Conseils de Cybersécurité

Nom de l'entreprise: Chez Marie Chou

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

Réponse: 0-10

Conseil: Vous pouvez sécuriser vos 0-10 ordinateurs et périphériques en suivant ces conseils :

1. Mettez à jour régulièrement vos logiciels et systèmes d'exploitation pour combler les failles de sécurité.

2. Utilisez des mots de passe forts et différents pour chaque appareil, et activez l'authentification à deux facteurs.

3. Installez un antivirus fiable et un pare-feu sur chaque appareil pour protéger contre les logiciels malveillants.

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

Réponse: localement

Conseil: 1. Chiffrez les données sensibles.

2. Mettez en place des pare-feux et des antivirus.

3. Effectuez des sauvegardes régulières.

4. Restreignez l'accès aux données importantes.

5. Mettez à jour régulièrement vos systèmes et logiciels.

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

Conseils de Cybersécurité

Réponse: externe

Conseil: Pour sécuriser le partage de données via un réseau externe, je vous conseille :

1. Utilisez un protocole de chiffrement robuste pour crypter les données échangées, comme le SSL ou le TLS.
2. Mettez en place des protections d'accès comme des mots de passe forts et l'authentification à plusieurs facteurs.

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

Réponse: ['aucun', '']

Conseil: Pour maintenir des logiciels sécurisés, voici quelques conseils :

1. Mettez à jour régulièrement les logiciels pour combler les failles de sécurité.
2. Utilisez des solutions de chiffrement pour protéger les données sensibles de l'entreprise.

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 d'investir dans la formation en cybersécurité pour réduire les risques de cyberattaques.

Conseil : Offrez des formations régulières en cybersécurité à vos employés dès que possible.

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

Conseils de Cybersécurité

professionnel ?

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

Conseil: Sur chaque réseau social, vous pouvez rencontrer différents risques liés à la cybersécurité, notamment en termes de confidentialité des données, d'usurpation d'identité, d'hameçonnage (phishing) et de social engineering.

Sur LinkedIn :

- Risque de collecte d'informations professionnelles sensibles pouvant être utilisées pour des attaques ciblées ou du spear phishing.
- Risque d'usurpation d'identité professionnelle afin d'envoyer des demandes de connexion frauduleuses à des collègues ou des partenaires.

Sur Facebook :

- Risque de fuite de données personnelles en raison des paramètres de confidentialité parfois mal configurés.
- Risque de phishing à travers des liens malveillants partagés sur la plateforme.
- Risque de manipulation psychologique par le biais de fausses informations ou de publicités ciblées.

Sur Instagram :

- Risque de divulgation de données personnelles et de localisation à travers des posts géolocalisés.
- Risque d'arnaque ou de fraude à travers des faux concours ou des offres trompeuses.
- Risque de manipulation des utilisateurs par des influenceurs malveillants ou des campagnes de désinformation.

Conseils de Cybersécurité

En ce qui concerne le social engineering, il s'agit d'une technique utilisée par les cybercriminels pour manipuler les individus et leur faire divulguer des informations confidentielles. Par exemple, un attaquant pourrait se faire passer pour un recruteur sur LinkedIn afin de demander des informations sensibles à un employé d'une entreprise. Sur Facebook, un attaquant pourrait créer un faux profil pour se faire passer pour un ami de la victime et obtenir des informations personnelles. Sur Instagram, un attaquant pourrait envoyer des messages trompeurs pour inciter la victime à cliquer sur des liens malveillants.

Il est essentiel de rester vigilant et de ne pas divulguer d'informations sensibles sur les réseaux sociaux. Assurez-vous également que vos paramètres de confidentialité sont correctement configurés et évitez de cliquer sur des liens suspects, même s'ils proviennent de personnes que vous connaissez en ligne.

Question 7: Quels outils de sécurité utilisez-vous ?

Réponse: ['antivirus', 'vpn']

Conseil: Je vous recommande de considérer en priorité le pare-feu, gestionnaire de mot de passe et système de sauvegarde.

Le pare-feu est essentiel pour filtrer le trafic réseau et bloquer les menaces. Le gestionnaire de mots de passe permet de sécuriser l'accès aux comptes. Le système de sauvegarde garantit la récupération des données en cas d'incident.

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

Conseils de Cybersécurité

Réponse: un mot de passe moyen (Entreprise12)

Conseil: Non, un mot de passe moyen comme "Entreprise12" n'est pas suffisamment sécurisé. Je recommande l'utilisation d'une passphrase, comme "La_Sécurité_de_Notre_Réseau_est_Importante!". Les risques d'un réseau wifi mal sécurisé incluent l'accès non autorisé aux données et la compromission des appareils connectés.

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', ' contact préstataire informatique', ' conservation des preuves via screenshot']

Conseil: Pour être plus efficace après une cyberattaque, vous pourriez ajouter les actions suivantes : contacter les autorités compétentes, isoler les systèmes infectés du réseau, informer les employés sur la situation et les mesures à prendre, et mettre en place un plan de communication pour gérer la crise.

Un plan d'urgence en cas de cyberattaque est essentiel pour réagir rapidement et efficacement face à une intrusion, minimiser les dommages, protéger les données sensibles, et limiter l'impact sur l'activité de l'entreprise.

Question 10: Quel est votre domaine d?activité ?

Réponse: Restauration

Conseil: 1. Phishing : Des attaquants envoient des e-mails frauduleux se faisant passer pour des

fournisseurs pour voler des informations sensibles.

2. Ransomware : Des logiciels malveillants bloquent l'accès aux données de l'entreprise et demandent une rançon pour les débloquer.

3. Intrusion dans le point de vente : Des attaquants compromettent les systèmes de paiement pour voler les informations de carte de crédit des clients.

Résumé global des conseils

Conseils pour Chez Marie Chou en matière de cybersécurité :

- Pour sécuriser 0-10 ordinateurs et périphériques :
  - Mettez à jour régulièrement vos logiciels et systèmes d'exploitation.
  - Utilisez des mots de passe forts et uniques pour chaque appareil, avec l'authentification à deux facteurs.
  - Installez un antivirus fiable et un pare-feu sur chaque appareil.

- Pour des données stockées localement :
  - Chiffrez les données sensibles.
  - Mettez en place des pare-feux et des antivirus.
  - Effectuez des sauvegardes régulières.
  - Restreignez l'accès aux données importantes.
  - Mettez à jour régulièrement vos systèmes et logiciels.

- Pour le partage de données externe :
  - Utilisez un protocole de chiffrement robuste comme SSL ou TLS.

Conseils de Cybersécurité

- Mettez en place des protections d'accès avec des mots de passe forts et l'authentification à plusieurs facteurs.

- Pour maintenir des logiciels sécurisés :
  - Mettez à jour régulièrement les logiciels.
  - Utilisez des solutions de chiffrement pour protéger les données sensibles.

- Pour la formation en cybersécurité :
  - Offrez des formations régulières en cybersécurité à vos employés.

- Pour l'utilisation des réseaux sociaux professionnels :
  - Soyez vigilant face aux risques liés à la confidentialité, l'usurpation d'identité, le hameçonnage et le social engineering.

- Pour les outils de sécurité utilisés :
  - Priorisez le pare-feu, le gestionnaire de mot de passe et le système de sauvegarde.

- Pour la sécurité du réseau wifi :
  - Utilisez une passphrase sécurisée au lieu d'un mot de passe simple.

- Après une cyberattaque :
  - Contactez les autorités compétentes.
  - Isolez les systèmes infectés du réseau.
  - Informez les employés et mettez en place un plan de communication.
  - Mettez en place un plan d'urgence pour réagir efficacement en cas d'intrusion.

Conseils de Cybersécurité

- Risques liés à l'activité de restauration :
  - Phishing.
  - Ransomware.
  - Intrusion dans le point de vente.