Conseils de Cybersécurité

Nom de l'entreprise: Origine Sounds Records

Question 1: Combien d'ordinateurs et de périphériques connectés utilisez-vous dans votre entreprise ?

Réponse: 0-10

Conseil: Vous pouvez sécuriser vos 10 dispositifs en suivant ces conseils :

1. Mettez à jour régulièrement vos logiciels pour combler les failles de sécurité potentielles.
2. Utilisez des mots de passe forts et différents pour chaque appareil pour renforcer la sécurité.
3. Installez et maintenez un logiciel antivirus sur chaque appareil pour détecter et bloquer les menaces.

Question 2: Vos données sont-elles stockées localement sur des serveurs ou dans le cloud ?

Réponse: cloud

Conseil: 1. Assurez-vous d'utiliser des identifiants forts et de mettre en place l'authentification à deux facteurs.
2. Chiffrez vos données sensibles avant de les stocker sur le cloud pour une meilleure protection.
3. Gardez vos logiciels et systèmes à jour pour éviter les failles de sécurité potentielles.

Question 3: Comment les données sont-elles partagées au sein de votre entreprise?

Réponse: externe

Conseils de Cybersécurité

Conseil: Pour sécuriser le partage de données via un réseau externe, voici deux conseils :

1. Utilisez un protocole de chiffrement fort tel que SSL/TLS pour crypter les données transitant sur le réseau.
2. Mettez en place des mesures d'authentification à double facteur pour renforcer l'accès aux données partagées.

Question 4: Quels types de logiciels utilisez-vous pour la gestion de votre entreprise?

Réponse: ['cms', 'comptabilité', 'Trello']

Conseil: Pour le logiciel CMS : 1. Assurez-vous de toujours installer les mises à jour de sécurité. 2. Limitez les accès administratifs.

Pour le logiciel de comptabilité : 1. Envisagez d'utiliser une authentification à deux facteurs. 2. Effectuez des sauvegardes régulières.

Pour Trello : 1. Limitez les membres autorisés à accéder aux tableaux sensibles. 2. Utilisez des paramètres de confidentialité adéquats pour chaque tableau.

Question 5: Offrez-vous des formations et/ou des séances de sensibilisations à la cybersécurité à vos employés ? Si oui, à quelle fréquence ?

Réponse: non

Conseil: Il est crucial de former vos employés en cybersécurité pour protéger vos données sensibles.

Conseils de Cybersécurité

Conseil : Priorisez la formation en cybersécurité dès que possible.

Question 6: Quels sont les réseaux sociaux que vous utilisez dans un cadre professionnel ?

Réponse: ['facebook', 'twitter', 'instagram', '']

Conseil: Sur chacun de ces réseaux sociaux, vous pourriez être confronté à différents risques liés à la cybersécurité. Voici quelques exemples :

1. Facebook : Sur Facebook, vous pourriez être victime d'attaques de phishing où des cybercriminels tentent de vous tromper en utilisant de faux messages ou liens pour voler vos identifiants de connexion. Vous pourriez également être exposé à des arnaques ou à des faux concours visant à collecter vos données personnelles.

2. Twitter : Sur Twitter, il y a un risque de propagation de fausses informations et de manipulation de l'opinion publique. Vous pourriez également être confronté à des comptes ou à des publications malveillantes visant à vous induire en erreur ou à vous inciter à partager des informations sensibles.

3. Instagram : Sur Instagram, le risque principal est lié à la vie privée et à la sécurité des données. En partageant des photos ou des vidéos, vous pourriez involontairement divulguer des informations personnelles ou sensibles. De plus, des comptes frauduleux pourraient tenter de vous suivre ou de vous contacter pour des desseins malveillants.

Il est important de rester vigilant sur ces plateformes et de prendre des mesures pour protéger vos comptes et vos données. En outre, je tiens à vous sensibiliser sur le social engineering, une

technique utilisée par les cybercriminels pour manipuler les individus et leur faire divulguer des informations confidentielles. Par exemple, sur Twitter, un attaquant peut se faire passer pour une personne de confiance (comme un membre de votre famille ou un collègue) pour vous inciter à partager des informations personnelles ou à cliquer sur des liens malveillants. Soyez donc prudent et ne divulguez jamais d'informations sensibles à des inconnus, même si ils semblent être légitimes.

Question 7: Quels outils de sécurité utilisez-vous ?

Réponse: ['sauvegarde', 'aucun']

Conseil: Je vous recommande d'utiliser en priorité un antivirus, un pare-feu et un gestionnaire de mots de passe.

Ces outils sont essentiels pour protéger vos données et votre système contre les attaques de logiciels malveillants, les intrusions non autorisées et les violations de données. Un antivirus aide à détecter et à supprimer les menaces pour la sécurité, un pare-feu permet de contrôler le trafic réseau et de bloquer les accès non autorisés, tandis qu'un gestionnaire de mots de passe assure la sécurité de vos identifiants en les stockant de manière sécurisée.

Question 8: Comment votre réseau wifi est-il accessible ?

Réponse: un mot de passe moyen (Entreprise12)

Conseil: Non, un mot de passe moyen comme "Entreprise12" n'est pas suffisamment sécurisé. Je vous recommande d'utiliser une passphrase, une phrase composée de plusieurs mots aléatoires pour renforcer la sécurité. Par exemple, "SoleilChatMaison72".

Conseils de Cybersécurité

Risques d'un réseau wifi mal sécurisé : accès non autorisé, interceptions de données, attaques de type "homme du milieu".

Question 9: Quelles sont les actions que vous avez entrepris après une cyberattaque ? (Dans le cas où vous n?avez pas subi de cyber attaque, veuillez répondre comme si cela l?était)

Réponse: ['vérification des logs', ' isoler les sauvegarde', ' conservation des preuves via screenshot']
Conseil: Pour être plus efficace lors d'une cyberattaque, vous pourriez également envisager de notifier les autorités compétentes, de mettre en place une communication interne claire à ce sujet, de contacter un expert en cybersécurité pour vous aider dans la remédiation, et de planifier une communication externe si nécessaire.

Un plan d'urgence en cas de cyberattaque est crucial pour réagir rapidement et efficacement face à une situation critique, limiter les dommages potentiels, sécuriser les données sensibles, préserver la réputation de l'entreprise et assurer une reprise d'activité plus rapide.

Question 10: Quel est votre domaine d?activité ?

Réponse: Studio d'enregistrement de musique
Conseil: Voici trois exemples d'attaques qui ont visé des entreprises similaires à la vôtre :

1. Phishing : Des employés ont reçu des e-mails frauduleux prétendant être de partenaires pour obtenir des informations sensibles.
2. Ransomware : Un logiciel malveillant a chiffré tous les fichiers de l'entreprise, exigeant une

rançon en échange de la clé de déchiffrement.

3. Ingénierie sociale : Des personnes se faisant passer pour des techniciens ont réussi à infiltrer le studio et voler du matériel important.

Résumé global des conseils

Voici un résumé des conseils de cybersécurité pour Origine Sounds Records :

- Pour sécuriser jusqu'à 10 dispositifs :
  - Mettre à jour régulièrement les logiciels.
  - Utiliser des mots de passe forts et différents pour chaque appareil.
  - Installer et maintenir un logiciel antivirus sur chaque appareil.

- Stockage de données dans le cloud :
  - Utiliser des identifiants forts et l'authentification à deux facteurs.
  - Chiffrer les données sensibles avant de les stocker.
  - Garder les logiciels et systèmes à jour.

- Partage de données externes :
  - Utiliser un chiffrement fort comme SSL/TLS.
  - Mettre en place l'authentification à double facteur.

- Gestion des logiciels d'entreprise :
  - CMS : Installer les mises à jour de sécurité et limiter les accès administratifs.
    - Comptabilité : Envisager l'authentification à deux facteurs et effectuer des sauvegardes

Conseils de Cybersécurité

régulières.

  - Trello : Limiter les membres autorisés, utiliser des paramètres de confidentialité adéquats.

- Formation en cybersécurité pour les employés.

- Utilisation des réseaux sociaux professionnels :

  - Facebook : Risque de phishing et d'arnaques.

  - Twitter : Risque de propagation de fausses informations.

  - Instagram : Risques liés à la vie privée et à la sécurité des données.

- Outils de sécurité recommandés : antivirus, pare-feu, gestionnaire de mots de passe.

- Sécurisation du réseau wifi avec une passphrase forte.

- Actions à entreprendre après une cyberattaque : vérification des logs, isolation des sauvegardes, conservation des preuves, notification des autorités, communication interne, contact d'un expert en cybersécurité, plan de communication externe.

- Conseils spécifiques pour un studio d'enregistrement de musique concernant les attaques potentielles (phishing, ransomware, ingénierie sociale).