Si vous êtes victime
(pour un ordinateur personnel)

Incident	Actions	État
Rançongiciel	**DÉBRANCHEZ VOTRE MACHINE D'INTERNET** ou du réseau informatique.	☐
	NE PAYEZ PAS LA RANÇON réclamée car vous n'êtes pas certain de récupérer vos données et vous alimenteriez le système mafieux.	☐
	CONSERVEZ LES PREUVES : message piégé, fichiers de journalisation (logs) de votre pare-feu, copies physiques des postes ou serveurs touchés. À défaut, conservez les disques durs.	☐
	DÉPOSEZ PLAINTE au commissariat de police ou à **la gendarmerie** ou en écrivant **au procureur de la République** dont vous dépendez en fournissant toutes les preuves en votre possession.	☐
	IDENTIFIEZ LA SOURCE DE L'INFECTION et prenez les mesures nécessaires pour qu'elle ne puisse pas se reproduire.	☐
	APPLIQUEZ UNE MÉTHODE DE DÉSINFECTION ET DE DÉCHIFFREMENT, lorsqu'elle existe*. En cas de doute, effectuez une restauration complète de votre ordinateur. Reformatez et réinstallez un système sain puis restaurez les copies de sauvegarde des fichiers perdus lorsqu'elles sont disponibles. **Le site suivant peut fournir des solutions dans certains cas : https://www.nomoreransom.org/fr/index.4html*	☐
	FAITES-VOUS ASSISTER AU BESOIN PAR DES PROFESSIONNELS QUALIFIÉS. Vous trouverez sur *www.cybermalveillance.gouv.fr* des professionnels en sécurité informatique susceptibles de pouvoir vous apporter leur assistance.	☐
	LISEZ LA FICHE "PREVENTION_Rancongiciel" pour ne plus vous faire avoir les prochaines fois.	☐