

# « Cybersécurité : quels risques, quelles menaces, quels moyens de lutte ? »

Webinaire du 25 janvier 2022

Intervenants Pragmatic Consulting Sàrl :

M. Charly Delay – *Co-fondateur, Directeur*

M. Vincent Ottinger – *Co-fondateur, Directeur*

Modérateur : M. Eric Biesel





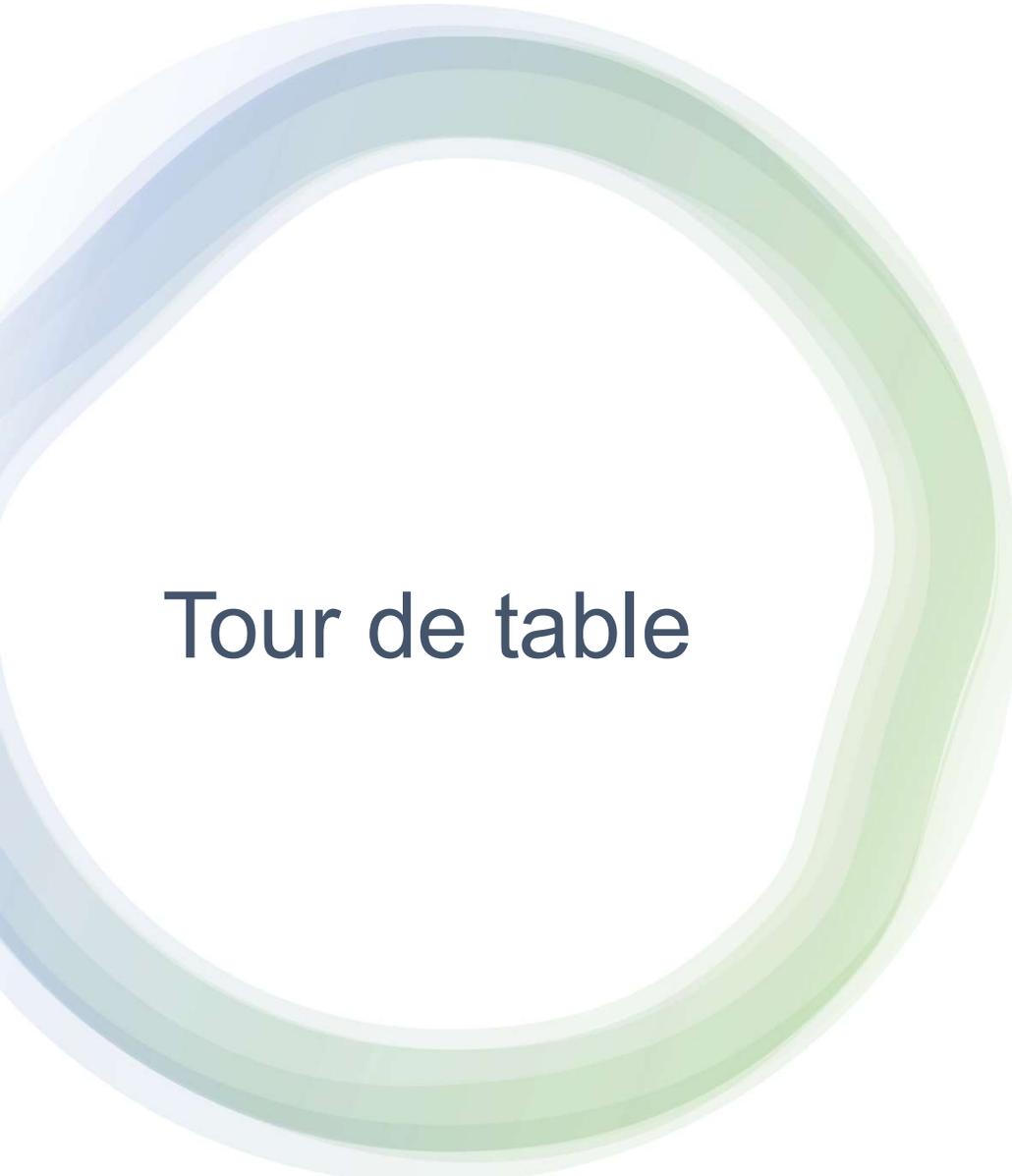
**GENÈVE**  
SOCIÉTÉ SUISSE  
DES ENTREPRENEURS



# Cybersécurité : quels risques, quelles menaces, quels moyens de lutte ?

Point Contact #1

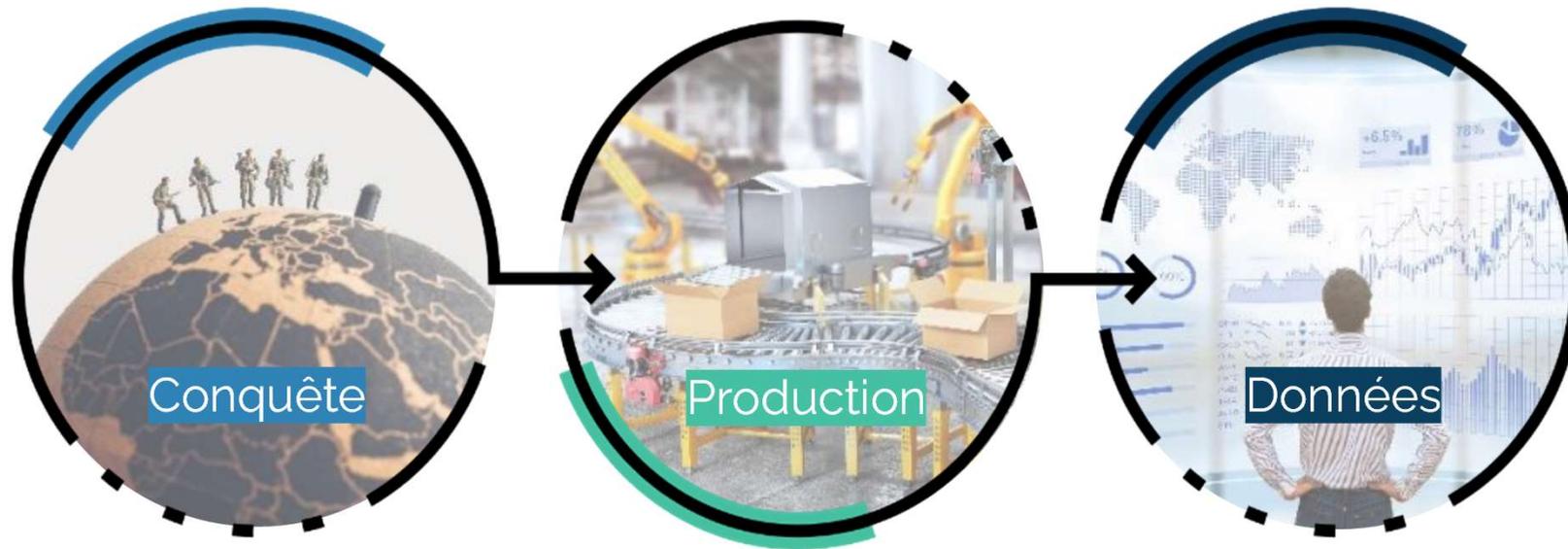
25.01.2022



# Tour de table

- Etes-vous tributaire de l'informatique ?
- Avez-vous déjà subi une cyberattaque ?
- Vous sentez-vous concerné par un risque de vol ou de perte de données ?
- Quel impact pour votre entreprise si vous devez vous passer d'informatique pour 1 jour, 1 semaine ou 1 mois ?
- Avez-vous déjà calculé les coûts d'un tel arrêt ?
- Au-delà des coûts, y aurait-il un risque humain ou d'image ?

# La données, une nouvelle richesse





**DONNÉES**

## Enquête ouverte après des failles informatiques concernant le registre national du don d'organes

Le Préposé fédéral à la protection des données et à la transparence (PFPDT) Adrian Lobsiger a ouvert jeudi dernier une enquête contre la fondation Swisstransplant

## e le CICR: les million de nises

u Comité international de la Croix- de 500'000 personnes humanitaire demande aux attaquants

ier 2022

Janvier 2022

Novembre 2021

# Les PME suisses

ÉTUDES

Augmentation significative

## 2'700 entreprises suisses rançonnées ces 12 derniers mois

Jeu 07.10.2021 - 15:48  
par Rodolphe Koller

Selon une analyse de Recorded Future, près de 2'700 organisations suisses ont vu leurs données fuiter sur le darknet depuis le mois d'août 2020. Un volume qui témoigne du caractère industriel du cybercrime.



(Source: shutterstock)





**Hacker, un business comme les autres**

## Vecteurs d'attaque



Phishing  
(hameçonnage)

Typosquattage

Ransomware

Espionnage  
(Keylogger,  
caméra, micro)

Utilisation des  
ressources (PC  
zombies)

Email  
frauduleux

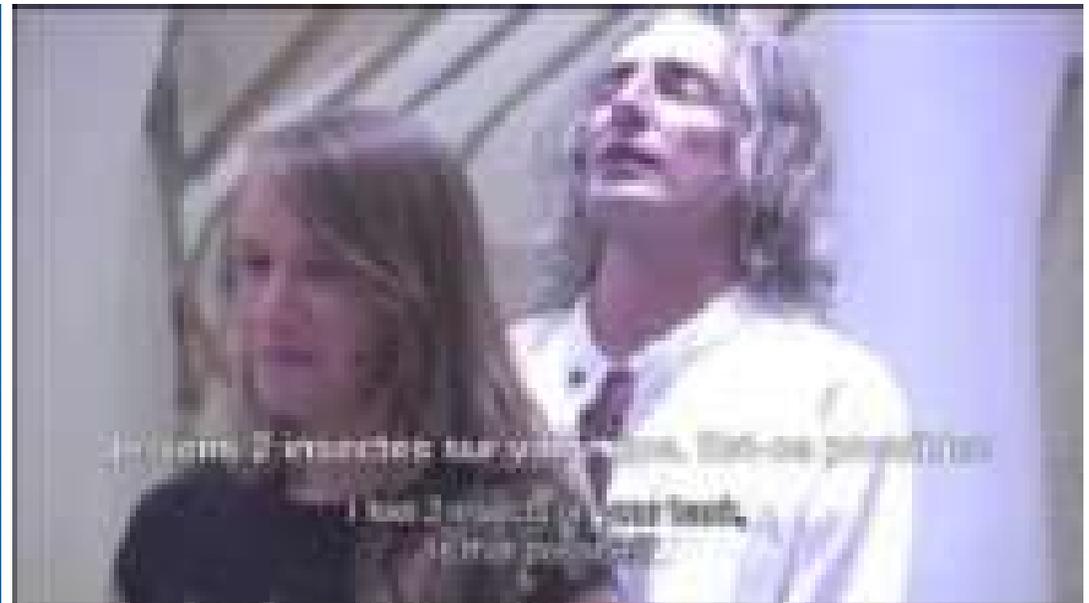
Site infecté

USB ou carte SD  
infectée

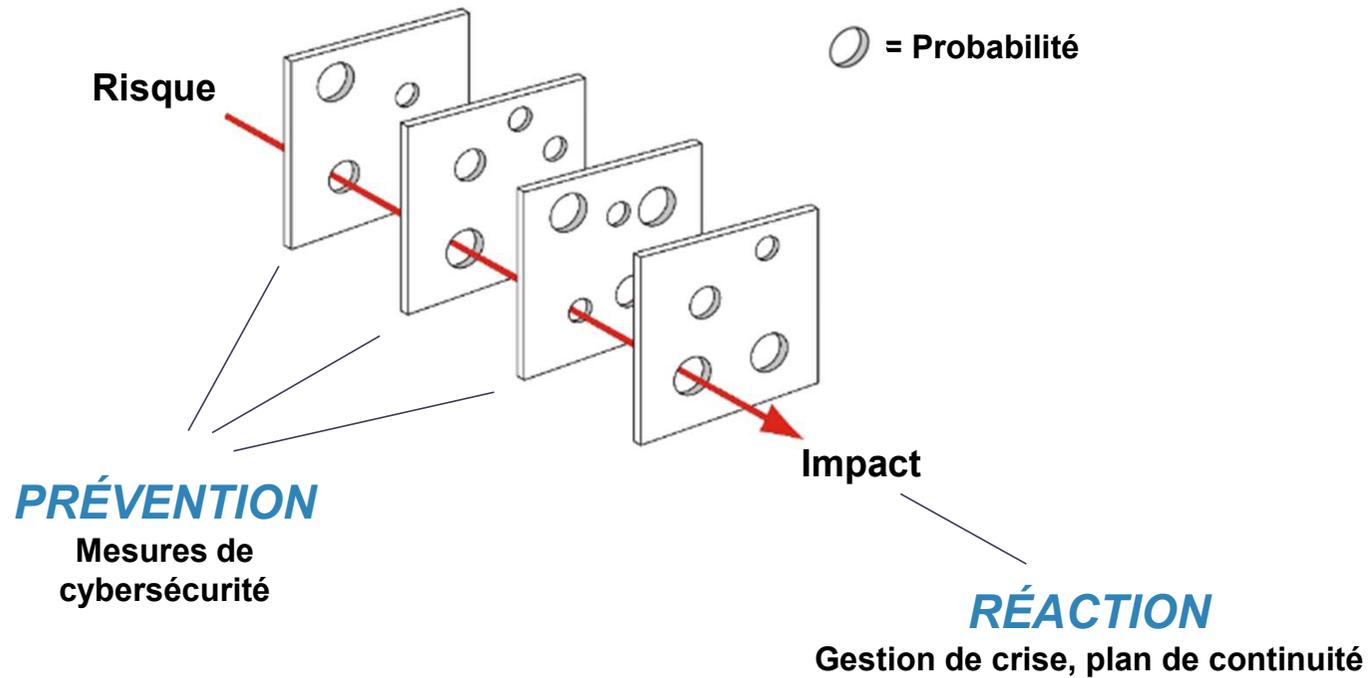
**Votre smartphone**



# Les réseaux sociaux



# Quel est votre risque ?





Soyez résilient



## Mesures de protection



Mot de passe

Antivirus /  
firewall

Verrouillage  
automatique

Mise à jour des  
applications

Coffre fort  
numérique

Comportement

VPN

Connexion Wifi

Gestion des  
accès

Sensibilisation  
/ Formation

# Mot de passe – Votre clé d'entrée dans votre vie numérique

## Les bonnes pratiques

- Un mot de passe est personnel !
- Minimum 9 caractères
  - Avec des chiffres [ 0 1 2 3 4 5 6 7 8 9 ]
  - Avec des lettres minuscules [ a b c ... x y z ]
  - Avec des lettres majuscules [ A B C ... X Y Z ]
  - Avec des caractères spéciaux [ ~ ! @ # \$ % ^ & \* ( ) - \_ = + [ ] { } ; : , . < > / ? | ]
  - <https://www.motdepasse.xyz/>

**\_t45.Xa8F**

- Idéalement un mot de passe différent par site web
- Utiliser un gestionnaire de mot de passe
  - <https://go.nordvpn.net/SH407> (VPN avec offre pour un gestionnaire de mot de passe)
  - Celui de l'explorateur internet (mieux que rien)
- Pour contrôler si votre compte a déjà été piraté
  - <https://haveibeenpwned.com/>

## Antivirus & Firewall

- Antivirus, c'est comme un médecin, pour éviter qu'un virus n'infecte votre ordinateur
- Firewall, c'est comme un agent de sécurité à l'entrée d'un immeuble, pour contrôler les connexions entrantes et sortantes de votre ordinateur
  
- Windows 10 intègre Antivirus Microsoft Defender
- Eviter les virus gratuits, ils sont moins complets
  
- Les antivirus les plus connus :
  - Bitdefender
  - Kaspersky
  - AVG
  - Avast
  - Panda



## Verrouiller son écran automatiquement

- Activer le verrouillage d'écran automatique permet d'éviter qu'un collègue ou un client ne puisse accéder à notre PC pendant notre absence
- Mettre un mot de passe pour déverrouiller son écran
- Aussi sur son smartphone

Pour verrouiller son PC en 1 clic :

Windows :  + L

Mac : **ctrl+⌘+Q**

- Verrouillage dynamique (éloignement du smartphone) : sous Windows 10, sélectionnez le bouton Démarrer > Paramètres > Comptes > Options de connexion.



## Mettre à jour ses applications

- Pour éviter les vulnérabilités, mettre à jour les applications, car les failles de sécurité sont corrigées régulièrement par les éditeurs
- Sous Windows, activer Windows Update
- Sous Mac, activer les mises à jour automatique
- Votre smartphone également : Android ou MacOS
- Votre site web, il peut y avoir des extensions à mettre à jour aussi



## Coffre fort numérique

- Des fichiers confidentiels peuvent être stockés dans un coffre fort numérique
- Avec Microsoft 365, OneDrive en intègre un par défaut
- Peut-être utile pour :
  - Papiers d'identité
  - Accès bancaires
  - Contrats spécifiques
  - Documents contenant des secrets industriels
  - Brevets



## Votre comportement

- Tout ce qu'on a dit plus haut
- Ne pas faire de streaming sur des plateformes «gratuites»
- Ne pas installer de logiciels «gratuits»
- Faire des sauvegardes
- Ne pas cliquer trop vite sur des liens que l'on reçoit
- Ne pas relayer les canulars
- Ne JAMAIS donner son mot de passe
- Être attentif aux emails avec des liens ou pièces jointes
  - Vérifier l'adresse de l'expéditeur
  - Ne jamais ouvrir une pièce jointe d'un email qu'on attend pas
  - Ne jamais ouvrir les extensions .pif, .bat, .exe, .vbs, .ink



## VPN – Pourquoi s'en servir ?



Débloquer les contenus limités dans certains pays



Masquer son adresse IP



Éviter d'être vu en utilisant un wifi public

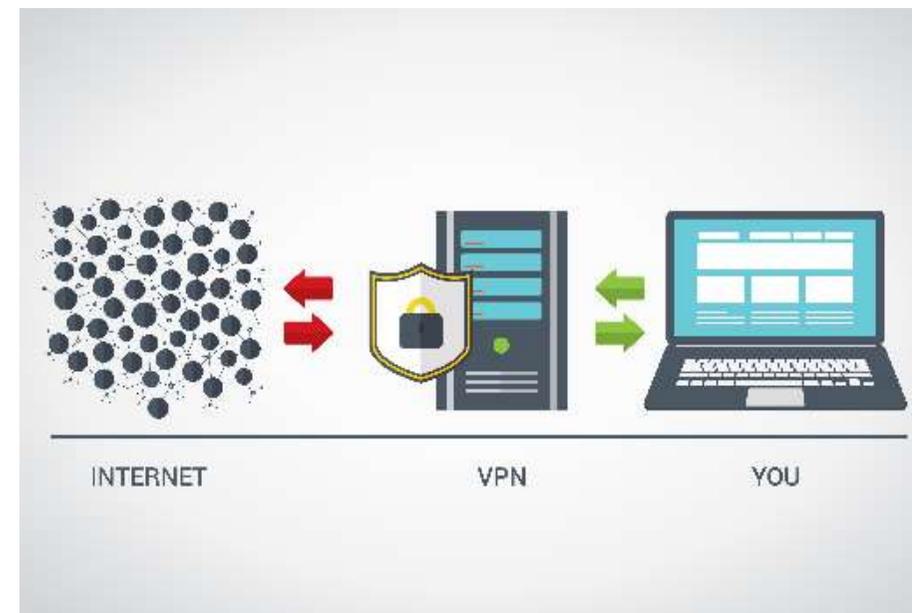


Éviter d'être surveillé (opérateur, gouvernement)

NordVPN - <https://go.nordvpn.net/SH407>

ExpressVPN

CyberGhost



## Connexion Wifi

- Chez vous
  - Changer le mot de passe par défaut
  - Respecter les règles de création de mot de passe vues précédemment
  - Ne JAMAIS laisser «admin», ou «password» ou «0123456» comme mot de passe
  - Utiliser au minimum du WPA 2 (pas de WEP, ou «sans mot de passe»)
  - Ne donner pas son accès wifi à n'importe qui
  - Activer si possible le réseau «Guest» qui permet d'accéder à internet sans accès au réseau principal
- Au bureau
  - Adopter les mêmes règles que chez vous
- Wifi extérieur
  - Utiliser un VPN
  - Ne pas se connecter au Wifi sans mot de passe
  - Limiter la durée de connexion



## Gestion des accès et des identités

- Ne pas partager son mot de passe avec ses collègues
- Dans la mesure du possible, utiliser un compte par personne pour les applications, l'accès aux ordinateurs et aux sites web
- Séparer les fichiers confidentiels du reste des fichiers de l'entreprise et ajouter un contrôle d'accès
- Désactiver les comptes des collaborateurs qui ont quitté l'entreprise
- Lorsqu'elle est proposée, activer l'authentification à deux facteurs ou authentification forte ou 2FA

- Google authenticator



## Formation & Sensibilisation

- Prendre le sujet de la sécurité informatique au sérieux
- Parler de sécurité informatique avec ses collègues
- Suivre annuellement une présentation de l'actualité de la cybersécurité (telle que celle d'aujourd'hui)
- Aller voir des chaînes Youtube qui en parlent
  - La nôtre par exemple «pragmatic consulting» 
- Se renseigner auprès de son prestataire informatique
- Nous demander conseil si besoin



# Résumons

- La **donnée** est LA nouvelle richesse des entreprises
- Les hackers sont des **professionnels** du vol de données
- Vous êtes une **cible** de choix pour les hackers
- Soyez **attentif** en tout temps, partout, un accident survient quand il y a une petite erreur d'inattention
- Les **conséquences** d'un vol ou d'une perte de données peuvent laisser des traces sur le long terme
- Le **risque zéro** n'existe pas, il faut être prêt à réagir
- Rendre son entreprise plus **résiliente**, c'est éviter de perdre **son capital**

# 3 actions pour la prochaine fois

Mot de passe

Antivirus /  
firewall

Verrouillage  
automatique

Mise à jour des  
applications

Coffre fort  
numérique

Comportement

VPN

Connexion Wifi

Gestion des  
accès

Sensibilisation  
/ Formation

# Pragm@TIC

— CONSULTING —

**Pragm@TIC-Consulting**

[www.pragmatic-consulting.ch](http://www.pragmatic-consulting.ch)

[info@pragmatic-consulting.ch](mailto:info@pragmatic-consulting.ch)



```
...mirror_mod.mirror_object :
operation == "MIRROR_X":
mirror_mod.use_x = True
mirror_mod.use_y = False
mirror_mod.use_z = False
operation == "MIRROR_Y":
mirror_mod.use_x = False
mirror_mod.use_y = True
mirror_mod.use_z = False
operation == "MIRROR_Z":
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True

#selection at the end add
mirror_ob.select= 1
mirror_ob.select=1
context.scene.objects.active
("Selected" + str(modifier))
mirror_ob.select = 0
= bpy.context.selected_objects
data.objects[one.name].select
print("please select exactly")

-- OPERATOR CLASSES --

types.Operator):
X mirror to the selected
object.mirror_mirror_x"
mirror X"

text): object is not
```

**Merci pour votre attention.**

**CONSTRUIRE AU 21<sup>e</sup> SIÈCLE**