Baronnies
INFORMATIQUE

Particuliers et familles · Ressource gratuite

Kit anti-arnaque

En 10 minutes, vos proches sauront reconnaître un faux SMS, et quoi faire s'ils ont cliqué.

Pour les seniors et leurs enfants. À imprimer et à garder près du téléphone.

Mis à jour le 1er octobre 2026 · Version en ligne : baronnies-informatique.fr/ressources/kit-anti-arnaque

Au sommaire

1. La fiche frigo : 5 réflexes
2. Où vérifier un message, sans cliquer
3. J'ai cliqué : que faire dans l'heure
4. Le mot de passe de famille
5. Nous contacter

Amende à payer, colis bloqué, carte Vitale à renouveler : les faux SMS imitent des messages officiels et poussent à agir vite. Ce kit tient en quelques pages. Imprimez-le, lisez-le avec vos proches et gardez la fiche près du téléphone.

La fiche frigo : 5 réflexes

✂ À découper et à garder à portée de main.

1. **Je ne clique pas sur un lien reçu par SMS.** Je passe par l'application ou par le site officiel, dont je tape l'adresse moi-même.
2. **Je ne donne jamais un code.** Ni ma banque, ni l'Assurance maladie, ni les gendarmes ne me demandent un code reçu par SMS ou mes mots de passe.
3. **L'urgence est un piège.** « Dernier rappel », « sous 24 h », « majoration » : je prends le temps et j'en parle à un proche.
4. **Je vérifie par moi-même.** Une amende, un colis, un remboursement : je regarde sur le site officiel, jamais depuis le message.
5. **Au moindre doute, je raccroche.** Je rappelle le numéro que je connais déjà : dos de la carte bancaire, courrier, contact enregistré.

Les numéros utiles

POUR	QUI APPELER	QUAND
Signaler un SMS suspect	**Transférer le SMS au 33700**	Gratuit, à tout moment
Bloquer ma carte bancaire	Le numéro de ma banque, ou le 0 892 705 705	24 h/24, appel surtaxé
Être conseillé après une arnaque	Info Escroqueries : 0 805 805 817	Gratuit, du lundi au vendredi, de 9 h à 18 h 30
Être aidé en tant que victime	France Victimes : 116 006	Gratuit, 7 jours sur 7, de 9 h à 19 h

Le numéro de ma banque : .....

Où vérifier un message, sans cliquer

Le bon réflexe : ouvrir soi-même le site ou l'application, puis regarder si le message y apparaît. S'il n'y a rien, c'était une arnaque.

Le message reçu, et où vérifier

LE MESSAGE PARLE DE…	À SAVOIR	OÙ VÉRIFIER
Une amende à payer	L'ANTAI n'envoie jamais de SMS.	antai.gouv.fr ou amendes.gouv.fr
Un colis en attente, des frais de livraison	Un petit montant à régler sert à voler la carte bancaire.	Le site du transporteur, avec le numéro de suivi reçu lors de la commande
La carte Vitale ou un remboursement de santé	L'Assurance maladie ne demande jamais vos identifiants ni votre numéro fiscal.	La messagerie de votre compte ameli
Votre compte formation (CPF)	Un message qui presse d'utiliser vos droits est suspect.	moncompteformation.gouv.fr
Une opération bancaire à valider	Votre banque ne vous demande jamais de valider une opération pour l'annuler.	Le numéro au dos de votre carte ou votre application bancaire
Un remboursement d'impôts, de CAF ou d'énergie	Un remboursement arrive sur votre compte bancaire : pas besoin de donner votre carte.	impots.gouv.fr, caf.fr ou l'espace client de votre fournisseur

J’ai cliqué : que faire dans l’heure

1. **Ne répondez plus**
   Fermez la page. Ne rappelez pas le numéro qui vous a écrit et ne répondez pas au message.

2. **Carte bancaire donnée ? Faites opposition**
   Appelez tout de suite le numéro de votre banque, ou le **0 892 705 705** (24 h/24). Vous recevrez un numéro d’enregistrement : notez-le.

3. **Mot de passe tapé ? Changez-le**
   Changez-le sur le vrai site, en tapant son adresse vous-même. Faites de même partout où vous utilisez ce mot de passe.

4. **Gardez les preuves**
   Ne supprimez pas le SMS. Faites une capture d’écran, puis transférez le message au 33700 pour le signaler.

5. **Surveillez vos comptes**
   Prévenez votre banque, même si rien n’a été débité, et regardez vos relevés dans les jours qui suivent.

6. **Faites-vous aider**
   Info Escroqueries vous conseille au **0 805 805 817**. Le site **17cyber.gouv.fr** propose un diagnostic en ligne. Si de l’argent a été pris, portez plainte au commissariat ou à la gendarmerie.

Vous avez seulement cliqué, sans rien taper ?

Le risque est plus faible. Fermez la page, n’installez rien de ce qu’elle propose et signalez le SMS au 33700.

Le mot de passe de famille

« Coucou maman, j'ai changé de numéro, tu peux m'aider ? » L'arnaque au faux proche arrive par SMS, par WhatsApp, et parfois par un appel dont la voix a été imitée. Le message demande de l'argent, vite.

La règle officielle : rappeler la personne sur son numéro habituel avant d'envoyer quoi que ce soit. Un mot de passe de famille rend cette vérification immédiate.

À faire ensemble, une fois pour toutes

- [ ] Choisir un mot ou une courte phrase facile à retenir, que personne ne peut deviner : ni un prénom, ni une date de naissance.
- [ ] Ne jamais l'écrire dans un SMS, un e-mail ou sur les réseaux sociaux.
- [ ] Se fixer une règle : une demande d'argent urgente sans le mot de passe, on raccroche et on rappelle la personne sur son numéro habituel.
- [ ] Le partager avec les grands-parents, et avec les petits-enfants.

⚠ **Quand la fiche ne suffit plus**

Votre proche reçoit plusieurs SMS suspects par semaine ? Il a déjà cliqué une fois ? Il vit seul, loin de vous ? Il faut alors aussi régler son téléphone et sa messagerie.

Aller plus loin avec Baronnies Informatique

On se déplace chez vos parents à Nyons, Vinsobres et dans les Baronnies, ou on les aide à distance. On sécurise leur téléphone et leur boîte mail, puis on leur montre les bons gestes, à leur rythme.

- ✓ Filtrer les SMS et les appels de numéros inconnus
- ✓ Faire les mises à jour et les rendre automatiques
- ✓ Activer la double authentification sur la messagerie
- ✓ Ranger les mots de passe en lieu sûr

Un doute, une question ?

Appelez-nous ou décrivez la situation. Une estimation vous est donnée avant toute intervention.

Appelez Baronnies Informatique

06 29 53 70 01

Ou scannez ce code pour nous écrire depuis votre téléphone.
baronnies-informatique.fr

Lundi, mardi, jeudi et vendredi, de 9 h 30 à 18 h. À domicile ou à distance, sur rendez-vous.

Sources

Informations vérifiées le 30 septembre 2026.

Hameçonnage (phishing) : que faire ?, Cybermalveillance.gouv.fr : www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing

Escroquerie à l'enfant qui a un problème avec son téléphone « Coucou maman/papa… », Cybermalveillance.gouv.fr : www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/escroquerie-enfant-probleme-telephone-coucou-papa-maman

Démarchage téléphonique abusif, spam vocal ou par SMS : que faire ?, Service-public.gouv.fr : www.service-public.gouv.fr/particuliers/vosdroits/F33267

Assurance maladie : se protéger des escroqueries et des messages frauduleux, Service-public.gouv.fr : www.service-public.gouv.fr/particuliers/actualites/A17150

Attention aux SMS, courriels et sites frauduleux, Préfecture du Haut-Rhin : www.haut-rhin.gouv.fr/Actions-de-l-Etat/Transports-deplacements-et-securite-routiere/Attention-aux-sms-courriels-et-sites-frauduleux

Opposition carte bancaire : réagir vite en cas de perte, vol ou fraude, Les clés de la banque : www.lesclesdelabanque.com/particulier/opposition-carte-bancaire/

17Cyber, l'assistance en ligne pour les victimes de cybermalveillance, Police nationale, Gendarmerie nationale et Cybermalveillance.gouv.fr : www.17cyber.gouv.fr/