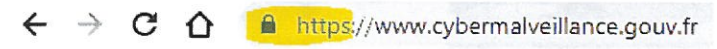
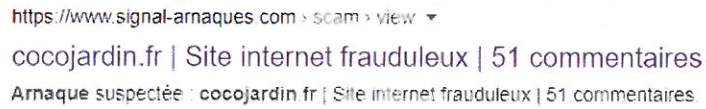
LE P'TIT MEMO DES BONNES PRATIQUES NUMÉRIQUES

- **Ne pas communiquez ses données personnelles sur les forums ou réseaux sociaux,** pour éviter un phishing ciblé.
- **Avant de cliquer sur un lien douteux, positionnez le curseur de votre souris sur ce lien (sans cliquer) clic droit et copiez le lien sur internet** pour vérifier l'exactitude de l'adresse du site Internet en prenant garde aux fautes d'orthographe
- **Vérifiez l'adresse du site qui s'affiche dans votre navigateur, (S** pour sécurisé, près de l'URL, d'un pictogramme en forme de **cadenas**)



- **Vérifiez le site concerné en tapant sur internet son nom+ le mot arnaque et/ou avis** ex : cocojardin.fr avis et arnaques – résultats :



- **N'ouvrez pas les courriels suspects** (trop alléchant ou trop alarmant)**, leurs pièces jointes et ne cliquez par sur les liens, regardez le détail de l'adresse expéditeur.**
- **Si possible, lors d'un achat en ligne** n'hésitez pas à vous rapprocher de **votre banque** pour connaître **et utiliser les moyens sécurisés qu'elle propose.**
- **Google demande souvent d'enregistrer notre mot de passe (mdp) ….bonne idée ou pas ? Mauvaise idée !** C'est très pratique… pour les hackers. Ils se trouvent dans des fichiers avec mdp déjà intégrés. facilement retrouvable**. N'enregistrez pas vos mdp sur votre PC !**
- **Séparez les usages personnels des usages professionnels**
- **Naviguez sur internet en mode privé,** car pas d'historique de navigation, réduction des pubs…
- **Mettez régulièrement à jour vos appareils et leurs logiciels ou applications**
- **Pour vos sauvegardes appliquez la règle 3.2.1 => 3 copies** de vos données sur **2 supports** différents et **1 sauvegarde hors site.**
- **Éteignez votre machine lorsque vous ne vous en servez pas**
- **Si mail douteux et ordinateur bloqué :** ne pas appelez de suite, faire un CRTL + ALT +Supp sur votre clavier en même temps pour vérifier que vous pouvez quitter la page

Face à une attaque : Isoler l'équipement infecté en débranchant le câble réseau (Ethernet) ou coupez l'accès au Wi-Fi et/ou Bluetooth s'il s'agit d'un appareil mobile (téléphone, tablette), le déconnecter d'internet, Attention : ne pas éteindre la machine infectée. *Faites-vous assister au besoin par des professionnels qualifiés. Vous trouverez sur www.cybermalveillance.gouv.fr*