CHECK-LIST GRATUITE · ARNAQUES ET NUMÉRIQUE

Protéger ses parents des arnaques

Les actions du guide, à cocher au fur et à mesure. Les explications, les délais et les lettres prêtes à adapter sont dans le guide complet.

Pour : _____

Remis par : _____ le _____

Pour me joindre : _____

Partie 1. En parler avec vos parents, sans les infantiliser

Se mettre d'accord sur une règle de famille

- [ ] Avant tout paiement demandé en urgence, on s'appelle.
- [ ] On ne donne jamais un code reçu par SMS, quel que soit l'interlocuteur.
- [ ] On raccroche, puis on rappelle soi-même le numéro habituel de la banque ou de l'organisme.

Partie 2. Le faux conseiller bancaire

Ce qu'une vraie banque ne demande jamais

- [ ] votre mot de passe ;
- [ ] des codes de confirmation ;
- [ ] de valider ou d'annuler des opérations dans l'application, pour une prétendue fraude ;
- [ ] le code confidentiel de votre carte ;

- [ ] de remettre votre carte à un coursier ou à toute autre personne venue la chercher.

Partie 3. Les faux messages : SMS, courriels et appels

Les indices qui doivent alerter

- [ ] Le message vient d'un service dont on n'est pas client.
- [ ] L'adresse ou le numéro ne ressemble pas à celui de l'organisme officiel.
- [ ] L'orthographe, la grammaire ou la signature paraissent étranges.
- [ ] Le ton est alarmiste et pousse à agir vite.

Partie 4. Quatre arnaques en forte hausse

Le faux dépannage informatique

- [ ] Ne pas appeler le numéro affiché, ne pas répondre au message.
- [ ] Prendre l'écran en photo, pour garder une preuve.
- [ ] Fermer la fenêtre. Si elle occupe tout l'écran, appuyer sur la touche Échap (« Esc ») ou F11. Si cela ne suffit pas, redémarrer l'ordinateur.
- [ ] Ne jamais laisser prendre la main à distance une personne qui vous a sollicité, sans être certain de son identité.

Les faux placements d'argent

- [ ] vous ne connaissez pas la personne qui vous contacte ;
- [ ] on vous promet des rendements très élevés et sans risque ;
- [ ] vous devez décider rapidement ;
- [ ] vous devez faire un virement vers un compte à l'étranger.
- [ ] Vérifier que la société ne figure pas sur les **listes noires de l'AMF** : amf-france.org, listes noires.
- [ ] Vérifier qu'elle est autorisée à exercer en France, sur le registre officiel regafi.fr. On y cherche le nom de la société, indiqué dans les mentions légales de son site.

- [ ] En cas de doute, appeler **AMF Epargne Info Service** au 01 53 45 62 00, du lundi au vendredi de 9 h à 12 h 30 (prix d'un appel local).

Le compte piraté

- [ ] Si votre parent ne peut plus se connecter : contacter le service concerné pour retrouver l'accès.
- [ ] Changer tout de suite le mot de passe, et le changer aussi sur les autres sites où il servait.
- [ ] Vérifier le numéro de téléphone et l'adresse de secours du compte : supprimer ceux qui sont inconnus, après une capture d'écran.
- [ ] Déconnecter les appareils inconnus, dans les paramètres du compte.
- [ ] Activer la double authentification (un code en plus du mot de passe).
- [ ] Prévenir ses contacts : l'escroc pourrait se faire passer pour votre parent auprès d'eux.
- [ ] Prévenir la banque si des coordonnées bancaires étaient enregistrées sur le compte.

Partie 6. Le démarchage à domicile et les faux artisans

Les bons réflexes à la porte

- [ ] On ne signe rien le jour même.
- [ ] On ne paie rien sur place.
- [ ] On demande un devis écrit et on en parle à un proche.
- [ ] En cas de panne urgente, on appelle un artisan que l'on connaît, ou on demande conseil à un proche.

Partie 7. Les protections à mettre en place ensemble

Le téléphone et l'ordinateur

- [ ] faire les mises à jour de sécurité (téléphone, ordinateur, applications) ;
- [ ] installer les applications uniquement depuis les magasins ou sites officiels ;

- [ ] utiliser un antivirus ;
- [ ] utiliser des mots de passe différents et complexes pour chaque site ;
- [ ] activer la double authentification (un code en plus du mot de passe).

La banque

- [ ] Noter le numéro officiel de la banque et le numéro d'opposition de la carte sur la fiche de la partie 8.
- [ ] Demander à la banque si elle peut envoyer une alerte à chaque opération.
- [ ] Rappeler la règle : aucun code ne se donne, à personne.

Partie 8. La fiche à poser près du téléphone

Avant de répondre « oui »

- [ ] Je ne donne **jamais** un code reçu par SMS, ni le code de ma carte.
- [ ] Je ne remets **jamais** ma carte à un coursier ou à un inconnu.
- [ ] Je ne clique pas sur un lien reçu par SMS ou courriel.
- [ ] Je ne paie rien à un vendeur venu à la maison avant 7 jours.
- [ ] Je ne laisse **personne** prendre la main à distance sur mon ordinateur.
- [ ] Je ne place pas d'argent sur le conseil d'un inconnu.
- [ ] En cas de doute, **je raccroche et j'appelle un proche**.

Partie 9. Si c'est arrivé : que faire tout de suite

2. Garder les preuves

- [ ] Les messages reçus (SMS, courriels), avec la date.
- [ ] Le numéro de téléphone de l'escroc, ou l'adresse du faux site.
- [ ] Les relevés montrant les opérations frauduleuses.
- [ ] Le contrat, le devis ou le reçu laissé par le vendeur.

Le guide complet

Protéger ses parents des arnaques : 25 pages, en PDF et en EPUB, 7,90 €.

Chaque étape y est expliquée, avec ses délais, les sources officielles et des lettres prêtes à adapter.

https://lesguidesuniques.com/fr/arnaques-numerique/anti-arnaque-parents/

Auteur : Yvan (micro-entreprise, Bastia). Mis à jour le 28 octobre 2026. Ce guide ne remplace pas un avocat ou un conseiller.