



Innovations numériques, Éducation Thérapeutique augmentée Voyage vers l'e-ETP

Journée de la filière ETP – GHT Alliance
de Gironde en partenariat avec les UTEP
des CHU de Poitiers et de Limoges

ACCUEIL



Cybersécurité, un enjeu de L'e-ETP



Jean-Michel Soenen, RSSI - CHU de Bordeaux / GHT Alliance de Gironde



Avez-vous répondu ?

<https://tinyurl.com/3hrfp7k5>



<https://app.wooclap.com/>

Code DEZJKB

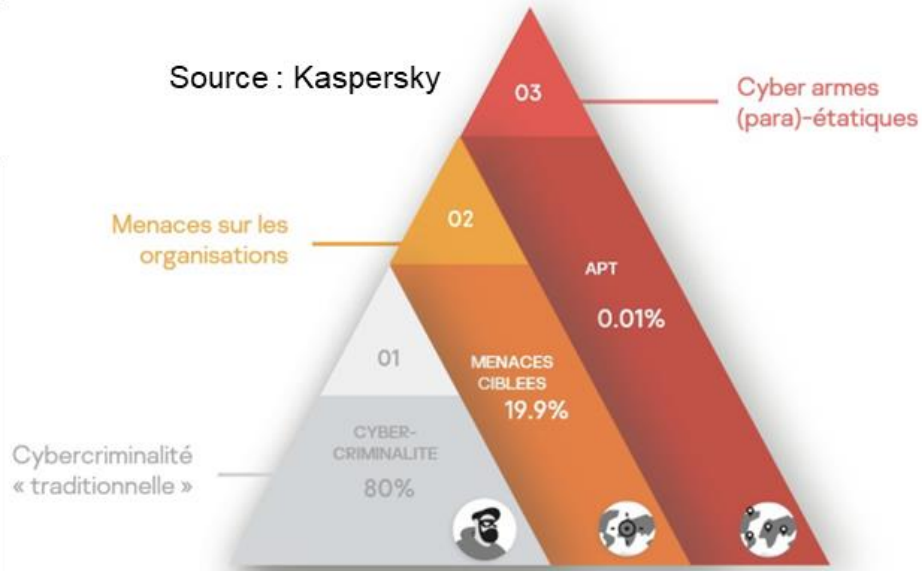


Pourquoi ?

Question 1

Quel est le coût total de la cybercriminalité dans le monde ?

1. 500 Millions de dollars (~PIB Dominique)
2. 2 Milliards de dollars (~PIB Cap vert)
3. **6 000 Milliard de dollars (~PIB Allemagne + Italie)**



APT : Advanced Persistent Threat, Menace persistante avancée

Données de la Banque mondiale, 2023 pour l'année 2022

Rang	Pays ou territoire	PIB (en milliards de dollars/an) ³
-	Monde	96 100,09
1	États-Unis	25 346,805
2	Chine ⁴	19 911,059
-	Union européenne	17 088,63
-	Communauté d'États latino-américains et caraïbes	6,700,000
3	Japon	4 912,147
4	Allemagne	4 256,540
5	Inde	3 534,743
6	Royaume-Uni	3 376,003
7	France	3 013,005
8	Canada	2 221,220

Quid de vos données personnelles ? Prix en dollars (2021)

Type de data	Cible	PRIX
Bancaire	Mastercard	25
Bancaire	Am. Express	35
Bancaire	Visa	25
Bancaire	Login banque 100\$ compte	40
Bancaire	Login banque 2000\$ compte	120
Compte En ligne	Paypal 100\$	30
Compte En ligne	Paypal 1000\$	120
Compte En ligne	Western Union	45

Type de data	Cible	PRIX
Compte	Facebook	65
Compte	Instagram	45
Compte	Twitter	35
Compte	Gmail	80
Compte	Netflix	44
Compte	Adobe Cloud 1 an	160
Compte	Ebay Bonne réputation	1000
Compte	Canva Pro	6

Source ESEA

Type de data	Cible	PRIX
Scan	Passeport Russe	100
Selfie	Selfie avec Carte ID	100
Passeport physique	France ou Europe	4000
Passeport physique	Maltais	6500
Dox	Identité Complète	120
Santé	Nom, prénom, tél, NIRPP	8
Nous tous	Ensemble des données Exploitable d'une personne	Moyenne 1285

On ne clique pas n'importe où !

Question 2

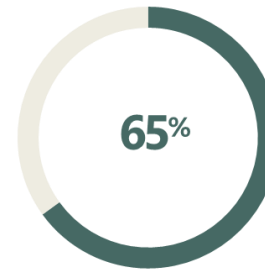
Quel a été votre 1^{er} réflexe pour vous connecter à ce questionnaire ?

1. Utiliser le QR code
2. Utiliser le lien court
3. **Renseigner l'adresse complète**

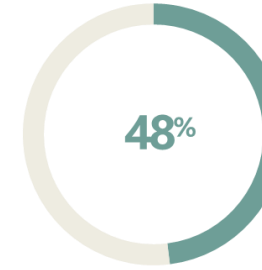
Question 3

Quel est le type d'attaque le plus utilisé contre les établissements de santé ?

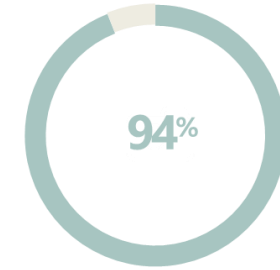
1. Vol d'équipement
2. **Phishing / Hameçonnage**
3. Logiciel malveillant
4. Attaque via prestataire informatique



Des attaques **ont débuté par un hameçonnage**



Des fichiers malveillants propagés par courriel sont des documents **Word, Excel ou Powerpoint**

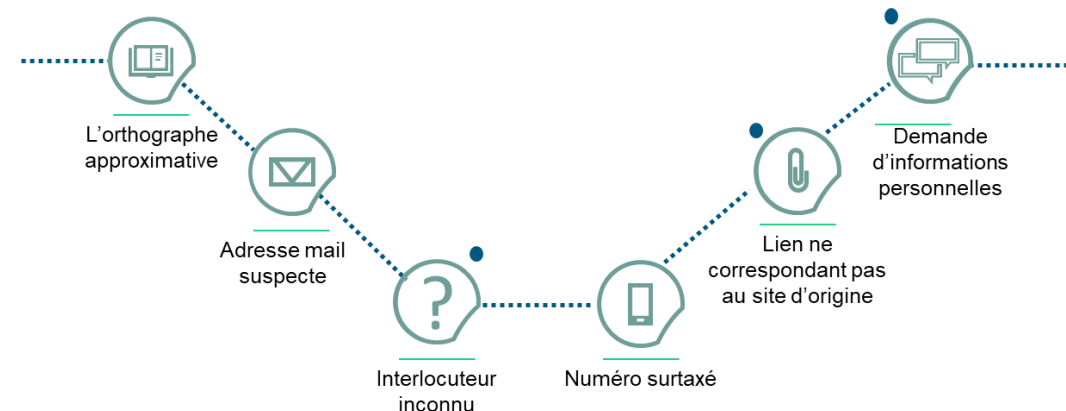


Des logiciels malveillants sont **propagés par courriel**

2 objectifs :

- Pirater votre poste si celui-ci n'est pas à jour
- Voler des données personnelles

6 Points de vigilance lors de la réception d'un mail



Les mots de passe : un indispensable !

Question 4

Lequel de ces mots de passe est le plus fiable ?

1. Choupinette1987 → 12m d'année mais ...
2. **Jevoled@nsles*lanuit!** → très robuste
3. 0123456789 → 1 seconde
4. Iloveyou → 28 secondes

Choupinette1987 :

- Robuste face à une **attaque en brute force** (test par dictionnaire, par combinaison)
- A priori, faible face à une **attaque par ingénierie sociale ou « social engineering »** consiste à exploiter la psychologie humaine pour s'infiltrer sur les systèmes informatiques ou accéder aux données confidentielles.
- https://www.youtube.com/watch?v=jQ_BzKKSzqE

Bonnes pratiques :

- Des mots de passe robustes, des mots de passe différents par service (web, appli, ...) et un coffre fort de mot de passe (Keepass par exemple) pour stocker ces différents mots de passe.
- Dans la mesure du possible, utiliser une authentification double facteur (SMS, ...)

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

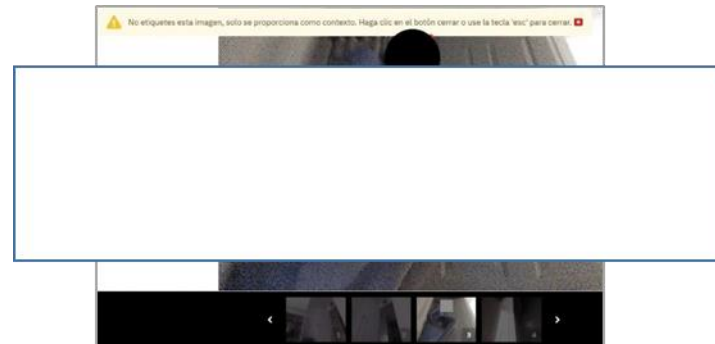
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

Attention aux objets connectés

Question 5

Quels sont les objets connectés ayant connu des problèmes de cybersécurité ?

1. Poupée connectée
2. Aspirateur connecté
3. Montre connectée
4. Réfrigérateur connecté
5. Caméra connectée



1. Poupée connectée
 - [Attention, les poupées connectées de vos enfants peuvent vous espionner | TF1 INFO](#),
 - [Certains jouets connectés susceptibles de se transformer en espions \(france24.com\)](#)
2. Aspirateur connecté
 - [Aspirateurs Roomba : pourquoi des photos très privées se sont retrouvées sur internet ? \(journaldugeek.com\)](#)
3. Montre connectée
 - [Une application de fitness dévoile la position de bases militaires secrètes \(lefigaro.fr\)](#),
 - [Monde - Bases secrètes américaines. Leur position trahie par des montres connectées - Le Télégramme \(letelegramme.fr\)](#)
4. Réfrigérateur connecté
 - Émission de spam
 - Émission de photos pédopornographiques
5. Caméra connectée
 - [10 millions de caméras chinoises pouvaient être pilotées à distance par des pirates - Numerama](#)

Protection des données personnelles - RGPD

Question 6

Selon le RGPD, le Responsable du Traitement est-il garant pour les données à caractère personnel de leur :

1. **Confidentialité**
2. **Authenticité**
3. **Intégrité**
4. **Disponibilité et Résilience**

Le responsable du traitement est responsable de l'ensemble des mesures techniques et organisationnelles à mettre en œuvre.

Rappel :

1. **Confidentialité** : *protéger des lectures non désirées*
2. **Authenticité** : *être sûr de l'origine du fichier*
3. **Intégrité** : *pas de modification*
4. **Disponibilité et Résilience** : *être en capacité d'utiliser*

- Un site de référence : [Comprendre le RGPD | CNIL](#)



Quelques bonnes pratiques, en Synthèse

- A titre personnel et professionnel, **ne pas cliquer sur un lien, un bouton sans réflexion ...**
- A titre personnel et professionnel, toujours
 - **Choisir des mots de passe robustes,**
 - **Choisir un mot de passe différent par service (web, appli, ...)**
 - **Utiliser un coffre fort de mot de passe (Keepass, ou autres)**
- A titre personnel, mettez systématiquement à jour votre système d'exploitation Windows et vos applications
 - **A minima sur les aspects patches de sécurité**
 - **N'utilisez que des versions officielles et maintenues par les éditeurs**
- A titre personnel et professionnel, soyez attentif à vos données personnelles (compte, mot de passe, adresse de messagerie, ..)
- A titre professionnel, tout traitement de données personnelles et/ou de données de santé doit faire l'objet d'une déclaration auprès du délégué à la protection des données (DPO) de votre structure .
 - Obligation légale liée au Règlement Général sur la Protection des Données (RGPD).

