



## **ATELIER DE SENSIBILISATION**

PROJET : RESILIENCE NUMERIQUE DES  
CENTRES DE REHABILITATION  
DES VICTIMES DE LA TORTURE

Février 2023



**HOLISTIC PROTECTION COLLECTIVE**

## 0 | Présentation de l'atelier

### 1 | État des lieux

- Ce que nous voulons protéger
- Notre matériel
- Menaces actuelles

### 2 | Le *Digital Care Guide* de l'irct

### 3 | Ateliers pratiques

- Mots de passe & Comptes
- Appareils
- Communication
- Données

### 4 | Étapes de la réponse aux crises

### 5 | Étapes suivantes



irct

International Rehabilitation  
Council for Torture Victims

# PRÉSENTATION DE LA FORMATION

## 0 | Introduction

### 1 | État des lieux

- Ce que nous voulons protéger
- Notre matériel
- Menaces actuelles

### 2 | Le *Digital Care Guide* de l'irct

### 3 | Séances pratiques sur la protection

- Mots de passe & Comptes
- Appareils
- Communication
- Données

### 4 | Étapes de la réponse aux crises

### 5 | Étapes suivantes

0 | Présentation de l'atelier

## 1 | État des lieux

- **Ce que nous voulons protéger**
- Notre matériel
- Menaces actuelles

2 | Le *Digital Care Guide* de l'**irct**

3 | Ateliers pratiques

- Mots de passe & Comptes
- Appareils
- Communication
- Données

4 | Étapes de la réponse aux crises

5 | Étapes suivantes



**irct**

International Rehabilitation  
Council for Torture Victims

# 1 | Ce que nous voulons protéger

## Informations sensibles qui ne doivent pas tomber entre de mauvaises mains :

- Toute **information identifiable** sur nos bénéficiaires, notamment les **documents médicaux** et les **dossiers judiciaires**
- Toute information identifiable sur notre **équipe** ou sur des **membres** de l'organisation, notamment des contrats, des adresses, etc. ?
- Toute information sensible utilisée lors de campagnes (publiques), etc., notamment les coordonnées des participants et des membres de la communauté ou de l'équipe ?
- → Certaines de ces informations doivent être conservées précieusement

0 | Présentation de l'atelier

## 1 | État des lieux

- Ce que nous voulons protéger
- **Notre matériel**
- Menaces actuelles

2 | Le *Digital Care Guide* de l'irct

3 | Ateliers pratiques

- Mots de passe & Comptes
- Appareils
- Communication
- Données

4 | Étapes de la réponse aux crises

5 | Étapes suivantes



irct

International Rehabilitation  
Council for Torture Victims

# 1 | Notre matériel

- Un ordinateur portable Lenovo
- Un disque dur externe (1 Tio)
- Un smartphone Samsung Galaxie A53
- Un smartphone Samsung Galaxie A13
- Un pack de vidéo surveillance
- Autres appareils ?

**Quels en sont les usages actuels ?**

**Quels usages futurs ?**

**Quelles sont les difficultés rencontrées dans leur utilisation ?**

0 | Présentation de l'atelier

## 1 | État des lieux

- Ce que nous voulons protéger
- Notre matériel
- **Menaces actuelles**

2 | Le *Digital Care Guide* de l'[irct](#)

3 | Ateliers pratiques

- Mots de passe & Comptes
- Appareils
- Communication
- Données

4 | Étapes de la réponse aux crises

5 | Étapes suivantes

# 1 | Menaces actuelles

## Menaces existant dès lors qu'on utilise le numérique :

- **Hameçonnage** : tentative d'informations personnelles se faisant passer pour une demande légitime
- **Attaque de compte** : des personnes malveillantes essayent de pirater ou de se connecter à nos comptes en ligne.
- **Panne ou mauvaise gestion des appareils** : nous perdons l'accès à nos données en raison de l'ancienneté de l'appareil ou de problèmes techniques ou humains.

## Menaces propres à CAPREC:

- **Perquisition & saisie, vol d'appareils** : lors de perquisitions ou d'action judiciaire à notre encontre, nos appareils sont saisis par les forces de l'ordre ou volés par des acteurs criminels.
- **Surveillance** : les forces de l'ordre ou des acteurs criminels observent nos comportements en ligne ou en personne. Cela peut se produire de manière numérique via notre fournisseur d'accès à internet, notre compagnie de téléphone, un logiciel espion ou la mise sur écoute de notre téléphone
- **Attaque de vidéoconférences.**
- **Crises ? ...**

0 | Présentation de l'atelier

1 | État des lieux

- Ce que nous voulons protéger
- Notre matériel
- Menaces actuelles

**2 | Le *Digital Care Guide* de l'irct**

3 | Ateliers pratiques

- Mots de passe & Comptes
- Appareils
- Communication
- Données

4 | Étapes de la réponse aux crises

5 | Étapes suivantes

## 2 | Le *Digital Care Guide* de l'irct

À l'**irct**, nous voulons prendre soin des données et informations partagées de la meilleure façon possible, ce qui nous permet de protéger nos clients, notre personnel, les centres membres et le secrétariat. À cette fin, nous avons créé le *Digital Care Guide*. Il nous permet de prendre les mesures nécessaires convenues pour protéger nos comptes, nos appareils, notre communication et nos données.

### Table des matières

- Que protéger ?
- Menaces actuelles
- PRÉVENTION
  - Sécuriser nos mots de passe & comptes
  - Sécuriser nos appareils
  - Sécuriser notre communication
  - Sécuriser nos données
- RÉPONSE AUX CRISES
  - Mesures d'urgence

0 | Présentation de l'atelier

1 | État des lieux

- Ce que nous voulons protéger
- Notre matériel
- Menaces actuelles

2 | Le *Digital Care Guide* de l'**irct**

**3 | Ateliers pratiques**

- **Mots de passe & Comptes**
- Appareils
- Communication
- Données

4 | Étapes de la réponse aux crises

5 | Étapes suivantes



**irct**

International Rehabilitation  
Council for Torture Victims

## 3 | Protéger nos comptes et mots de passe

- **Mots de passe forts & uniques** : utiliser des mots de passe composés de plusieurs mots. Il est important d'utiliser un mot de passe unique à chaque compte

→ **Pratique** : inventer des mots de passe

- **Gestionnaire de mots de passe** : si possible, utiliser des gestionnaires de mots de passe comme <https://keepassxc.org> ou <https://bitwarden.com>. Ils utilisent un mot de passe principal fort pour protéger tous les autres mots de passe qui se trouvent dans le gestionnaire

→ **Pratique** : tester Bitwarden

- **Authentification à deux facteurs (2FA)**
- **Prévention de l'hameçonnage (phishing)**

0 | Présentation de l'atelier

1 | État des lieux

- Ce que nous voulons protéger
- Notre matériel
- Menaces actuelles

2 | Le *Digital Care Guide* de l'**irct**

**3 | Ateliers pratiques**

- **Mots de passe & Comptes**
- Appareils
- Communication
- Données

4 | Étapes de la réponse aux crises

5 | Étapes suivantes

# 3 | Protéger nos comptes et mots de passe

## Hameçonnage | Prévention

- Formation : <https://phishingquiz.withgoogle.com/>
- Vérifier les liens et les pièces jointes AVANT de cliquer : <https://virustotal.com>
- Ne jamais saisir les détails du compte et les informations d'identification avant de vérifier la demande

## Hameçonnage | Réaction

- 1) Mettre l'appareil concerné hors ligne
- 2) Changer les mots de passe concernés
- 3) Prévenir les personnes concernées
- 4) Consulter <https://digitalfirstaid.org>







Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE URL SEARCH



Choose file

By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the **sharing of your Sample submission with the security community**. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more](#).

Want to automate submissions? [Check our API](#), or access your [API key](#).



0 | Présentation de l'atelier

1 | État des lieux

- Ce que nous voulons protéger
- Notre matériel
- Menaces actuelles

2 | Le *Digital Care Guide* de l'**irct**

**3 | Ateliers pratiques**

- Mots de passe & Comptes
- Appareils
- **Communication**
- Données

4 | Étapes de la réponse aux crises

5 | Étapes suivantes



**irct**

International Rehabilitation  
Council for Torture Victims

## 3 | Protéger nos communications

LES MENACES :

• **Bombardement visioconférence**



• **Écoutes téléphoniques**  
(acteurs institutionnels)



• **Surveillance par les opérateurs**  
(acteurs institutionnels)



0 | Présentation de l'atelier

1 | État des lieux

- Ce que nous voulons protéger
- Notre matériel
- Menaces actuelles

2 | Le *Digital Care Guide* de l'**irct**

**3 | Ateliers pratiques**

- Mots de passe & Comptes
- Appareils
- **Communication**
- Données

4 | Étapes de la réponse aux crises

5 | Étapes suivantes

# 3 | Protéger nos communications

## Vidéoconférences

Utiliser :

- des services respectueux des données personnelles  
→ Signal, Wire, Whatsapp
- des services sur des serveurs fiables :  
→ JitsiMeet :
  - <https://meet.systemli.org>
  - <https://vc.autistici.org>
  - <https://meet.jit.si>
- BigBlueButton
  - <https://public.senfcall.de/gdpr/consent?>



Plus d'informations sur les vidéoconférences sécurisées ici :

- <https://www.frontlinedefenders.org/en/resource-publication/guide-secure-group-chat-and-conferencing-tools>

0 | Présentation de l'atelier

1 | État des lieux

- Ce que nous voulons protéger
- Notre matériel
- Menaces actuelles

2 | Le *Digital Care Guide* de l'**irct**

**3 | Ateliers pratiques**

- Mots de passe & Comptes
- Appareils
- **Communication**
- Données

4 | Étapes de la réponse aux crises

5 | Étapes suivantes

## 3 | Protéger nos communications

### Applications de messagerie

- Pour les informations et fichiers sensibles et confidentiels, privilégier Signal, Wire, Whatsapp
- Autant que possible, utiliser la fonctionnalité messages éphémères.



### E-mail

- Attention ! le hameçonnage vise majoritairement les boîtes mail
- Utiliser un mot de passe dédié
- Quand on envoie un mail à plusieurs personnes, se poser la question de la visibilité des adresses mail destinataires
- Éviter de se connecter à sa boîte mail sur un ordinateur public

0 | Présentation de l'atelier

1 | État des lieux

- Ce que nous voulons protéger
- Notre matériel
- Menaces actuelles

2 | Le *Digital Care Guide* de l'**irct**

**3 | Ateliers pratiques**

- Mots de passe & Comptes
- **Appareils**
- Communication
- Données

4 | Étapes de la réponse aux crises

5 | Étapes suivantes



**irct**

International Rehabilitation  
Council for Torture Victims

## 3 | Protéger nos appareils

LES MENACES :

• **Virus**



• **Piratage**



• **Perte de données**

(saisie judiciaire, vol, incendie,  
obsolescence, ...)



0 | Présentation de l'atelier

1 | État des lieux

- Ce que nous voulons protéger
- Notre matériel
- Menaces actuelles

2 | Le *Digital Care Guide* de l'**irct**

**3 | Ateliers pratiques**

- Mots de passe & Comptes
- **Appareils**
- Communication
- Données

4 | Étapes de la réponse aux crises

5 | Étapes suivantes



**irct**

International Rehabilitation  
Council for Torture Victims

# 3 | Protéger nos appareils



## Virus | Prévention

### Mises à jour

- Système d'exploitation : nous effectuons des mises à jour régulières de nos systèmes d'exploitation (mises à jour automatiques ou vérifications programmées)
- Applications & programmes : nous effectuons des mises à jour régulières de nos applications et programmes (mises à jour automatiques ou vérifications programmées)

### • Protection contre les virus

- Nous nous assurons que l'antivirus intégré à Windows 10 est activé
- Vous vérifions les liens et les pièces jointes AVANT de cliquer : <https://virustotal.com> <https://virustotal.com>

0 | Présentation de l'atelier

1 | État des lieux

- Ce que nous voulons protéger
- Notre matériel
- Menaces actuelles

2 | Le *Digital Care Guide* de l'[irct](#)

**3 | Ateliers pratiques**

- Mots de passe & Comptes
- **Appareils**
- Communication
- Données

4 | Étapes de la réponse aux crises

5 | Étapes suivantes



**irct**

International Rehabilitation  
Council for Torture Victims

# 3 | Protéger nos appareils



## Piratage | Prévention

- Sécuriser l'accès à tous nos appareils mobiles, portables ou de bureau à l'aide de **mots de passe longs et dédiés**.
- Faire des **mises à jour** régulières de nos appareils.
- **Séparation des appareils professionnels et personnels :**  
Si ce n'est pas possible, nous séparons au moins les profils d'utilisateur sur nos appareils.
- **Profils d'utilisateur et mots de passe :** il est possible de créer des profils d'utilisateur pour chaque personne qui utilise l'appareil.
- **Chiffrement du système de l'appareil :** pour protéger les données qui se trouvent sur nos appareils des accès non-autorisés, nous pouvons chiffrer les disques ou le système

0 | Présentation de l'atelier

1 | État des lieux

- Ce que nous voulons protéger
- Notre matériel
- Menaces actuelles

2 | Le *Digital Care Guide* de l'**irct**

**3 | Ateliers pratiques**

- Mots de passe & Comptes
- **Appareils**
- Communication
- Données

4 | Étapes de la réponse aux crises

5 | Étapes suivantes

## 3 | Protéger nos appareils



### Perte de données | Prévention

Il est bon d'être préparées à la **disparition de nos appareils**.

- Saisie (policière ou judiciaire)
- Vol
- Casse, incendie, obsolescence...

→ Parer à la **perte de données** avec des **sauvegardes**

→ **Réduire les risques de vol** (cachettes, garder en lieu sûr, ...)

→ Conserver des appareils de **rechange**

→ **Savoir réagir** lorsqu'un incident arrive (gestion de l'urgence)



0 | Présentation de l'atelier

1 | État des lieux

- Ce que nous voulons protéger
- Notre matériel
- Menaces actuelles

2 | Le *Digital Care Guide* de l'**irct**

**3 | Ateliers pratiques**

- Mots de passe & Comptes
- Appareils
- Communication
- **Données**

4 | Étapes de la réponse aux crises

5 | Étapes suivantes

## 3 | Protéger nos données

LES MENACES :

• **Panne ou mauvaise gestion des appareils**



• **Vol**



• **Partage non protégé de fichiers**



0 | Présentation de l'atelier

1 | État des lieux

- Ce que nous voulons protéger
- Notre matériel
- Menaces actuelles

2 | Le *Digital Care Guide* de l'**irct**

**3 | Ateliers pratiques**

- Mots de passe & Comptes
- Appareils
- Communication
- **Données**

4 | Étapes de la réponse aux crises

5 | Étapes suivantes

## 3 | Protéger nos données

### Stockage des fichiers

- Si l'on souhaite cacher nos données en cas de vol ou de saisie d'un appareil, il faudra chiffrer (crypter) le support de stockage de l'appareil.
  - Téléphone ou tablette (niveau facile)
  - Ordinateur (niveau facile à difficile)
    - Mac : <https://support.apple.com/fr-fr/HT204837>
    - Windows : Tutoriel 01net
  - Disque dur externe ou clé USB (niveau moyen)

### Sauvegardes

- Conserver plusieurs copies des données importantes, dont au moins une située dans un autre lieu ou en ligne

### Transfert de fichiers

- Les fichiers sensibles ne sont transférés en ligne que via des services fiables et de confiance, tels que:
  - <https://cryptpad.fr>
  - <https://upload.disroot.org>

0 | Présentation de l'atelier

1 | État des lieux

- Ce que nous voulons protéger
- Notre matériel
- Menaces actuelles

2 | Le *Digital Care Guide* de l'[irct](#)

**3 | Ateliers pratiques**

- Mots de passe & Comptes
- Appareils
- Communication
- **Données**

4 | Étapes de la réponse aux crises

5 | Étapes suivantes



**irct**

International Rehabilitation  
Council for Torture Victims

# 3 | Protéger nos données

## Gérer les sauvegardes

*Dans l'idéal : méthode « 3-2-1 » : 3 copies, 2 sur des supports distincts, 1 dans un autre lieu.*

- **Quoi sauvegarder**
  - Mots de passe, documents de travail (contrats, dossiers juridiques, dossiers médicaux des bénéficiaires, données de recherche...), historiques de conversation, ...
- **Sur quel support**
  - Disques durs externes
  - En ligne (serveur de confiance)
- **Où ranger le disque de sauvegarde**
  - Avoir au moins une copie dans un autre lieu et faire le déplacement régulièrement
- **À quelle fréquence faire des sauvegardes**
  - Définir une procédure et s'y tenir (une fois par semaine, ...)
- **Quel outil utiliser**
  - Copier/coller
  - Logiciel de sauvegarde (nécessite une formation)

0 | Présentation de l'atelier

1 | État des lieux

- Ce que nous voulons protéger
- Notre matériel
- Menaces actuelles

2 | Le *Digital Care Guide* de l'**irct**

**3 | Ateliers pratiques**

- Mots de passe & Comptes
- Appareils
- Communication
- **Données**

4 | Étapes de la réponse aux crises

5 | Étapes suivantes

# 3 | Protéger nos données

Gérer le site web **caprec.org**

**Mises à jour de WordPress**

- Pour éviter les piratages et les bugs
- Nécessite quelques compétences techniques
- Peut être automatisé (ou presque)
- Déléguer à une association/entreprise tierce ?

→ **Pratique** : mettre à jour le site web

**Activer HTTPS sur le site web**

- Pour que le site fonctionne avec plus de navigateurs web (Chrome, Firefox, Edge)
- À faire une seule fois dans les options de l'hébergement OVH

→ **Pratique** ?

0 | Présentation de l'atelier

1 | État des lieux

- Ce que nous voulons protéger
- Notre matériel
- Menaces actuelles

2 | Le *Digital Care Guide* de l'**irct**

3 | Ateliers pratiques

- Mots de passe & Comptes
- Appareils
- Communication
- Données

**4 | Étapes de la réponse aux crises**

5 | Étapes suivantes



**irct**

International Rehabilitation  
Council for Torture Victims

# 4 | Étapes de la réponse aux crises



Exemples d'incidents liés aux outils numériques :

- Ordinateur ou téléphone volé ou perdu
- Détection du piratage d'un appareil
- Surveillance accrue d'un·e membre de CAPREC
- ...

0 | Présentation de l'atelier

1 | État des lieux

- Ce que nous voulons protéger
- Notre matériel
- Menaces actuelles

2 | Le *Digital Care Guide* de l'irct

3 | Ateliers pratiques

- Mots de passe & Comptes
- Appareils
- Communication
- Données

**4 | Étapes de la réponse aux crises**

5 | Étapes suivantes



irct

International Rehabilitation  
Council for Torture Victims

## 4 | Étapes de la réponse aux crises



Certains incidents requièrent une réaction rapide, d'urgence.

### Étape 1 :

Selon la situation :

- Entrer en contact avec l'irct pour les informer et obtenir un suivi de la situation (à faire dans les 48h)
- Désactiver les accès des personnes concernées aux outils de CAPREC et de l'irct
- Informer les membres de CAPREC

### Étape 2 :

Pour reprendre l'activité normale de CAPREC :

- Se former afin de réduire les risques que l'incident se produise à nouveau
- Remplacer le matériel disparu (commander)
- Restaurer ses données depuis une copie de sauvegarde
- Rétablir les accès aux outils de CAPREC et de l'irct

0 | Présentation de l'atelier

1 | État des lieux

- Ce que nous voulons protéger
- Notre matériel
- Menaces actuelles

2 | Le *Digital Care Guide* de l'**irct**

3 | Ateliers pratiques

- Mots de passe & Comptes
- Appareils
- Communication
- Données

4 | Étapes de la réponse aux crises

**5 | Étapes suivantes**

## 5 | ETAPES SUIVANTES

Est ce qu'on les aide à se projeter dans la suite ?

0 | Présentation de l'atelier

1 | État des lieux

- Ce que nous voulons protéger
- Notre matériel
- Menaces actuelles

2 | Le *Digital Care Guide* de l'**irct**

3 | Ateliers pratiques

- Mots de passe & Comptes
- Appareils
- Communication
- Données

4 | Étapes de la réponse aux crises

**5 | Étapes suivantes**



**irct**

International Rehabilitation  
Council for Torture Victims

# CONTACTS

**Nos mails ?**

**+ nos dispos, possibilités de support à distance**

***MERCI !***

