

# Entre 11 et 14 actions à réaliser en cas de cyberattaque

## Actions immédiates

### Suspicion d'escroquerie avec pertes financières :

1. Faire opposition sur le moyen de paiement compromis immédiatement, simultanément couper le terminal du réseau retirer le câble ou arrêter le WIFI... (ne pas l'arrêter)
2. Rassembler les preuves et préparer le dépôt de plainte
3. Déposez plainte au commissariat de police ou à la brigade de gendarmerie en fournissant les preuves en votre possession
4. Suivre ensuite les étapes de 1 à 11 ci-dessous

### Si attaque sans pertes financières (avec certitudes) :

Suivre les étapes de 1 à 11 ci-dessous.

## A partir du terminal attaqué

### 1. Isoler l'appareil affecté :

- Déconnectez l'appareil d'Internet (débrancher le câble réseau, arrêter le WIFI ou le partage de connexion) pour éviter la propagation de l'attaque. Arrêter votre routeur Internet (Box).

**Option A - Si l'attaque est grave : ne provient pas d'un navigateur ou provoque un arrêt de service, ou rend l'accès impossible aux fichiers...) ou si elle concerne un terminal mobile (téléphone – tablette – système automatisé – objet connecté)**

- **contacter un expert en cybersécurité pour obtenir de l'aide. Pour ce faire, rendre compte de l'attaque sur le site <https://www.cybermalveillance.gouv.fr> ou appeler votre service informatique qui vous conseillera ou prendra l'intervention à son compte.**

**Option B Si l'attaque se fait via un navigateur et ne bloque pas de fonctions majeures de l'ordinateur**

### 2. Isoler l'appareil

- supprimer l'accès à Internet (débrancher le câble réseau, arrêter le WIFI ou le partage de connexion)
- prendre une photo de l'écran (servira éventuellement pour le compte rendu ou le dépôt de plainte)
- Vider totalement le cache du navigateur
- Arrêter l'ordinateur, attendre une minute puis le relancer.

### 3. Analyser et identifier :

- Exécutez un scan complet avec un logiciel antivirus ou antimalware pour identifier les menaces.
- Si le symptôme persiste appeler un expert.

**Comme l'appareil a été compromis on peut donc supposer que l'attaquant a eu accès à des informations, contacts, informations sensibles se trouvant sur l'ordinateur.**

## **A partir d'un autre terminal**

### **4. Changer les mots de passe :**

- modifiez immédiatement les mots de passe de tous vos comptes, en commençant par les plus sensibles (emails, banque, réseaux sociaux).

### **5. Vérifier les paramètres de messagerie :**

- Vérifiez que vous avez toujours accès à votre messagerie et que des modifications de paramétrage n'ont pas eu lieu (transfert de mails notamment).

### **6. Vérifier les comptes en ligne :**

- Consultez vos relevés bancaires et de cartes de crédit pour détecter toute activité frauduleuse (pour le cas où vous n'auriez pas remarqué l'escroquerie en premier lieu)

## **Une fois les opérations précédentes effectuées et l'attaque écartée**

### **7. Mettre à jour le logiciel :**

- Assurez-vous que votre système d'exploitation et tous vos logiciels sont à jour avec les derniers correctifs de sécurité.

### **8. Restaurer les données (éventuel) :**

- Si des fichiers ont été corrompus ou supprimés, restaurez-les à partir de sauvegardes récentes.

## **Pour terminer**

### **9. Prévenir vos contacts :**

Informez vos contacts que votre compte a été compromis, car ils peuvent recevoir des messages suspects de votre part.

### **10. Surveiller l'activité :**

- Continuez à surveiller vos comptes et appareils pour détecter toute activité suspecte future.

### **11. Signaler l'incident :**

- Rendez-compte de l'attaque sur le site <https://www.cybermalveillance.gouv.fr>

Ces actions vont **limiter** les conséquences de l'attaque. Il faudra prendre des **mesures complémentaires, notamment de renforcement de la sécurité** dès le retour à la normale.