Arnaques et escroqueries : comment les identifier et agir

3 grands principes à retenir :

- **L'ingéniosité des nuisibles n'a d'égal que la crédulité des victimes**
- **Le maillon le plus faible de la chaîne de sécurité est l'utilisateur lui-même**
- **La meilleure protection est le bon sens et le temps de réflexion**

Les arnaques se manifestent sous deux formes :

- Le contact direct : visite à domicile, prospectus de dépannage ou contact téléphonique
- La forme numérique : courriel ou site Web

Leur but est toujours le même :

- Vous extorquer des informations et de l'argent. Mots de passe, données personnelles, coordonnées bancaires, accès à vos comptes en ligne...
- Reconnaître vos locaux dans le cas d'une visite pour cambriolage ultérieur
- Vous faire signer des contrats divers
- …

Même si vous pensez être un cas isolé, n'oubliez pas qu'un cybercriminel peut toucher des milliers de personnes par jour.

Premier cas :

- Une ou plusieurs personnes se présentent à votre domicile sous un prétexte quelconque
- Un défaut a été repéré sur votre toit
- La mairie fait contrôler les compteurs ou les circuits d'eau, de gaz ou d'électricité
- Document dans votre boîte aux lettres proposant différents services de dépannage semblant provenir de ma mairie (bleu blanc rouge)
- Enquêtes diverses
- Vous recevez un coup de téléphone vous informant que vous avez gagné un lot, un voyage ou autre
- Mettre en place votre compte CPF (compte personnel de formation)
- …

Comment réagir :

- Ne pas laisser entrer le ou les personnes avant d'avoir vérifié leurs dires. Au besoin utiliser un entrebâilleur.
- Demander une carte professionnelle avec photo
- Téléphoner à la mairie (01 65 49 59 49) ou à l'organisme qu'ils représentent
- En cas de doute appeler la police municipale (01 64 49 55 60 / 06 22 66 79 64) et/ou la gendarmerie de Nozay (01 69 63 25 00 ou 17)
- Ne signer aucun papier directement : demandez un délai.
- Au téléphone ne donner aucun renseignement personnel immédiatement et rappeler directement l'organisme. Se méfier des numéros en 06 ou 07 et ceux venant de l'étranger.

Second cas :

Cela se manifeste par un courriel semblant venir d'un organisme officiel, le plus souvent avec une pièce jointe et/ou un lien internet.

Comment identifier une arnaque ?
Souvent les mails sont d'un français approximatif, fautes d'orthographe, adresse d'expéditeur à l'étranger etc.
Les sujets des arnaques en ligne se renouvellent régulièrement mais le fonctionnement reste souvent le même : vous recevez une fausse information et vous êtes invité à cliquer sur un lien pour corriger une situation qui n'existe pas.

Les exemples sont nombreux :

- Vous recevez un mail ou un sms provenant d'un expéditeur ou d'un organisme de confiance, vous invitant à cliquer sur un lien pour mettre à jour votre compte, toucher une somme ou récupérer un colis
- Lors de votre navigation, vous découvrez un juteux filon pour investir simplement dans une crypto-monnaie (Bitcoin, Ethereum) ;
- Un mail vous indique qu'on a piraté votre webcam, enregistré votre historique de navigation sur des sites pornographiques et, bien entendu, recueilli la liste de tous vos codes et contacts.
- Vous êtes héritier d'une forte somme mais vous devez acquitter des frais préalablement.

Tout cela est faux !

Comment réagir ?
Vous avez un doute sur le message que vous avez reçu :

- Ne paniquez pas ! Vous n'avez sans doute rien de compromettant à vous reprocher ;
- Ne cliquez pas sur un lien ou une pièce jointe sans être sûr de la fiabilité de son expéditeur ;
- Vérifiez l'adresse de l'expéditeur : contactez-le par un autre canal ou regardez l'adresse d'expédition en passant le curseur dessus. Un organisme officiel aura presque systématiquement une adresse mail de type "ne-pas-repondre@ministere.gouv.fr" ;
- Si vous pensez qu'il s'agit de désinformation (Hoak) consultez les sites https://hoaxbuster.com/ et https://hoaxkiller.com/
- Ne répondez jamais à un mail suspect ou à du chantage, pour ne pas montrer à l'expéditeur que vous êtes réceptif au message et ne payez pas de demande de rançon ;
- Changez vos mots de passe régulièrement, évitez d'avoir le même mot de passe pour chaque compte afin d'éviter les contaminations en chaîne et si possible, activez l'authentification à double facteur ;
- Faîtes des captures d'écran et signalez le mail ou le sms sur le site www.signal-spam.fr Ce site met à disposition une application qui s'installe dans les navigateurs Internet (Firefox, Chrome, Safari…) et les applications de messagerie (Outlook, Thunderbird…).

Vous avez déjà payé ou communiqué des informations personnelles ? Vous êtes victime d'une escroquerie.
Dans ce cas :

- Vérifiez qui a accédé aux comptes dont vous avez communiqué les identifiants ;
- Changez immédiatement les mots de passe des comptes compromis et suspendez votre carte de crédit;
- Adressez-vous à votre banque pour tenter de faire annuler le paiement ;
- Signalez les faits sur le site www.internet-signalement.gouv.fr et/ou sur la plateforme PHAROS ici https://www.service-public.fr/particuliers/vosdroits/R17674 ;
- Rendez-vous dans la gendarmerie de Nozay (01 69 63 25 00 ou 17) pour déposer plainte pour escroquerie ou extorsion de fonds, ou adressez votre plainte par écrit au procureur de la République du tribunal judiciaire de votre domicile.

Ce texte est largement inspiré su site de la gendarmerie www.gendarmerie.interieur.gouv.fr