

## L'arnaque au faux support technique (ou au faux dépannage informatique)

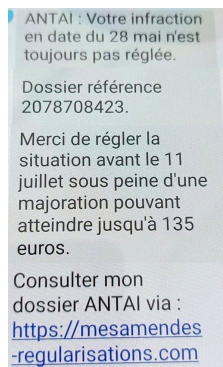
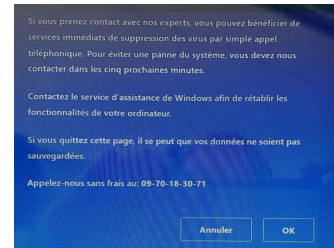
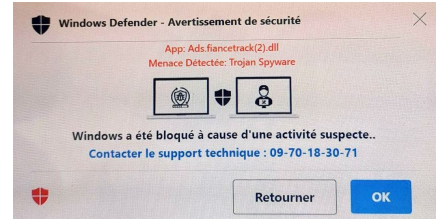
Scénario : Vous naviguez sur Internet et un message "de sécurité" (visuel ET sonore) surgit, "bloquant" votre ordinateur : "Vous êtes victime d'un virus, et vous DEVEZ appeler le numéro de téléphone affiché", avec les logos "rassurants" de Microsoft et Windows.

**N'APPELEZ SURTOUT PAS** : votre ordinateur N'EST PAS BLOQUE, c'est seulement la page de votre navigateur qui ne se ferme pas ! Forcez sa fermeture et arrêtez votre ordinateur.

**Ne restaurez pas les pages** au redémarrage.

Cet appel vers un(e) soit-disant technicien(ne) TRES convaincant(e) entraîne l'installation de logiciels malveillants avant de vous facturer un présumé service d'assistance !

**Parade : Ne pas appeler et redémarrer l'ordinateur.**



## L'arnaque à l'amende impayée de l'ANTAI

Un SMS vous propose de régulariser une amende impayée : l'ANTAI n'envoie **jamais** de SMS. Ne cliquez pas sur le lien !

Le but recherché est de voler des informations personnelles ou professionnelles (comptes, mots de passe, coordonnées bancaires...) pour en faire un usage frauduleux ou les revendre sur le Darknet (web clandestin).

Si le lien de paiement ne vous redirige pas vers l'UNIQUE site officiel de paiement des amendes : [www.amendes.gouv.fr](http://www.amendes.gouv.fr) alors l'expéditeur n'est pas l'ANTAI. C'est un site frauduleux !

**Réflexe : Ne pas cliquer et supprimer le SMS.**

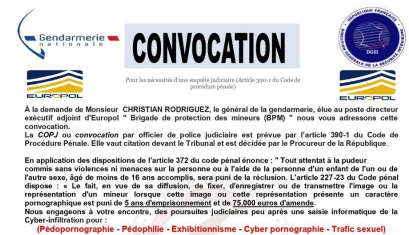
## L'arnaque à la convocation à la Brigade des Mineurs

Un mail portant le logo de la Gendarmerie ou de la Police Judiciaire avertit son destinataire qu'il fait l'objet de poursuites judiciaires après une "saisie de la Cyber-infiltration pour pédopornographie, pédophilie, exhibitionnisme, cyber pornographie, trafic sexuel" pour avoir visionné des photos/vidéos sur des sites à caractère pornographique.

Vue la gravité des infractions citées dans ce faux mail, la Justice ne vous envoie pas de convocation, elle vous fait réveiller à 6 heures du matin ... et sans café ni croissant.

La Justice **ne convoque pas par mail** et n'utilise pas de boîtes Gmail, Outlook, etc... mais uniquement en ".gouv.fr"

**Riposte : Ignorer le Mail.**



Si vous voulez coopérer, en plus de mon inaction, je vous donnerai toutes les informations sur le client et la raison pour laquelle cette personne en a après vous.

**PS ... Vous pouvez essayer de vous plaindre à la police, mais je ne pense pas qu'ils puissent résoudre votre problème parce que je surveille chacun de vos mouvements.**

Envoyez un courriel à [redacted]@gmail.com

Vous avez 48 heures pour prendre une décision.

L'ange de la mort



## L'arnaque au tueur à gages

Vous recevez un mail d'un "Ange de la Mort" qui dit avoir été engagé pour vous assassiner et qui vous propose de le payer pour annuler ce contrat et vous révéler le nom de son commanditaire !

Pas de panique, il ne s'agit que d'une tentative d'arnaque qui vise à vous effrayer et susciter votre curiosité pour vous extorquer de l'argent.

**Riposte : Ignorer le Mail.**

## Les arnaques au phishing : AMELI, Impôts, Colissimo ou autre distributeur.

Des mails ou SMS promettent le remboursement d'un soin médical, ou d'un trop perçu fiscal !

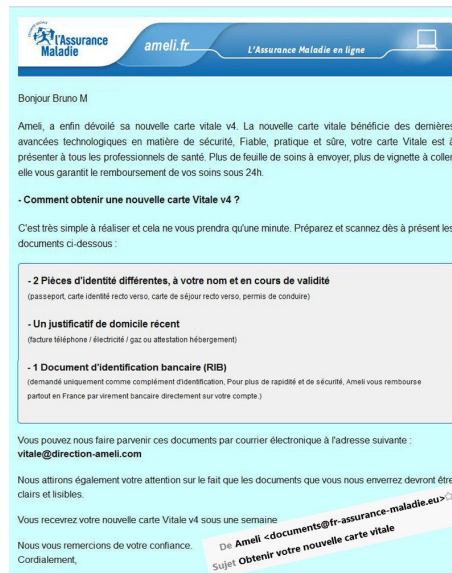
D'autres vous invitent à obtenir votre nouvelle Carte Vitale ou à réclamer un colis non remis.

Il s'agit évidemment d'une escroquerie au phishing, vous orientant vers un faux site internet, très bien imité, qui a pour objectif de récupérer vos données personnelles, d'identité et bancaires.

Ne communiquez jamais d'informations sensibles par messagerie ou téléphone : aucune administration ne vous demandera vos coordonnées bancaires ou vos mots de passe par message.

Elle vous invitera à vous connecter sur votre Espace Personnel et à utiliser la messagerie sécurisée.

**Réflexe : Ne jamais cliquer sur les liens.**



## CONSEILS DE SECURITE :

- ne répondez **JAMAIS** à un message vous demandant votre numéro de carte bancaire ou une copie de vos pièces d'identité (... *d'ailleurs, avez-vous vraiment reçu ce message ?*)
- ne cliquez **JAMAIS** sur un lien proposé dans un courriel ou un SMS : saisissez l'adresse du site officiel que vous aurez recherché par vous-même
- vérifiez toujours l'adresse de l'expéditeur d'un message avant de l'ouvrir (affichez les détails)
- renseignez et confirmez votre numéro de téléphone portable sur votre espace personnel pour en protéger l'accès avec la double authentification (2FA).

**Combattez** ces arnaques en les signalant sur la plate-forme correspondante :

Spam par mail : [www.signal-spam.fr](http://www.signal-spam.fr)



Spam par SMS : **33700** et [www.33700.fr](http://www.33700.fr)



Fraude à la carte bancaire : **Perceval**



[www.service-public.fr](http://www.service-public.fr)

Escroquerie sur Internet : **Thesee**



[www.service-public.fr](http://www.service-public.fr)

Contenu illicite sur Internet : **Pharos**



[www.internet-signalement.gouv.fr](http://www.internet-signalement.gouv.fr)

Assistance : [www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)



Et consultez les pages **Sécurité et Sauvegarde** du site : <https://www.eponacli.fr>