

## Café numérique du Dream Café « Atelier d'écriture »

Atelier « Mon bilan de cyber-vulnérabilité » animé par Rosario avec la participation de benasof, fredolerouge, Gabrielsanchez, GAEL, guigui, Imran, Lefebvre, mél21, mumu, Nass, nicolafella, nuts, Sébastien0475, soukari, Vio80, restitution sous la forme d'une auto-évaluation

Et si nous faisons notre bilan de cybervulnérabilité ? Il permet à chacun d'être actif dans son apprentissage de la cybersécurité !

Les questions à se poser sont les suivantes :

### 1- Vos appareils sont-ils bien à jour ?

- a. Oui, et c'est important car les mises à jour permettent notamment de renforcer la sécurité\*\*
- b. Non, car qui dit nouvelles versions dit nouvelles failles et nouvelles arnaques

### 2- Vos mots de passe sont :

- a. Longs (>12 caractères) ? O\*/N
- b. Un mix de caractères : majuscules/minuscules, chiffres, lettres, caractères spéciaux ? O\*/N
- c. Compréhensibles (il s'agit d'un mot existant) ? O/N\*
- d. En lien logique avec vous (le nom d'un proche, une date, ...) O/N\*
- e. Vous les avez déjà donnés à quelqu'un sans les changer ? O/N\*
- f. Vous les changez : tous les 3 mois\*, tous les ans\*, tous les 2 ans, moins fréquemment ?
- g. Parmi vos applications, pour celles qui ont nécessairement vos coordonnées bancaires (ex. Uber, Deliveroo), avez-vous un mot de passe renforcé ? O\*/N

### 3- Vous séparez sur vos appareils le pro du perso (« cyberhygiène ») ? O\*\*/N

### 4- Avez-vous et utilisez-vous un antivirus ? O\*\*/N

### 5- Répondez-vous par téléphone ou mail à des contacts inconnus ? O/N\*\*

### 6- Vous connectez-vous parfois à des réseaux wifi publics ou inconnus ? O/N\*\*

### 7- Êtes-vous en liste rouge ou noire ? O\*\*/N

### 8- Faites-vous des sauvegardes régulières ? O\*\*/N

### 9- Téléchargez-vous des applications sur des sites autres que ceux qui sont officiels et connus (AppStore, PlayStore, etc) ? O/N\*\*

### 10- Vérifiez-vous la sécurité des sites sur lesquels vous faites des achats ? O\*\*/N

### 11- Connaissez-vous les risques et les arnaques possibles ? O\*/N

### 12- Êtes-vous plutôt :

- a. de nature optimiste et à faire confiance en vous disant que l'assurance de votre carte bancaire par exemple pourrait vous couvrir ou que le risque est minime
- b. ou de nature craintive quitte à ne pas obtenir ce que vous souhaitez par peur de l'arnaque ?\*\*

### 13- Laisseriez-vous votre téléphone à charger sur un chargeur de quelqu'un d'autre (dans un bar, ou un lieu public à la gare par exemple) ?

- a. Oui il ne peut rien se passer par un chargeur
- b. Non, des informations peuvent transiter par certains chargeurs \*\*

Comptabilisez les étoiles des réponses que vous avez choisies et cela vous donnera votre score de cybervulnérabilité sur 30. Plus le score est petit, plus vous êtes vulnérable.

**Voici pour compléter cette webographie indicative :**

**Orange Cybersécurité :**

[Cybersécurité : Protégez votre vie numérique avec Orange](#) : présentation complète de l'offre de cybersécurité d'Orange. Vous pouvez tester des URL si jamais vous avez un doute, pensez-y !

**Sur la communauté d'entraide :**

- [Votre mot de passe et sa sécurité - Communauté Orange](#) : sur les mots de passe
- [Sécuriser l'accès aux sites où l'on a un compte. - Communauté Orange](#) : sur la sécurisation de l'accès aux sites sur lesquels on a un compte
- [Limiter les risques sur internet : nos conseils \(orange.fr\)](#) : limiter les risques sur le web
- [Orange - Communauté Orange - Livebox - Mobile - Smartphones - Abonnements - Réponses à vos questions](#) : autres sources d'infos, le blog
- [Internet et la cyber sécurité \(orange.fr\)](#) : internet et la cybersécurité

**Sur Bien vivre le digital :**

- <https://bienvivreledigital.orange.fr/securite/protection-des-donnees/cybersecurite-tous-concernes-voici-pourquoi.html> : pourquoi c'est important, quelques bons gestes à adopter
- <https://bienvivreledigital.orange.fr/securite/protection-des-donnees/cybersecurite-les-10-gestes-numeriques-essentiels-a-adopter.html> : vous trouverez des explications sur les items abordés ci-dessus.
- <https://bienvivreledigital.orange.fr/securite/protection-des-donnees/doxing-comment-protoger-votre-identite-en-ligne.html> : sur le volet publications d'informations personnelles en particulier pour la partie prévention

**Sur Dream Café :**

- Orange DreamCafé | Des conversations de café sur la cybersécurité
- [Orange DreamCafé | Le sentiment d'insécurité sur internet](#)

**Sur d'autres sites :**

- <https://www.quechoisir.org/actualite-arnaque-mefiez-vous-des-qr-codes-n113198/> : sur le quishing ou arnaque au faux qr code
- [https://fr.wikipedia.org/wiki/Juice\\_jacking](https://fr.wikipedia.org/wiki/Juice_jacking) : « certains lieux publics, gares ou aéroports, certains lieux comme les centre commerciaux, proposent des bornes de recharges USB pour les mobiles, sauf que des pirates peuvent "cacher" des PC derrière ces bornes et dès qu'on branche son appareil, on donne un accès direct à l'appareil au pirate, parce que les câbles USB contiennent les fils d'alimentation et les fils de données »
- <https://passwordsgenerator.net/> : générateur de mot de passe fort pour lequel on peut préciser ses paramètres désirés
- [Tester les ports ouverts : avec un outil de contrôle des ports - IONOS](#) : pour tester la visibilité de son IP et la vulnérabilité des ports de la box familiale avec des services de scan en ligne ; une bonne partie

des intrusions / infection est réalisée par des bots qui scannent systématiquement toutes les adresses ip disponibles. D'où l'intérêt de vérifier que l'on n'est pas visibles d'eux en vérifiant que tous les ports de sa box sont bien fermés ou abrités derrière un pare-feu.