



ayming

Cybersécurité

Notre exemple pour  
tester vos salariés

# 1- Testez vos collaborateurs avec des quiz de différents niveaux

## ○ Quiz Découverte - Exemple de question

**Vous recevez un message ou un appel d'une organisation connue et d'apparence officielle qui vous demande des informations personnelles ?**

- Je communique les informations demandées si je connais la société qui me le demande
- Je ne communique aucune information
- J'informe la hotline avant de répondre

## ○ Quiz Maîtrise - Exemple de question

**Comment se prémunir de l'hameçonnage ?**

- Si j'ai un doute concernant un mail, je transfère le mail à l'expéditeur pour en confirmer l'authenticité
- Je vérifie qu'il y ait bien un logo officiel dans le message reçu
- Avant de cliquer sur un lien douteux, je positionne le curseur de ma souris sur le lien sans cliquer pour vérifier l'adresse vers laquelle il pointe
- Je ne communique jamais d'informations sensibles (mot de passe ou code secret) par téléphone ou messagerie électronique

Plusieurs bonnes réponses possibles

## ○ Quiz Expertise - Exemple de question

**En cas d'incident de sécurité avec violations de données à caractère personnel, qu'est-ce que le DPO d'Ayving doit faire ?**

- Analyser la situation afin de déterminer si la CNIL et/ou le client doivent être notifiés dans les meilleurs délais et si possible dans les 72h de la connaissance de la violation
- Noter cet incident et faire un récapitulatif annuel de tous les incidents à la direction d'Ayving
- Faire un Easyvista à la DAFM (Direction des Achats & Facility Management) pour les informer de l'incident





ayming

2020



# Certificate of achievement

---

Carole PODYMSKI

---

- Followed the SSI program

Date : 06/05/2020

Signature RSSI : 

### 3- Pour aller plus loin sur ce sujet

---

« *Pour toujours* plus de transparence et afin de mesurer l'efficacité des actions de sensibilisation réalisées au sein d'Ayming, nous réalisons **un test bi-annuel** de phishing. Le but est de reproduire une attaque de phishing classique par l'envoi d'un faux mail identique à ceux que nous recevons très régulièrement. L'objectif d'un mail de phishing **est de récupérer les identifiants de la personne afin de se connecter à nos systèmes** pour récupérer des informations personnelles et/ou confidentielles, de voler de la donnée professionnelle voire de contaminer notre ordinateur. »

*Pour prévenir les cyberattaques, Ayming :*

- *Mène des actions de sensibilisation,*
- *Réalise des tests et analyse leurs résultats afin d'identifier les nouveaux risques potentiels,*
- *Rappelle les bonnes pratiques que chaque collaborateur doit mettre en œuvre*
- *A mandaté une équipe de 3 acteurs clefs (le RSSI, le responsable/chef de projet ISO 27001 et le DPO) afin de veiller à la bonne application de la sécurité et d'accompagner ses salariés dans l'acquisition des bons réflexes de sécurité et ce dans une optique d'assurer une sécurité toujours optimale des données de ses clients.*

