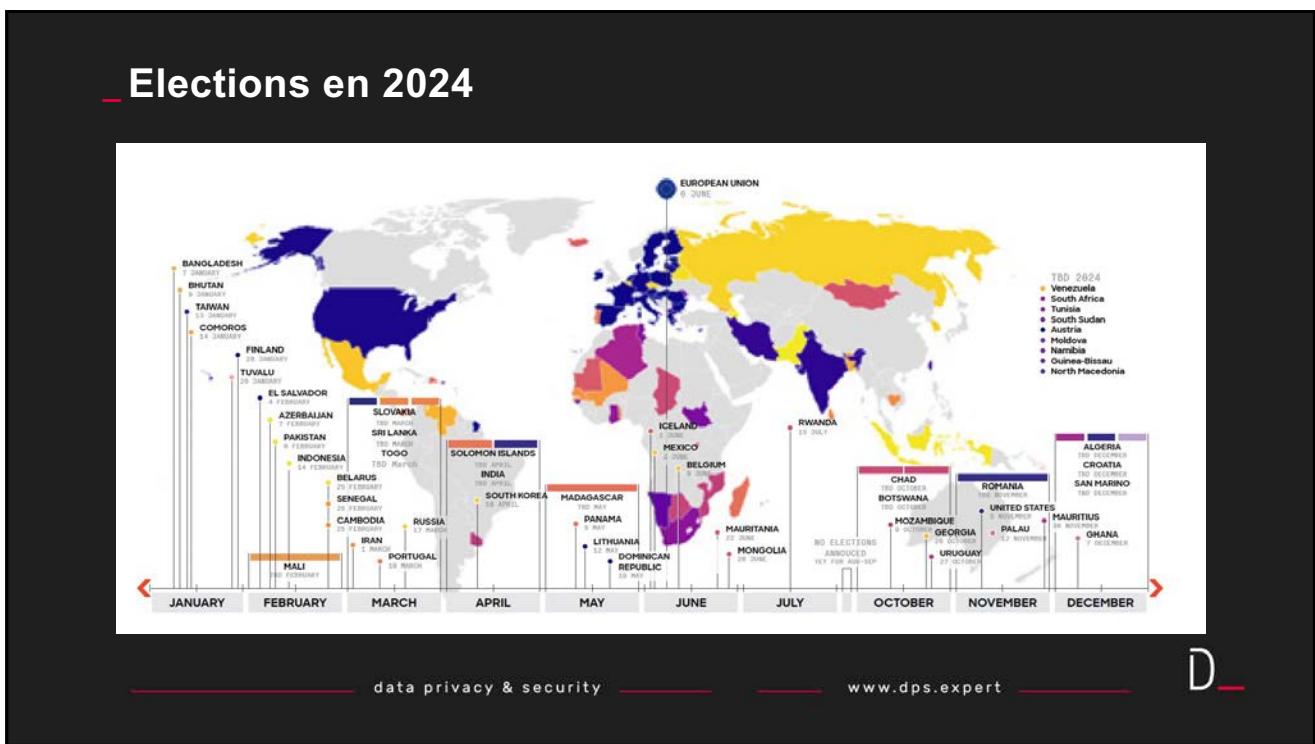
data privacy & security      www.dps.expert      D\_

4

**Deepfake scam – \$ 25 mios payé par un employé piégé dans fausse visio conférence**

data privacy & security | www.dps.expert | D

5



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

<b>Arnaques...</b> <small>au président, abonnements payants, noms de domaine, jeux concours, ...</small>	<b>Fraude à l'investissement</b>	<b>Money mule</b>
<b>Hameçonnage</b> <small>phishing, vishing, smishing,</small>	<b>Faux support</b>	<b>Cybermobbing</b>
<b>Defacement</b>	<b>DDoS</b>	<b>Romance Scam</b>
<b>Faille de sécurité</b>	<b>Vol / fuite de données</b>	<b>Usurcation</b> <small>Réseaux sociaux, documents identité</small>
	<b>Ransomware</b>	<b>&lt;fake&gt; sextortion</b>
	<b>Maliciel</b>	<b>Messagerie prof. piratée</b>

8

## Acteurs & tendances - Etats



Stuxnet

NotPetya

WhisperGate

Industroyer

+ 9...

2010

2016

2022

Hermetic wiper

AcidRain

D

9



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



...37 morts,  
> 3'0000 blessés !



10

## Acteurs & tendances: Hacktivists



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

# Big breaches 2023

Logiciel de transfert de fichiers sécurisé  
MOVEit aide votre entreprise à répondre aux normes de conformité en matière de cybersécurité, à savoir PCI-DSS, HIPAA, RGPD, SOC2 etc. Créez un environnement plus sécurisé pour vos données sensibles, tout en favorisant la fiabilité de vos processus d'entreprise fondamentaux.

[Télécharger](#) [Télécharger le PDF](#)

MOVEit - Vue d'ensemble

MOVEit 2023 - Découvrez toutes les nouveautés de la dernière version [Découvrir](#)

ATTENTION!  
We have never attacked hospitals, orphanages, nursing homes, charitable foundations, and we will not. Certain pharmaceutical organizations are not eligible for this list.  
They are the only ones who benefit from the current policies.  
If an attack mistakenly occurs on one of the foregoing organizations, we will provide the decryptor for free, apologize and help fix the vulnerabilities.

Imagine a situation  
You are the owner of a large business, you have a company revenue of 1 million - 100 billion and more. Thousands or hundreds of thousands of employees, large staff of IT specialists. Everything is good for you, you make a profit, company success.  
Your company has been attacked and all the servers and workstations of your company are not working! All files are encrypted without the ability to decrypt, the company stopped, can not serve customers! All your employees can't even log in to a Windows account on a computer!  
One hour of company downtime costs you thousands or hundreds of thousands dollars  
Now imagine...  
Imagine a problem? Do you feel goosebumps on body?  
If you feel - then presented, if you did not feel go-coat in numbers, attract a consultant.  
From personal experience we can tell you:  
All companies have security holes, regardless of size/infrastructure, regardless of IT specialists, the number of antivirus and monitoring systems. A very small percentage of companies that are really at the highest level of security.  
At the same time, companies with 100, 1000, 100000+ employees and computers allow privilege admin in administration which makes it easy for us to break into your system and destroy your business in 4 hours of work but you have been building it many years  
This is exactly what you got the call for right?  
This is exactly what we been doing for many years!  
Now take a deep breath through your nose  
breath out...

We can help you avoid this situation!  
We can't guarantee that no one will hack you!  
But we can guarantee you that your specialists will close the holes that contribute to penetration and distribution.  
Invest in security, so that your network administrators and suffer losses from knowing them threat.  
We can offer you instructions.txt - 250000\$ in BTC  
E-mail: [unicssupport@unics.com](mailto:unicsupport@unics.com)  
OR  
[unicssupport.unics.com](http://unicsupport.unics.com)  
If you are interested in detailed logs and files of any companies, we have - write to us

13

## Big breaches 2023/4



MGM Resorts

MGM Resorts International is a 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:

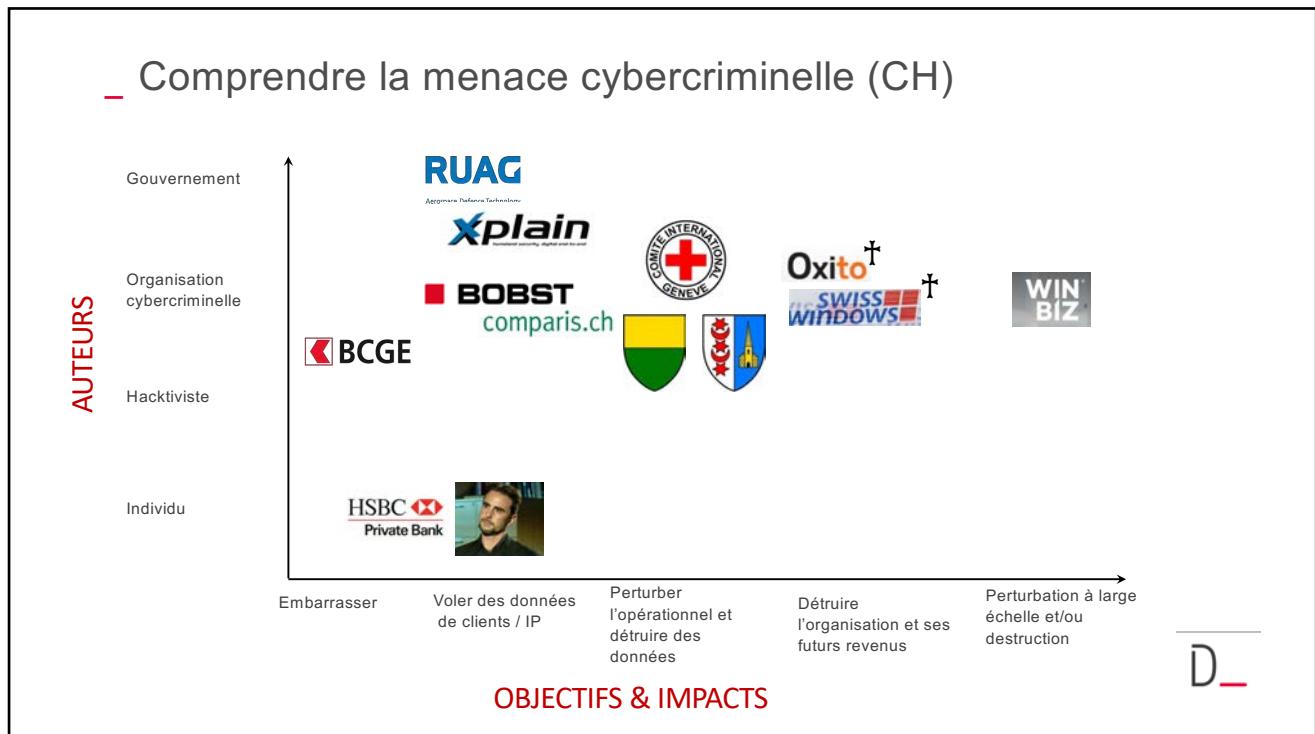
- Social engineering
  - Intrusion
  - Vol de données clients +
  - Chiffrement des systèmes (ransomware)

## Coûts

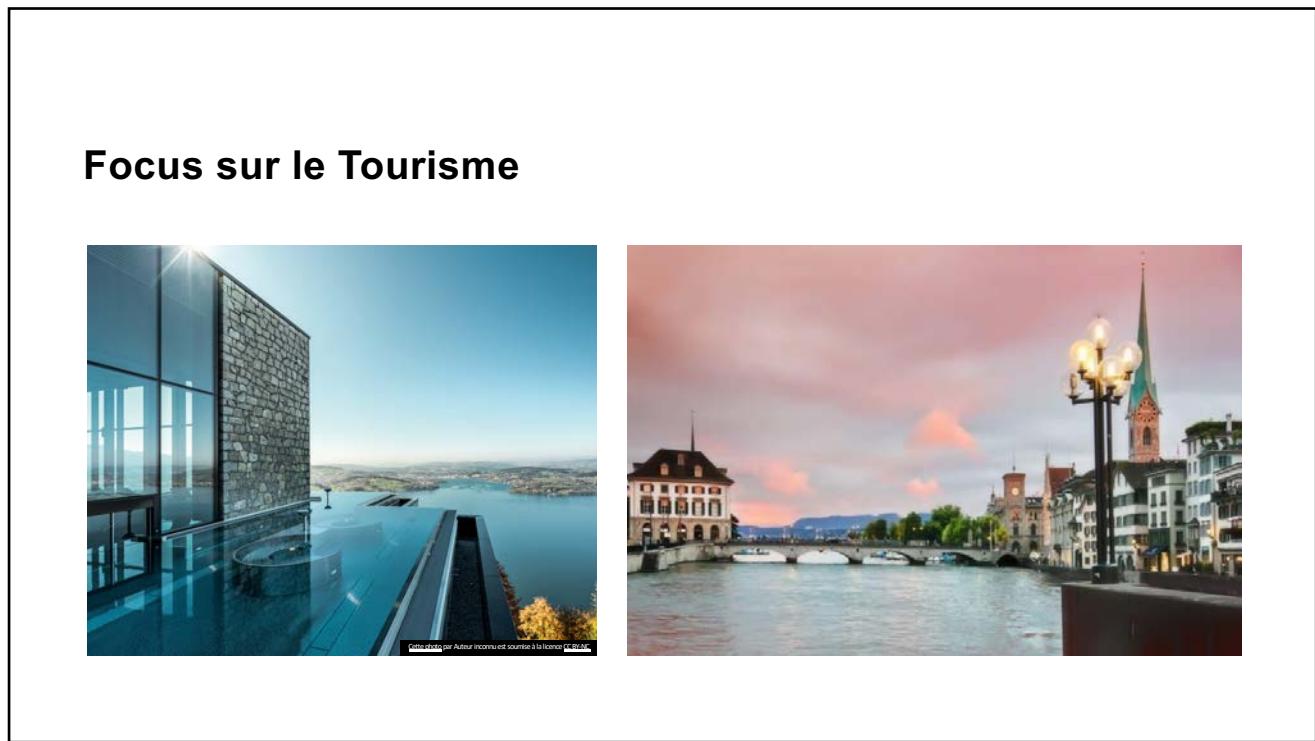
- \$ 100 mios perte de revenus
  - \$ 10 mios coûts gestion incident

D\_

14



15



16

### Hameçonnage (phishing, vishing, smishing)



17

## Usurpation d'identité

Bonjour

je viens de voir votre offre sur le site <https://www.3j.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

Pour louer une maison , ce monsieur par texto m'a donné un nom , prenom et adresse usurpées . Le vrai

monsieur henri Bellanger

Telephone: 079624193

Virginia is 2010/2014 a 1

Je viens aussi de signaler  
et basculer sur un autre fil

Locataire le 31/08/2024 à

#### **Initial training experience**

Signalement #788884 à 0

je viens de voir votre offre  
nommée d'accord pour ré

possible veuillez nous envoier une période plus

[View details](#)

deux fois à notre mail avec  
appartient pas.

Du coup, je n'ai pas répondu.  
Désolée, je n'ai pas refusé.

different et deux prénoms.  
Je n'ai pas répondu à cette

10 of 10



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.

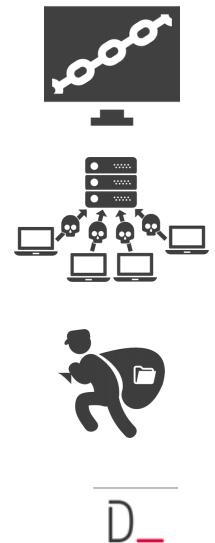


D\_

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 autorisé 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 ?*
  - *...*



25

## AGENDA



1

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

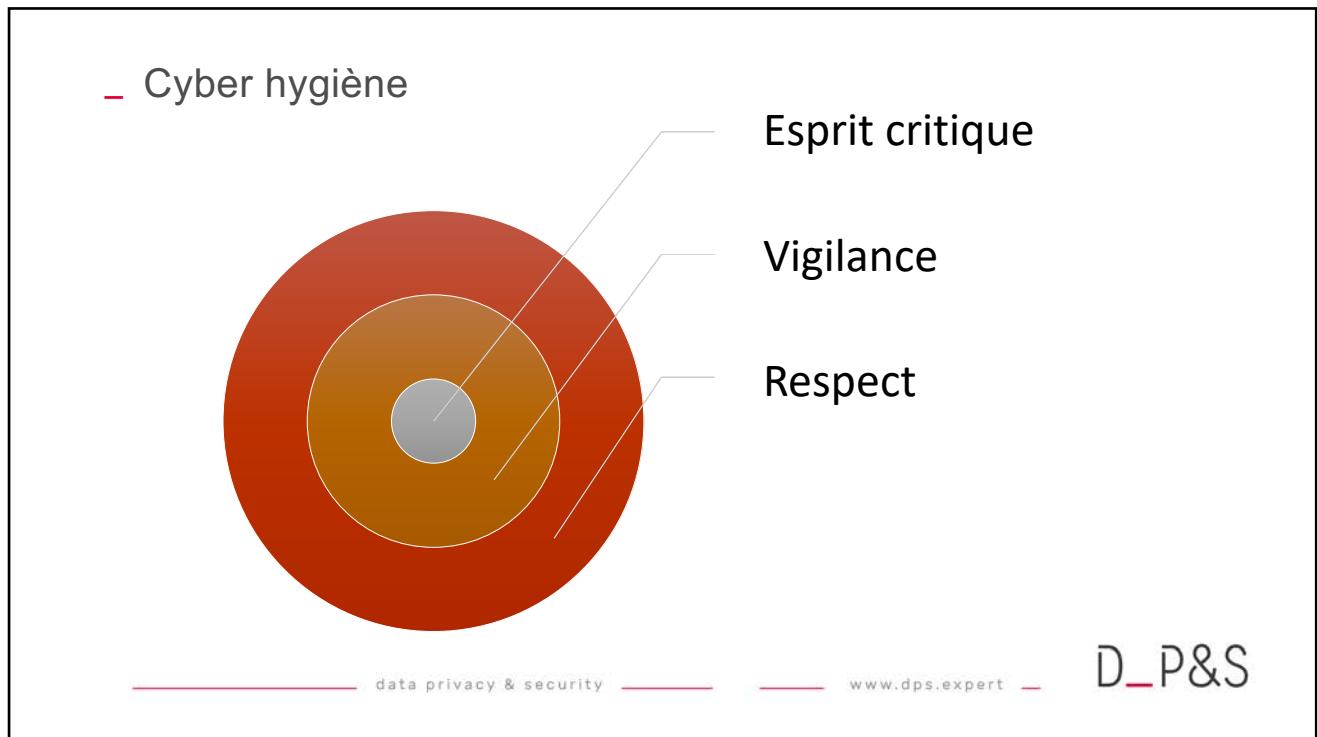
2

Comment y faire face ?

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



26



27

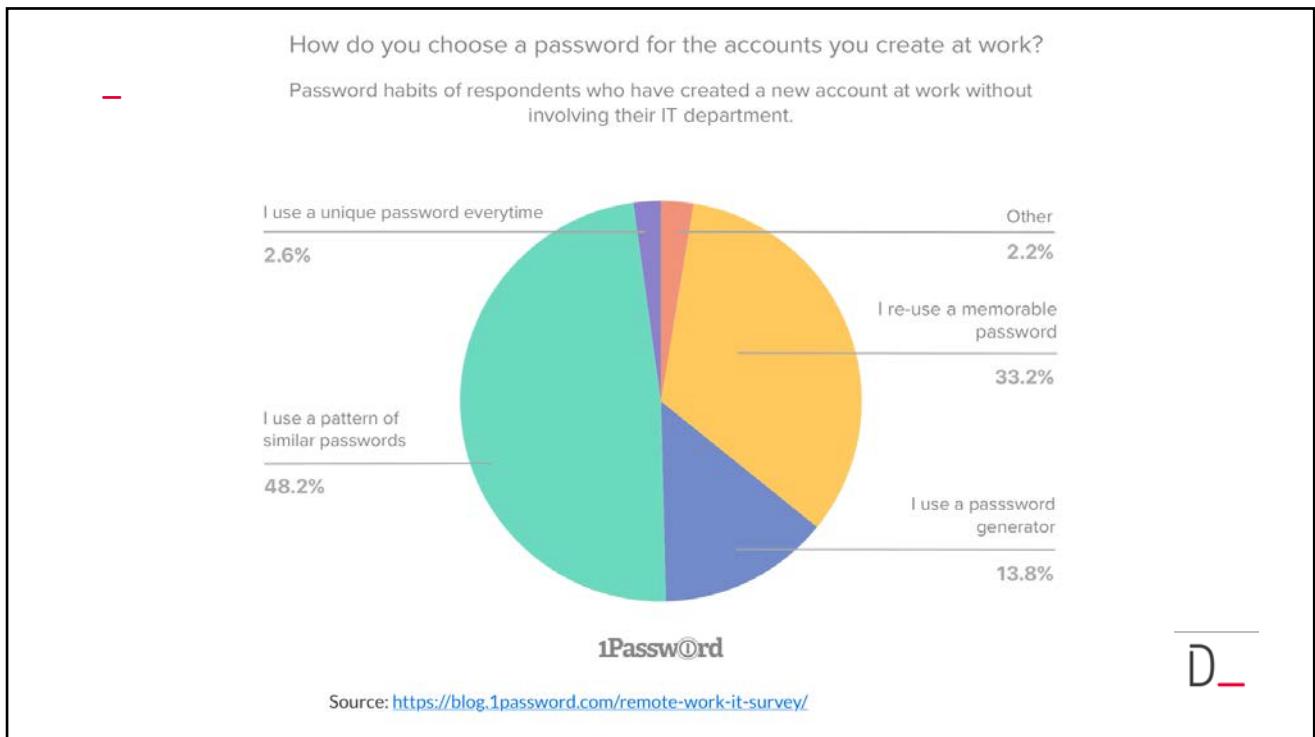
Comment choisissez-vous vos mots de passe ?

Cyber hygiène - Mots de passe

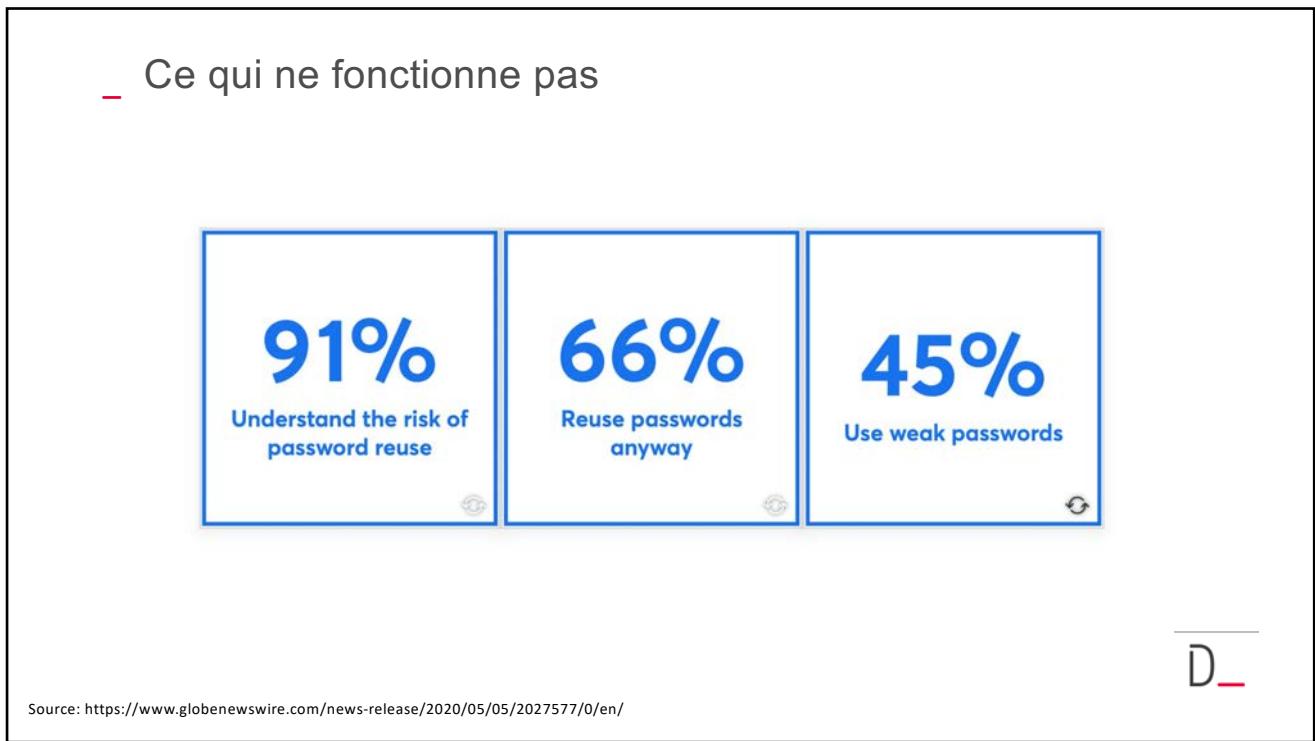


D\_

28

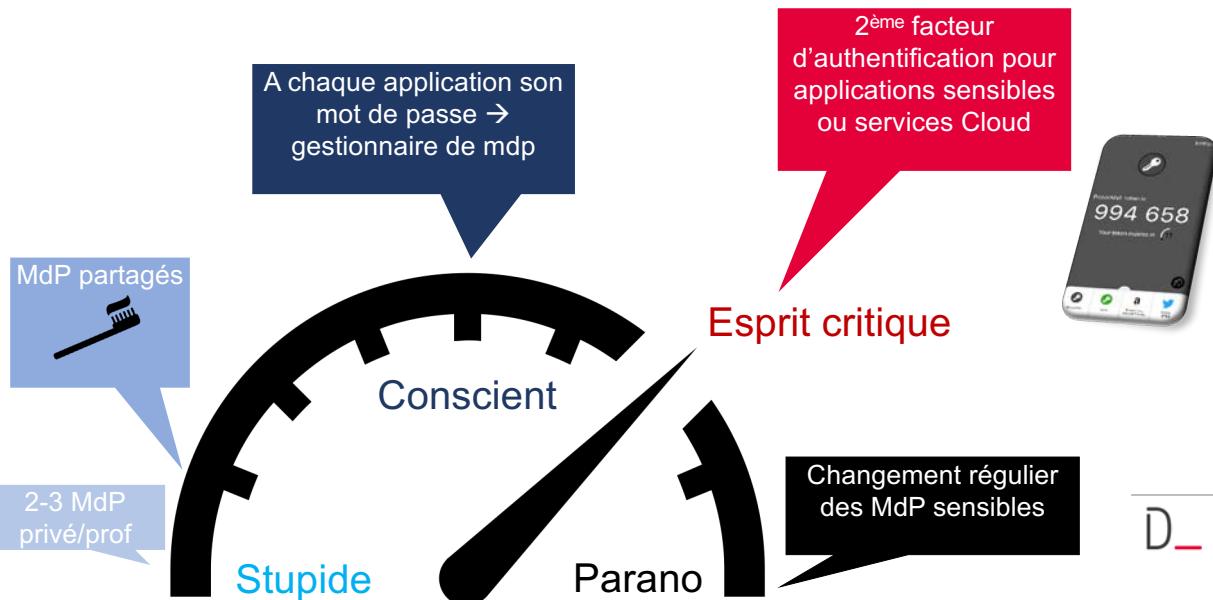


29



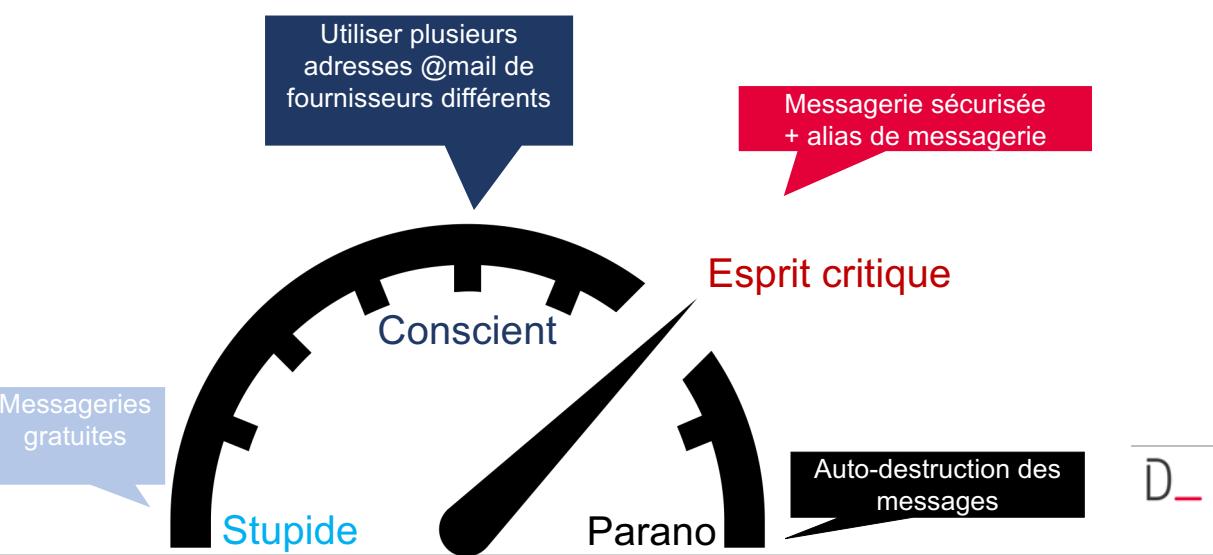
30

## Mots de passe



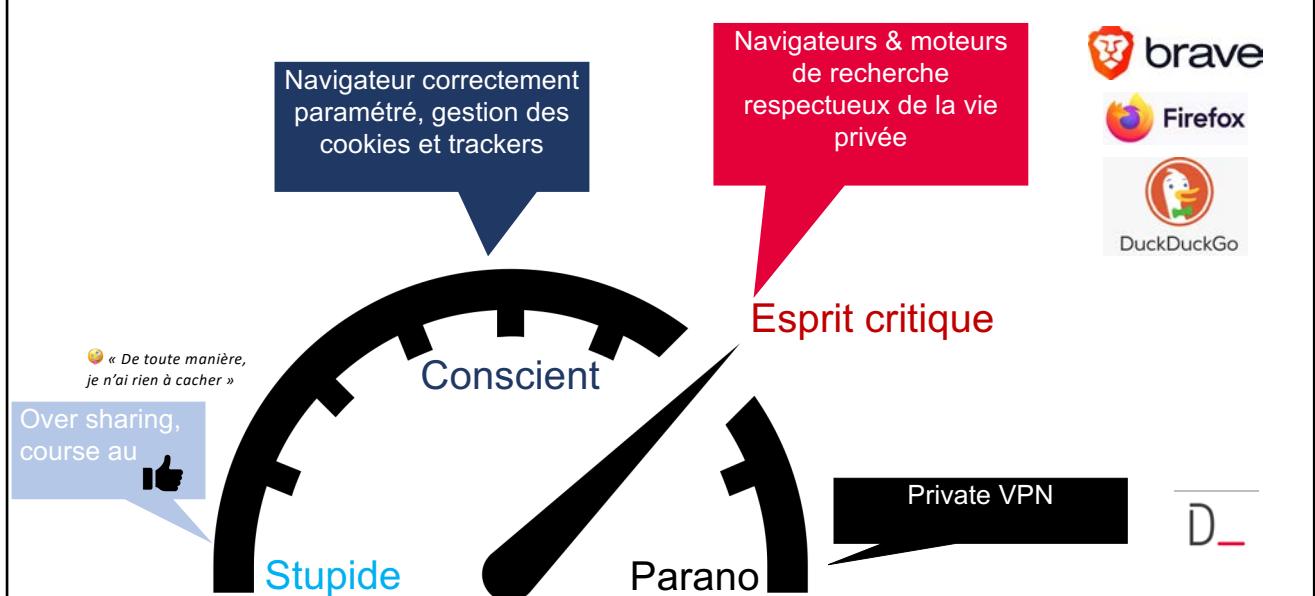
32

## Messagerie



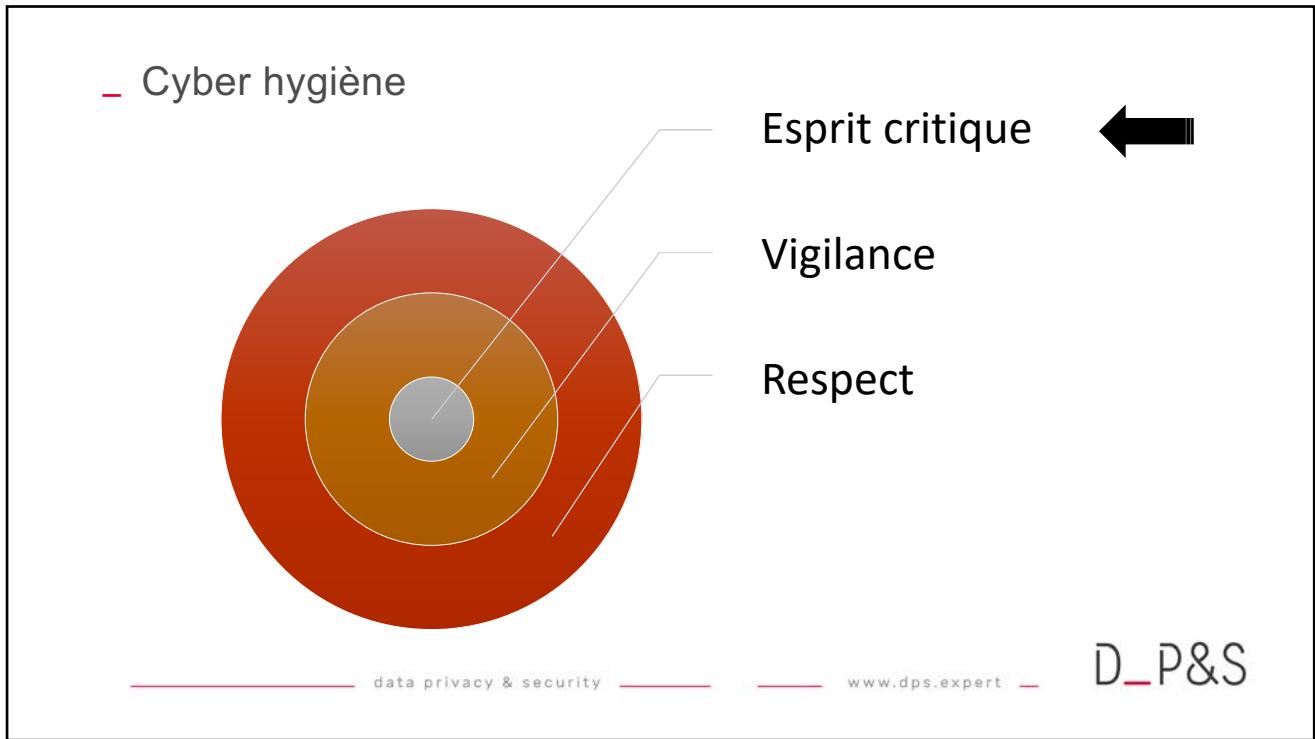
33

## Navigation internet / réseaux sociaux



34

## Cyber hygiène



35

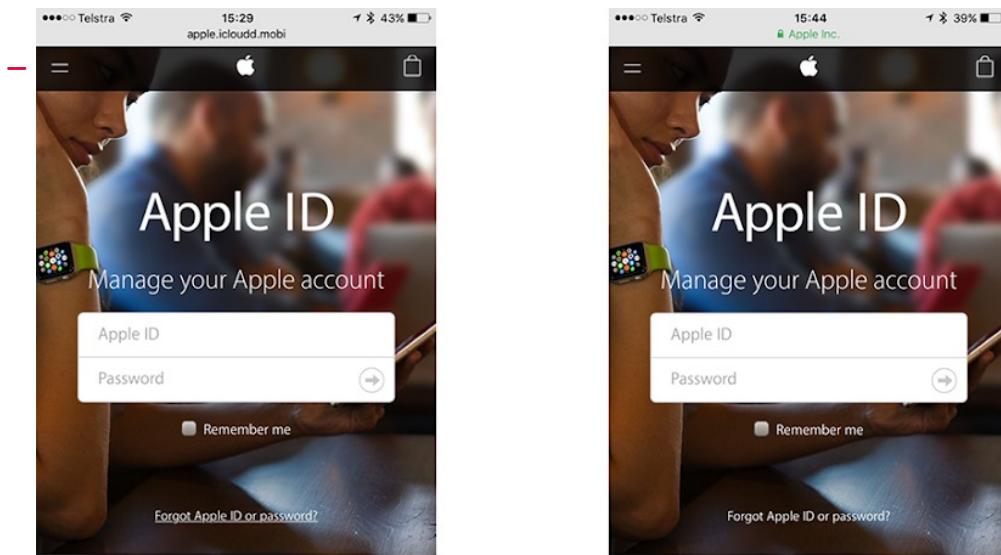
Attention à ce qui semble familier...

Augmentation des app malicieuses sur Apple et Google Stores

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



36



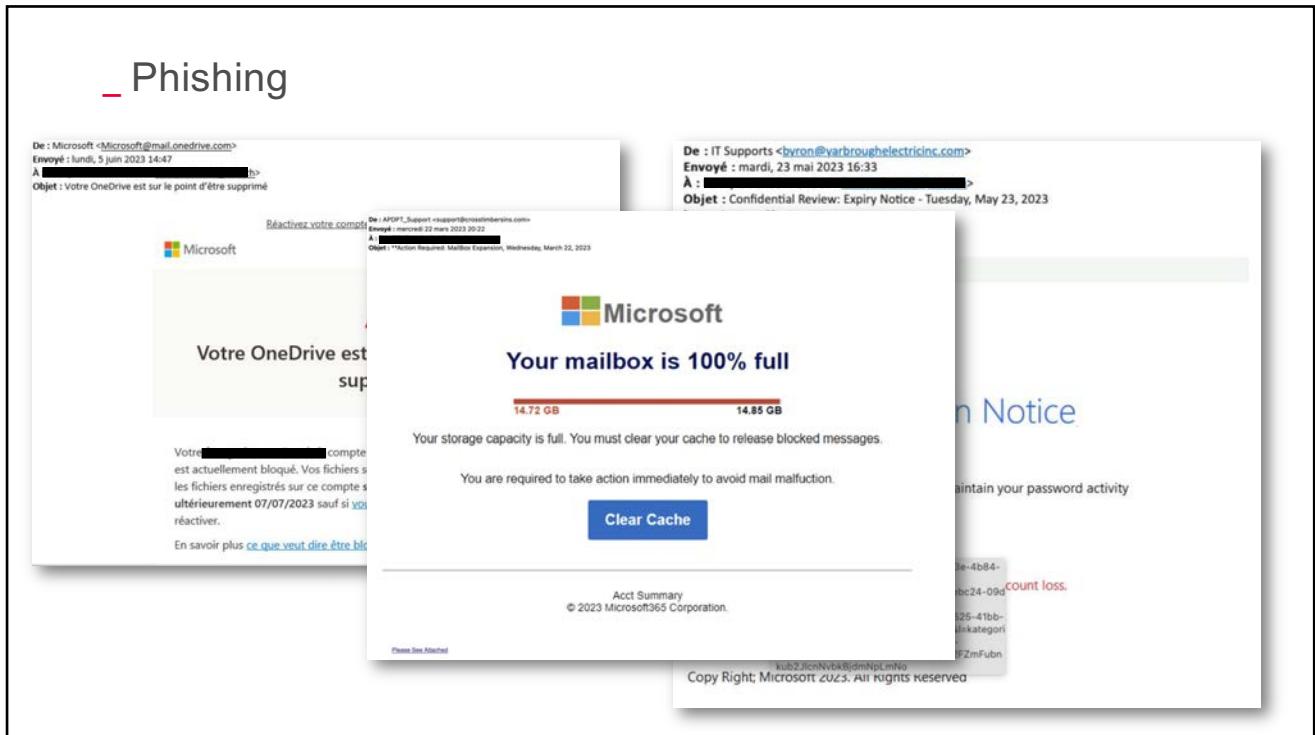
Your account  
for everything Apple.

A single Apple ID and password gives you access to all Apple services.  
[Learn more about Apple ID >](#)

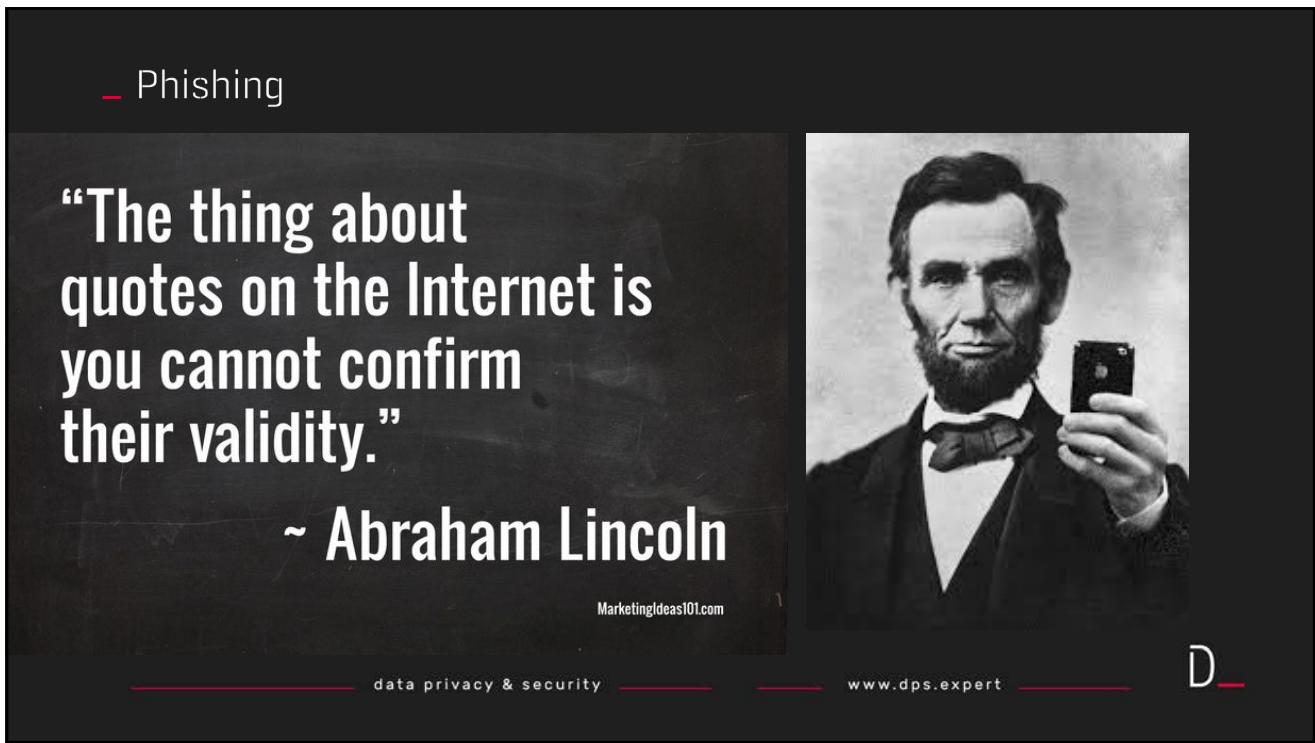
Your account  
for everything Apple.

A single Apple ID and password gives you access to all Apple services.  
[Learn more about Apple ID >](#)

37



39



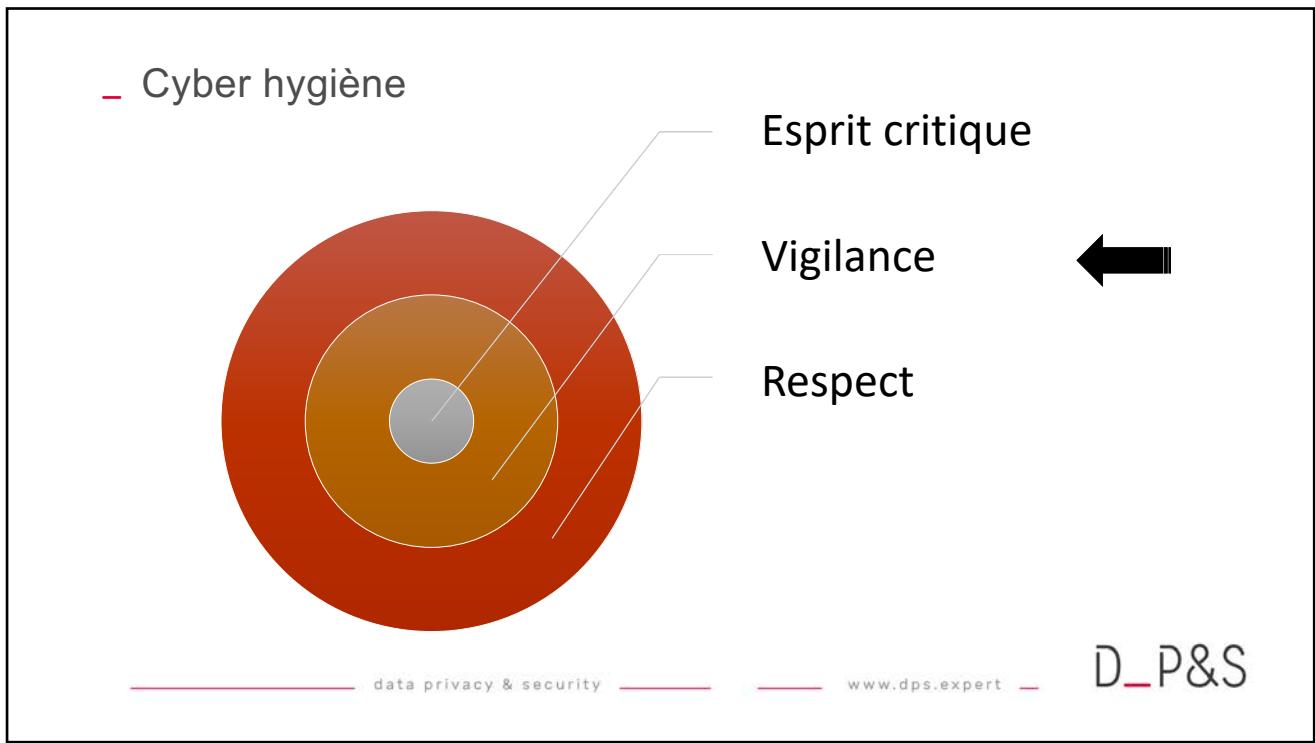
43

## 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



45

# AGENDA

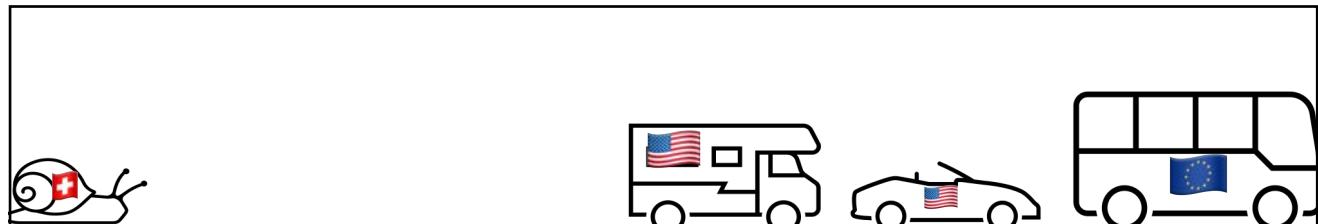
3

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

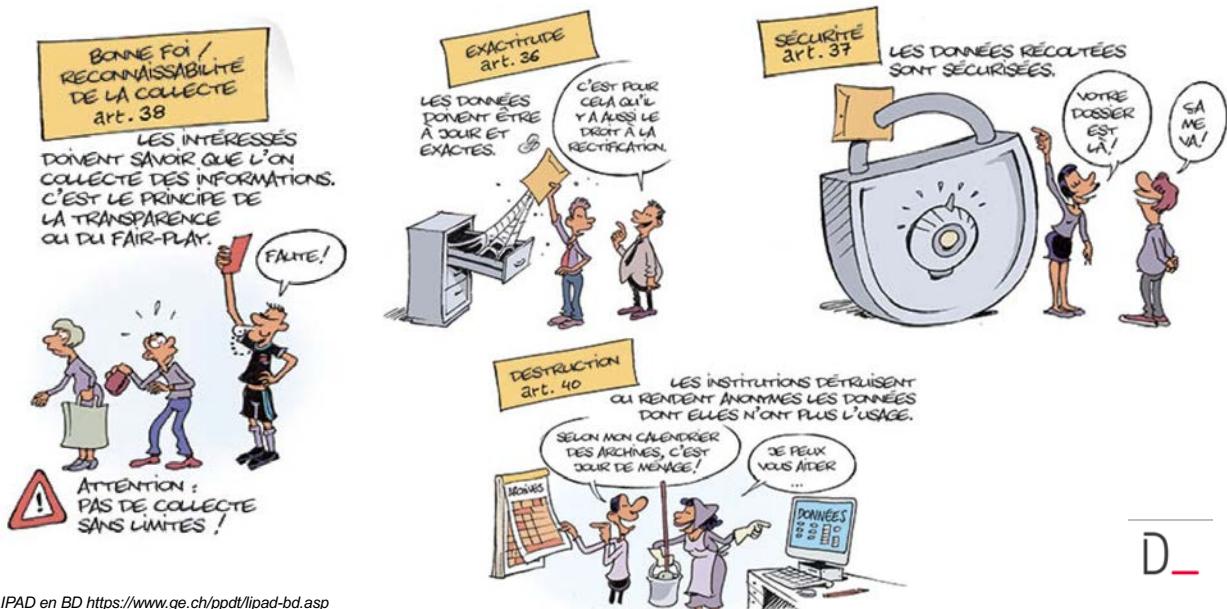
## Les 7 principes généraux de la protection des données



D\_

48

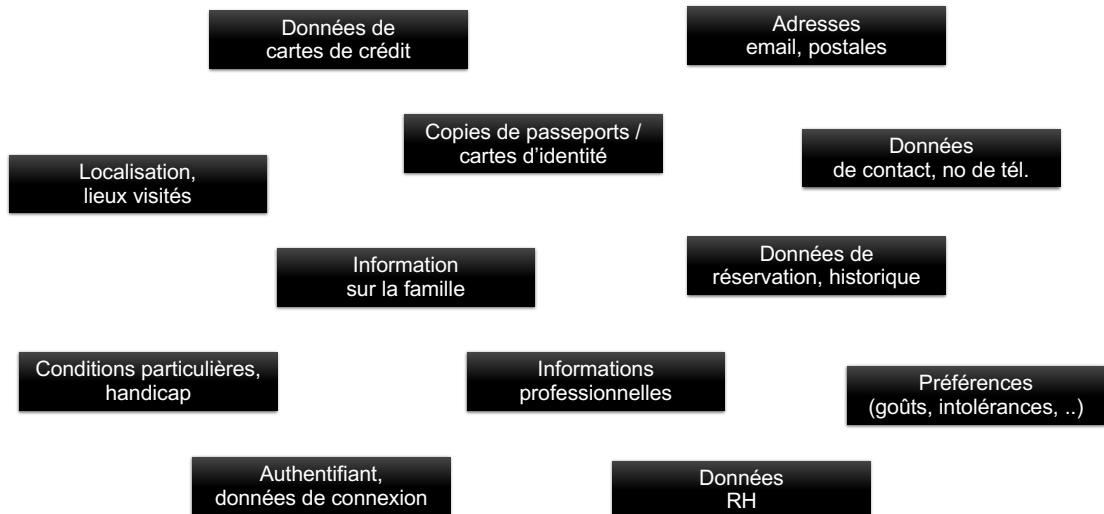
## Les 7 principes généraux de la protection des données



D\_

49

## Secteur du tourisme – données personnelles traitées



50

## Cyber sécurité

10 choses à ne pas faire

51

10 choses....

...à ne pas faire 😞

...à faire 😊

<b>1</b> Réutilisation des mots de passe	}	Utiliser un (bon) gestionnaire de mots de passe
<b>2</b> Partage d'identifiants entre utilisateurs		
<b>3</b> Mots de passe faibles		
<b>4</b> Applications Cloud sans 2FA		
<b>5</b> Ordinateurs & applications non sécurisés		

Antivirus, chiffrement DD  
Effectuer les mises à jour.

D\_

52

10 choses...

...à ne pas faire 😞

...à faire 😊

<b>6</b> Collaborateurs non formés	Cyber sensibilisation
<b>7</b> Confiance aveugle envers les sous-traitants	Evaluation & contrat
<b>8</b> Données personnelles conservées indéfiniment	Inventaire, archivage
<b>9</b> « <i>De toute manière, je n'ai rien à cacher !</i> »	Le respect de la sphère privée n'est pas une option!
<b>10</b> Paniquer en cas d'incident	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