apave

parole client

FORMATION CYBERSÉCURITÉ (E-LEARNING)

acta digital services

1 POURQUOI AVEZ-VOUS ENGAGÉ CETTE DÉMARCHE DE FORMATION ?

Acta Digital Services est un prestataire de service informatique de 16 collaborateurs (ESN : Entreprise de Services du Numériques) dédié au domaine agricole. En parallèle de notre activité principale, nous souhaitons sensibiliser nos clients au risque cyber. En effet, on observe une multiplication des cyberattaques en France et partout dans le monde. Toutes les typologies d'organisations sont concernées, les instituts agricoles - nos clients principaux - également !

2 POURQUOI AVEZ-VOUS CHOISI L'E-LEARNING APAVE ?

Nous avons contacté et testé différents prestataires afin d'être certain de notre choix final. La formation en e-Learning proposée par le groupe Apave a retenu notre attention pour différentes raisons :

- Le coeur de la formation est orientée sur la sensibilisation et le partage des bonnes pratiques à adopter quotidiennement, ce qui correspondait parfaitement à nos intentions.
- Le format court de 30 minutes, qui s'intègre parfaitement aux emplois du temps.
- Le format ludique avec des exemples concrets expliqués tout au long de la formation.
- La fiche des bonnes pratiques récapitulatives à télécharger en fin de formation, qui permet de synthétiser les acquis.

3 QUELS SONT LES BÉNÉFICES APPORTÉS POUR VOUS & VOTRE CLIENT ?

Nous avons réalisé cette première formation pour le compte de l'un de nos clients, dans le domaine de la recherche agronomique 48 personnes ont été formées sur toutes typologies de fonctions : tant administratives que chefs de projets.
Nous sommes globalement satisfaits des résultats : la formation est pertinente et permet à chacun de découvrir (ou redécouvrir) les bonnes pratiques cyber à adopter quotidiennement dans le cadre de sa mission professionnelle. Chacun assure ses missions de façon sereine (et nos clients aussi) !
Nous aimerions désormais poursuivre cette démarche avec la mise en oeuvre de campagnes de phishing pour tester les réactions des collaborateurs dans un contexte réel de cyberattaque !