

## La réalité numérique :

Internet est un espace merveilleux dans lequel une multitude d'informations et de services sont accessibles.

Toutefois, les délinquants ont bien compris l'intérêt qu'ils avaient à commettre des arnaques dans cet univers où les frontières n'existent plus vraiment et où l'anonymat est aisé.

Tout internaute peut devenir la victime de cette délinquance numérique. Il convient donc de prendre des mesures qui constituent

## *La cybersécurité*

### Qui peut m'aider ?

La plupart des personnes qui subissent une arnaque sur internet auraient pu éviter d'être victime en adoptant des comportements simples de bon sens.

La première protection contre ce fléau concerne donc votre attitude.

### ***Réfléchissez avec de Cliquez***

*Et adoptez des réflexes simples...*

<https://www.cybermalveillance.gouv.fr/>

## *Si vous êtes victime*

*Rendez vous à votre  
gendarmerie et  
demandez à rencontrer  
le correspondant NTECH*



Ne modifiez rien sur vos équipements numériques.

N'ayez pas honte de ce qui vient de vous arriver.

Contactez très rapidement votre banque pour tenter de bloquer la transaction que vous venez de faire dans le cadre d'une escroquerie.

Pour en savoir plus connectez vous sur :

<https://www.internet-signalement.gouv.fr/>

Site de l'ANSSI : [www.ssi.gouv.fr/](http://www.ssi.gouv.fr/)

## *Conseils pour prévenir les actes de délinquance*

### *Fiche d'informations*

## *Comment se protéger des arnaques sur internet*



## La sensibilité, une faiblesse sur internet :

-De nombreuses internautes pensent pouvoir faire de belles rencontres sur internet et c'est parfois le cas. Toutefois certaines personnes sont très exposées aux escrocs car ils se servent de leur fragilité affective.

- Les victimes les plus nombreuses sont les personnes seules en quête d'affection et qui ne connaissent pas bien le fonctionnement d'internet. Ne vous laissez jamais attendrir par une personne que vous n'avez jamais rencontrée physiquement.

L'amitié ou l'amour se construisent toujours dans la vraie vie, ne soyez pas naïf

## Protéger ses mails :



Évitez d'indiquer votre nom et prénom dans votre adresse mail.

Ne communiquez jamais votre mot de passe donnant accès à votre boîte mail.

N'ouvrez jamais un mail et ses fichiers joints si vous avez un doute sur sa provenance ou si vous ne connaissez pas l'expéditeur.

Dans votre boîte mail ne conservez pas d'informations personnelles ou sensibles.

Ne laissez pas traîner la liste de vos mots de passe sur un bout de papier.

Partenaire de  
votre sûreté



## Choisir son mot de passe :

Il est nécessaire de choisir des mots de passe robustes, difficiles à retrouver à l'aide d'outils automatiques.

Utilisez un mot de passe unique pour chaque service. Votre messagerie professionnelle et personnelle doivent impérativement avoir un mot de passe différent. Suivez ces conseils :

- Choisir un mot de passe qui n'a pas de lien avec vous (pas de date, nom ou prénom...)

- Renouvelez vos mots de passe avec une fréquence raisonnable ou en cas de doute.

- Ne pas stocker vos mots de passe dans un fichier sur un poste informatique exposé, et encore moins sur un papier facilement accessible.

- Ne vous envoyez pas vos mots de passe sur votre messagerie.

- Configurez les logiciels, y compris votre navigateur Web, pour qu'ils ne mémorisent pas les mots de passe choisis.

La robustesse d'un mot de passe dépend de sa complexité, optez pour un mot de 8 à 12 caractères différents comportant des majuscules, des minuscules, des chiffres et des caractères spéciaux.

Afin de faciliter la mémorisation de ces mots de passe, vous pouvez utiliser une méthode phonétique ou la méthode des premières lettres d'une phrase.

## Les achats sur internet :

- Lors d'un paiement en ligne assurez vous que l'adresse internet commence par Https// la présence du S fait état d'une sécurisation

- Privilégiez les systèmes de paiement pas e-card (renseignez vous auprès de votre banque)

Ne communiquez jamais vos coordonnées bancaires par mail.

Évitez les commandes en ligne à partir d'un accès internet public.

## L'identité numérique :

- Sur les réseaux sociaux ne divulguez pas votre identité réelle.

Pensez à utiliser un pseudonyme. Ne communiquez pas votre numéro de téléphone, votre adresse ou vos photos et celles de vos enfants.

Ne communiquez pas d'information qui peuvent porter atteinte à votre réputation.

Il n'est pas aisé de retirer définitivement un contenu indélicat laissé sur internet.

Vous êtes responsables de vos publications et du contenu de vos échanges



Testez vos connaissances en cyber sécurité :  
<https://www.referentsurete.com/q/quizGNCYBERNIVEAU1.html>

Consultez des fiches conseils sur notre espace  
[referentsurete.com](https://www.referentsurete.com) :

