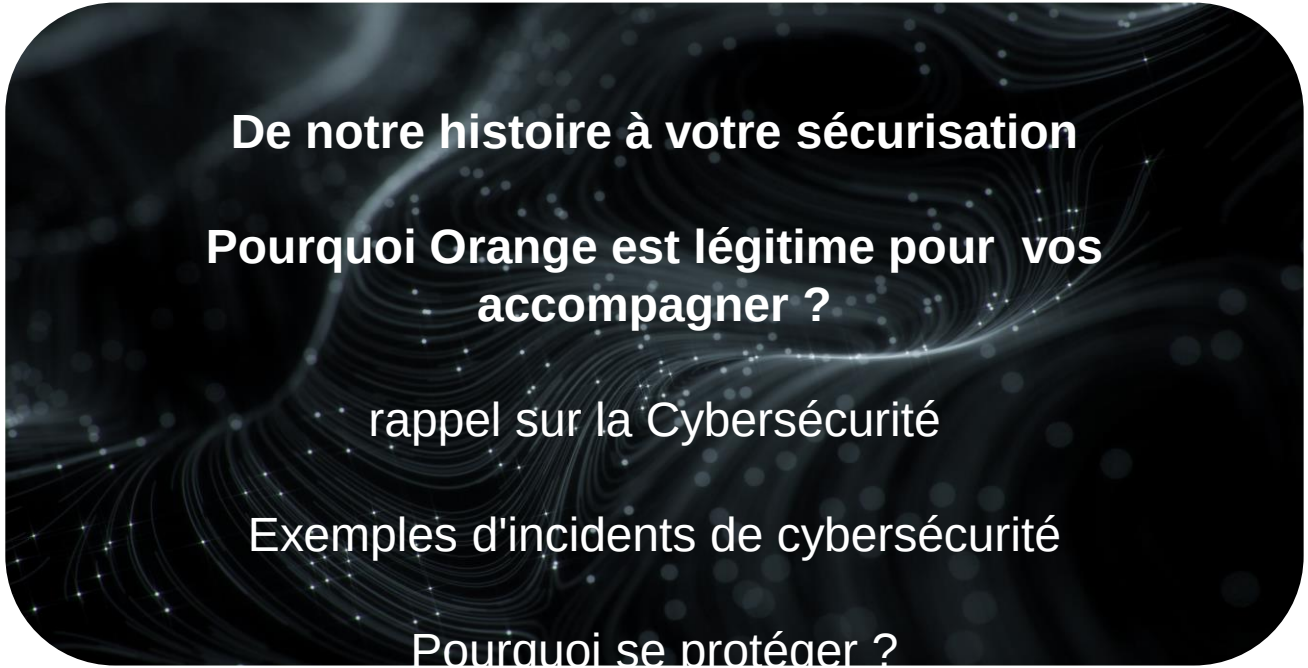
Cybersécurité

Pourquoi Orange est légitime pour accompagner les entreprises sur le domaine cybersécurité ?



Luc BESTORY
Directeur DSPI

De notre histoire à votre sécurisation ?

Orange est légitime pour soutenir les entreprises dans ce domaine en raison de son expérience.

L'histoire des réseaux d'Orange est marquée par plusieurs étapes clés :

- **Début des années 1980** : France Télécom, l'ancêtre d'Orange, commence à développer des réseaux de télécommunications en France, avec un accent sur la téléphonie fixe.
- **Lancement de la téléphonie mobile (1987)**
- **Création d'Orange (1994)**
- **Acquisition et intégration (2000)**
- **Développement de la 3G et 4G (2000s)** : Orange investit massivement dans le déploiement de réseaux 3G et 4G, améliorant la connectivité mobile et les services de données.
- **Transition vers la fibre optique (2010s)** : L'entreprise se concentre sur le déploiement de la fibre optique pour offrir des services internet haut débit.
- **5G et innovations récentes** : Orange a lancé des réseaux 5G dans plusieurs pays

Aujourd'hui, Orange est un acteur majeur dans le domaine des réseaux, offrant des services variés allant de la téléphonie mobile à l'internet fixe, tout en continuant d'innover dans le secteur des télécommunications.

Pourquoi Orange est légitime pour vos accompagner ?

Orange est légitime pour accompagner les entreprises dans le domaine de la cybersécurité pour plusieurs raisons

Notre Histoire

Expertise reconnue

Orange dispose d'une vaste expérience dans le secteur des télécommunications et de la cybersécurité, avec des équipes spécialisées.

Solutions variées

L'entreprise propose une gamme complète de services, allant de la prévention à la réponse aux incidents.

Infrastructure robuste

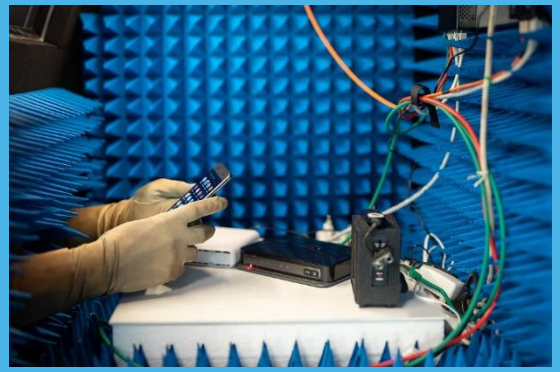
Orange bénéficie d'une infrastructure technologique avancée, essentielle pour assurer la sécurité des données.

Partenariats stratégiques

L'entreprise collabore avec des acteurs clés du secteur pour renforcer ses offres de cybersécurité.

Engagement envers l'innovation

Orange investit continuellement dans la recherche et le développement pour anticiper les nouvelles menaces.
Ces éléments font d'Orange un partenaire de choix pour les entreprises souhaitant sécuriser leurs systèmes d'information.



Cybersécurité et mesures de protection

Cybersécurité

La cybersécurité concerne la protection des systèmes informatiques, des réseaux et des données contre les cyberattaques

Objectifs : Sensibiliser aux enjeux de la cybersécurité et présenter des mesures de protection.

Croissance des menaces : Augmentation des cyberattaques (phishing, ransomware, etc.).

Importance : Protection des données personnelles et des infrastructures critiques.

Types de Menaces

- **Malware** : Logiciels malveillants qui compromettent les systèmes.
- **Phishing** : Techniques de fraude pour obtenir des informations sensibles.
- **Attaques DDoS** : Surcharge des serveurs pour les rendre inaccessibles.

Mesures de Protection

- Mises à jour régulières : Maintenir les logiciels à jour pour corriger les vulnérabilités.
- Utilisation de mots de passe forts : Combinaisons complexes et uniques pour chaque compte.
- Formation des utilisateurs : Sensibilisation aux bonnes pratiques de sécurité.

Règlementations et Normes

- **RGPD :** Règlement sur la protection des données en Europe.
- **ISO/IEC 27001 :** Norme pour la gestion de la sécurité de l'information.

Conclusion

Résumé : La cybersécurité est essentielle pour protéger les informations et les systèmes.

Perspectives : Évolution des technologies et des menaces, nécessité d'une vigilance continue.

quelques chiffres clés

concernant l'état de la menace cyber

Attaques DDoS : En 2023, le nombre d'attaques DDoS a augmenté de 15 % par rapport à l'année précédente.
Coût des cyberattaques : Le coût global des cyberattaques pour les entreprises pourrait atteindre 10,5 trillions de dollars d'ici 2025.
Exposition aux ransomwares : Environ 70 % des entreprises ont été ciblées par des ransomwares en 2023.
Impact sur les PME : 60 % des petites et moyennes entreprises (PME) ont fermé dans les six mois suivant une cyberattaque.
Vulnérabilités zero-day : En 2023, le nombre de vulnérabilités zero-day signalées a atteint un niveau record, avec plus de 100 cas.

Ces chiffres illustrent l'ampleur croissante des menaces cybernétiques et l'importance de la cybersécurité. Pour des données spécifiques à 2024, il est conseillé de consulter des rapports récents.

quelques tendances anticipées basées sur les évolutions précédentes :

Augmentation des attaques : On s'attend à ce que les attaques par ransomware continuent d'augmenter, avec des prévisions de hausse de 20-30 %.
Phishing : Les tentatives de phishing pourraient représenter jusqu'à 40 % de tous les e-mails envoyés.
Coût des violations : Le coût moyen d'une violation de données pourrait dépasser 5 millions de dollars.
Vulnérabilités : Le nombre de vulnérabilités signalées pourrait atteindre 25 000 ou plus.

Exemples d'incidents de cybersécurité survenus dans des collectivités

Ransomware sur des systèmes municipaux

En 2019, la ville de Baltimore a été victime d'une attaque par ransomware, paralysant plusieurs services municipaux et entraînant des coûts de récupération élevée. La cyberattaque de Baltimore a coûté plus de 18 millions de dollars à la ville - Le Parisien

Fuite de données personnelles

En 2020, une municipalité en France a subi une fuite de données sensibles, exposant les informations personnelles de milliers de citoyens.

Attaque sur les infrastructures critiques

En 2021, une attaque ciblant les systèmes de contrôle d'une station d'épuration a mis en danger la sécurité de l'eau potable dans une collectivité.

Phishing ciblé

Plusieurs collectivités ont été victimes de campagnes de phishing, entraînant des pertes financières et des compromissions de comptes.

Défaillance des systèmes de gestion

Une attaque a perturbé les systèmes de gestion des déchets d'une ville, entraînant des retards dans les services de collecte.

Autres incidents survenus

La mairie de Val-de-Reuil annonce ce jeudi 5 septembre 2024 de nombreuses lignes téléphoniques et internet de ses services sont suspendues pour 24 à 48h.

France Travail a été victime d'une cyberattaque ayant conduit à une fuite de données susceptible de toucher 43 millions de personnes. La CNIL accompagne l'organisme afin d'assurer la bonne information des personnes concernées et rappelle quelques conseils pour leur permettre de se protéger 08/03/2024

Les données personnelles d'habitants de Betton divulguées sur internet après une cyberattaque 31/08/2023

Cyberattaque au CHU de Nantes : « un ou deux jours pour revenir à la normale », estime la direction (ouest-france.fr)

L'université visée par une cyberattaque, un exemple de la "piraterie" moderne - Mo News - Hebdomadaire d'informations de la Guyane (monewsguyane.com)

Cyberattaque : le système informatique de la CTM s'est fait pirater (franceantilles.fr)

L'ANSSI a traité 187 incidents cyber affectant les collectivités territoriales, de janvier 2022 à juin 2023, soit une moyenne de 10 incidents par mois. Or, la majorité des incidents (126) concernent des communes et/ou des EPCI à fiscalité propre.

Pourquoi se protéger ?

- Protection des données sensibles
- **Continuité des services** : une cyberattaque peut perturber les services essentiels.
- **Confiance du public** : la sécurité renforce la confiance des clients.
- **Conformité légale** : respect des réglementations sur la protection des données

Nos solutions

Cybersecure cela inclut :

- protection des données - détection des menaces - consultation et audits - formation
- L'objectif est d'aider les entreprises à renforcer leur sécurité numérique et à se protéger contre les cybermenaces.

Cyberprotection ensemble des services et solutions offerts par Orange pour sécuriser les systèmes d'information et les données cela comprend :

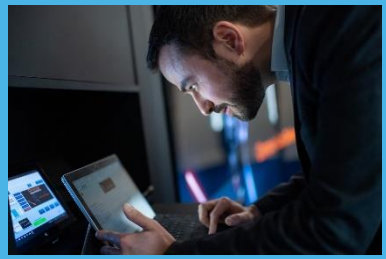
- solutions de sécurité - surveillance et détection - consultation et accompagnement - formation et sensibilisation

L'objectif est de garantir la sécurité des données et de minimiser les risques liés aux cyberattaques.

Microsoc fait référence à une offre de services de cybersécurité destinée aux petites et moyennes entreprises (PME). Cette solution vise à :

- protéger les données - simplifier la gestion de la sécurité - assurer la conformité - fournir un support
- L'objectif est de rendre la cybersécurité accessible et efficace pour les entreprises de taille modeste

Quelques conseils



- gérer vos habilitations
- sensibiliser et former vos collaborateurs
- faire de la détection au niveau des infrastructures : flux normal / flux anormal
- chiffrer vos échanges : confidentialité RGPD
- auditer (techniques et organisationnels)

✓ Évitez les achats impulsifs, adoptez une stratégie claire et évitez d'accumuler les solutions.

✓ **Faites-vous accompagner** par des entreprises fiables.

Que faire en cas de phishing ou hameçonnage ?

- Que faire en cas de phishing ou hameçonnage ? - Assistance aux victimes de cybermalveillance
- Dix règles pour vous prémunir contre le piratage de vos données personnelles | economie.gouv.fr
- Piratage d'un compte d'utilisateur (réseaux sociaux, messagerie électronique...) | Service-Public.fr

Merci