# TEST CYBER 2026

## Page 1

ID

Q2 Êtes vous  étudiants, indépendants  ou salariés  ?

☐ Étudiant / Indépendant (  20 minutes pour avoir son score rapidement )

☐ Salarié ( 30 minutes + questions RH )

# Page 2

Q3 Comment évaluez-vous votre niveau d'expertise en en sécurité informatique /cybersécurité ?

☐ 5 = Expert(e) en cybersécurité

☐ 4 = Utilisateur avancé

☐ 3 = Utilisateur régulier

☐ 2 = Utilisateur occasionnel

☐ 1 = Débutant(e) en cybersécurité

# Page 3

Q4 Comment évaluez-vous votre degré de curiosité intellectuelle lors de la recherche d'une problématique spécifique sur Google ?

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| ☐ | ☐ | ☐ | ☐ | ☐ |

Q5 Dans quelle mesure faites-vous preuve de créativité dans les domaines suivants de la cybersécurité ?

| | Pas du tout créatif 1 | 2 | 3 | 4 | 5 Très créatif |
|---|---|---|---|---|---|
| dans la création de nouvelles idées cyber | ☐ | ☐ | ☐ | ☐ | ☐ |
| dans la résolution de problème informatique cyber | ☐ | ☐ | ☐ | ☐ | ☐ |

# Page 4

Q6 L'attitude informatique c'est cultiver un certain état d'esprit, c'est avoir un certain comportement, c'est faire des choses qui nous animent et qui se retrouvent chez les personnes reconnues gérant leur sécurité informatique /cybersécurité au quotidien.
Vous retrouvez-vous dans ces différents comportements ?

| | Tout à fait moi | Moi | Indifférent | Peu moi | Pas du tout moi |
|---|---|---|---|---|---|
| Formaliser sa politique de sécurité informatique | ☐ | ☐ | ☐ | ☐ | ☐ |
| Lister le matériel de son parc informatique | ☐ | ☐ | ☐ | ☐ | ☐ |
| Calculer son budget informatique à l'année | ☐ | ☐ | ☐ | ☐ | ☐ |
| Sensibiliser les utilisateurs du parc informatique | ☐ | ☐ | ☐ | ☐ | ☐ |
| Mettre à jour ses connaissances liées à la sécurité | ☐ | ☐ | ☐ | ☐ | ☐ |
| Mettre à jour les systèmes d'exploitation (OS) sur tous les matériels (ordinateurs, tablettes, smartphones...) | ☐ | ☐ | ☐ | ☐ | ☐ |
| Mettre à jour les logiciels, navigateurs, plugins, Java, etc. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Changer régulièrement de mots de passe | ☐ | ☐ | ☐ | ☐ | ☐ |
| Faire des sauvegardes ordinateurs/ smartphones régulières | ☐ | ☐ | ☐ | ☐ | ☐ |
| Surveiller la présence éventuelle de ses données personnelles sur le darknet et autres plateformes | ☐ | ☐ | ☐ | ☐ | ☐ |
| Réaliser des audits de sécurité pour vérifier l'intégrité de son écosystème informatique | ☐ | ☐ | ☐ | ☐ | ☐ |
| Respecter les règles relatives aux réseaux sociaux | ☐ | ☐ | ☐ | ☐ | ☐ |
| Respecter les règles de mot de passe WIFI | ☐ | ☐ | ☐ | ☐ | ☐ |
| Respecter les règles de paiement en ligne | ☐ | ☐ | ☐ | ☐ | ☐ |

| | | | | | |
|---|---|---|---|---|---|
| Respecter les chartes Internet utilisateurs | ☐ | ☐ | ☐ | ☐ | ☐ |
| Faire attention en ouvrant les e-mails (phishing, virus) | ☐ | ☐ | ☐ | ☐ | ☐ |
| Utiliser un firewall et/ou un VPN | ☐ | ☐ | ☐ | ☐ | ☐ |
| Protéger vos données en déplacement (nomadisme) | ☐ | ☐ | ☐ | ☐ | ☐ |
| Protéger son identité numérique en ligne | ☐ | ☐ | ☐ | ☐ | ☐ |

Q7 Avez-vous réussi à établir aisément votre propre politique de sécurité domestique (plan d'actions défini pour maintenir un certain niveau de sécurité) en vous basant sur votre compréhension de la politique de sensibilisation de votre entreprise ?

| | 2 | 3 | 4 | 5 | 5 |
|---|---|---|---|---|---|
| Sur une échelle de 1 à 5 | ☐ | ☐ | ☐ | ☐ | ☐ |

# Page 5

Q8 Quelle est votre opinion sur les idées couramment répandues que nous allons énumérer ci-dessous ?

| | Tout à fait d'accord | Plutôt d'accord | Ni d'accord ni pas d'accord | Plutôt pas d'accord | Pas du tout d'accord | Ne sait pas |
|---|---|---|---|---|---|---|
| Naviguer uniquement sur des sites réputés écarte tout risque de sécurité. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| La navigation en 'https' assure une protection complète en ligne. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Il n'y a aucun danger tant que je m'abstiens de télécharger des fichiers. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Sans l'installation de nouvelles applications, mon appareil est hors de danger. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Les attaques DDoS (attaques par déni de service distribué) visent uniquement à interrompre les services, sans intentions malicieuses supplémentaires. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Les virus informatiques affectent exclusivement les systèmes d'exploitation Windows. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Le risque de sécurité survient uniquement lors de l'installation d'applications sur mon ordinateur. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Les données personnelles ne constituent pas une catégorie de données sensibles. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| L'adoption de protocoles Zero Trust offre une sécurité infaillible. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Seuls les acteurs étatiques sont à l'origine des attaques | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

detype APT (Advanced PersistentThreat).

Q9 **Selon vous, dans quelle mesure les attitudes suivantes peuvent-elles limiter l'efficacité d'une politique de sécurité informatique et de cybersécurité ?**

**Merci d'indiquer, pour chaque affirmation**, si cela représente pour vous un frein important, un frein modéré, ou pas de frein du tout.

| | Tout à fait d'accord | Plutôt d'accord | Ni d'accord ni pas d'accord | Plutôt pas d'accord | Pas du tout d'accord |
|---|---|---|---|---|---|
| Considérer la sécurité informatique, la cybersécurité comme non essentielle. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Percevoir les budgets informatiques comme un obstacle à la sécurité informatique. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Croire que les attaques ne concernent que les autres. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Manquer de temps pour se consacrer à la sécurité informatique /cybersécurité. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Trouver la sécurité informatique trop complexe et technique. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Ressentir une difficulté à mettre en pratique les recommandations de sécurité. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Prévoir de déléguer la sécurité informatique à un proche plutôt d'agir immédiatement. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Faire confiance en la protection totale offerte par un antivirus. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Voir dans l'interopérabilité des systèmes sécurisés une source d'inefficacité opérationnelle. | ☐ | ☐ | ☐ | ☐ | ☐ |
| L'évolution constante des menaces rend obsolètes les solutions mises en place en un temps record. | ☐ | ☐ | ☐ | ☐ | ☐ |

**En tant que particulier,** comment réagiriez-vous en cas d'escroquerie, de cyberattaque ou de phishing ?
Q10 Quels sont les bons renseignements à fournir et les bonnes actions à faire en premier lieu LORS D'ESCROQUERIES ?

| | Tout à fait d'accord | Plutôt d'accord | Ni d'accord ni pas d'accord | Plutôt pas d'accord | Pas du tout d'accord |
|---|---|---|---|---|---|
| Traçage des transactions financières suspectes. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Identification des contacts suspects. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Localisation des détails complets des cartes bancaires utilisées. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Utilisation de l'adresse IP pour identifier les fraudeurs. | ☐ | ☐ | ☐ | ☐ | ☐ |

**En tant que particulier,** comment réagiriez-vous en cas d'escroquerie, de cyberattaque ou de phishing ? Q11 Quels sont les bons renseignements à fournir et les bonnes actions à faire en premier lieu LORS DE CYBERATTAQUES ?

| | Tout à fait d'accord | Plutôt d'accord | Ni d'accord ni pas d'accord | Plutôt pas d'accord | Pas du tout d'accord |
|---|---|---|---|---|---|
| Tentative de localisation des cybercriminels. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Déconnexion immédiate d'internet en cas de menace. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Nettoyage du système avec des outils antivirus /antimalware. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Consultation d'un spécialiste si le système est compromis. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Se faire justice soi-même. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Paiement d'une rançon pour récupérer des données. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Changement systématique des mots de | ☐ | ☐ | ☐ | ☐ | ☐ |

passe après une attaque.

| | | | | | |
|---|---|---|---|---|---|
| Ne prévenir que la police dans un premier temps. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Déposer une plainte officielle auprès des autorités compétentes. | ☐ | ☐ | ☐ | ☐ | ☐ |

**En tant que particulier,** comment réagiriez-vous en cas d'escroquerie, de cyberattaque ou de phishing ?
Q12 Quels sont les bons renseignements à fournir et les bonnes actions à faire en premier lieu LORS DE PHISHING (vol de comptes, mots de passe, données bancaires...) ?

| | Tout à fait d'accord | Plutôt d'accord | Ni d'accord ni pas d'accord | Plutôt pas d'accord | Pas du tout d'accord |
|---|---|---|---|---|---|
| Méfiance face aux messages, appels ou SMS non sollicités. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Non-divulgation d'informations sensibles. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Vérification de la fiabilité des sites web visités. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Prudence avec les e-mails d'expéditeurs inconnus. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Faire confiance aux pièces jointes de vos proches et des sites marchands. | ☐ | ☐ | ☐ | ☐ | ☐ |

Q13 **Chez vous,** comment pourriez-vous développer au quotidien des mesures de prévention en matière de sécurité/cybersécurité ?

| | Toutà fait d'accord | Plutôtd'accord | Ni d'accord nipas d'accord | Plutôtpas d'accord | Pasdu toutd'accord |
|---|---|---|---|---|---|
| Anticiper les menaces en fonction de son utilisation d'internet. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Se former seul(e) ou en entreprise sur les meilleures pratiques de sécurité. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Lister les risques informatiques au niveau du foyer. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Mettre en place des | ☐ | ☐ | ☐ | ☐ | ☐ |

| | | | | | |
|---|---|---|---|---|---|
| mesures de protection robustes pour les ordinateurs, les smartphones et les tablettes. | | | | | |
| Identifier des mesures préventives, comme le VPN et les sauvegardes. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Élaborer une stratégie de sécurité adaptée au budget. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Mettre en place des solutions préventives, avec ou sans assistance. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Procéder à des évaluations régulières de votre politique de sécurité pour en vérifier l'efficacité sur le long terme. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Utiliser des solutions de chiffrage avancé pour les données sensibles stockées sur les appareils domestiques. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Utiliser des solutions avancées de protection de l'endpoint, allant au-delà des antivirus traditionnels. | ☐ | ☐ | ☐ | ☐ | ☐ |

Q14 Pour le BYOD (Bring Your Own Device : Pratique qui consiste à utiliser ses équipements personnels (téléphone, ordinateur portable, tablette électronique) dans un contexte professionnel, quelles sont les questions essentielles à poser pour assurer une mise en œuvre efficace et sécurisée ?

| | Tout à fait d'accord | Plutôt d'accord | Ni d'accord ni pas d'accord | Plutôt pas d'accord | Pas du tout d'accord |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| Vérification des bonnes pratiques et fourniture de guides de sécurité au format PDF. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Recommandation de logiciels de sécurité spécifiques et établissement d'une charte informatique. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Contrôle de l'accès et de la protection des données de l'entreprise sur les appareils personnels. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Implémentation d'une application de gestion du parc mobile (MDM - Mobile Device Management). | ☐ | ☐ | ☐ | ☐ | ☐ |
| Anticipation des procédures en cas de panne ou de perte de dispositif spécifique. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Conseils pour éduquer les enfants à une utilisation sécurisée d'Internet | ☐ | ☐ | ☐ | ☐ | ☐ |

Q15 **En tant que particulier,** êtes-vous sensible aux recommandations des sites internet de sécurité comme l'ANSSI (séparation des usages pro-perso) ?

| | Tout à fait d'accord | Plutôt d'accord | Ni d'accord ni pas d'accord | Plutôt pas d'accord | Pas du tout d'accord |
|---|---|---|---|---|---|
| Séparer clairement les mots de passe professionnels des mots de passe personnels. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Réunir messagerie professionnelle et personnelle. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Naviguer sur internet de manière responsable au travail. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Se servir des réseaux Wi-Fi publics occasionnellement pour le travail. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Éviter les solutions de chiffrement trop complexes. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Gérer prudemment sa présence sur les réseaux | ☐ | ☐ | ☐ | ☐ | ☐ |

sociaux.

Q16 Selon vous, **se former** à la sécurité informatique pour développer ses compétences, c'est :

| | Tout à fait d'accord | Plutôt d'accord | Ni d'accord ni pas d'accord | Plutôt pas d'accord | Pas du tout d'accord |
|---|---|---|---|---|---|
| Suivre les bonnes pratiques lors des déplacements. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Connaître de façon approfondie les menaces, risques et types d'attaques. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Connaître les différentes solutions à mettre en œuvre. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Établir une politique de sécurité robuste. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Prendre des mesures pour sécuriser son poste de travail. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Gérer les méthodes d'authentification. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Maitriser les bonnes pratiques pour les achats en ligne. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Réagir appropriément en cas d'alerte de sécurité. | ☐ | ☐ | ☐ | ☐ | ☐ |

Q17 **En entreprise**, comment percevez-vous les idées couramment admises énumérées ci-dessous ?

| | Tout à fait d'accord | Plutôt d'accord | Ni d'accord ni pas d'accord | Plutôt pas d'accord | Pas du tout d'accord | Ne sait pas |
|---|---|---|---|---|---|---|
| Les pertes de données proviennent principalement du matériel informatique. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| A ce jour, les techniques de phishing sont considérées comme obsolètes. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| L'espionnage via le cyberespace connaît une croissance significative. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Les attaques de type 'man-in-the-middle' sont restreintes aux réseaux locaux uniquement. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Payer la rançon demandée lors d'un ransomware garantit la restitution des données. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| La prise en charge du paiement de la rançon par les cyberassureurs dispense de se préparer à une attaque de ransomware. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Les backups sont la protection la plus fiable face aux logiciels de rançon. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| L'augmentation du télétravail entraîne une hausse des cyberattaques. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Les solutions EDR sont supérieures et peuvent remplacer tous les | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

| | | | | | | |
|---|---|---|---|---|---|---|
| autres antivirus existants. | | | | | | |
| Les protocoles BGP sont pleinement sécurisés et immunisés contre les risques de détournement et d'interception | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

Q18 **En entreprise**, pensez-vous que les attitudes suivantes constituent des freins à l'implémentation d'une politique efficace de sécurité informatique et de cybersécurité :

| | Tout à fait d'accord | Plutôt d'accord | Ni d'accord ni pas d'accord | Plutôt pas d'accord | Pas du tout d'accord |
|---|---|---|---|---|---|
| Lors des conséquences d'un sous-investissement face aux risques. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Lors des dangers de sous estimer les cyberattaques. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Lorsqu'on rencontre des obstacles à l'adoption des mesures de sécurité recommandées parmi les salariés. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Lorsqu'une diversité de solutions de sécurité peut mener à une cohérence opérationnelle fragmentée. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Lors de l'identification et la hiérarchisation des ressources. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Lors de l'évaluation des risques d'incidents de sécurité. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Lors de la compréhension du paysage de risque de l'entreprise. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Lors de la mise en oeuvre du télétravail sécurisé. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Lorsque la stratégie de sécurité n'est pas alignée avec les objectifs métier de l'entreprise. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Lorsqu'il y a des | ☐ | ☐ | ☐ | ☐ | ☐ |

| | |
|---|---|
| préoccupations sur la souveraineté des données et la dépendance envers les fournisseurs étrangers | |

Q19 **En entreprise**, quelles peuvent être les conséquences d'une cyberattaque ?

| | Tout à fait d'accord | Plutôt d'accord | Ni d'accord ni pas d'accord | Plutôt pas d'accord | Pas du tout d'accord |
|---|---|---|---|---|---|
| Risques liés à la perte de données sensibles. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Interruption prolongée des services. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Menaces liées aux ransomwares et autres formes de chantage. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Réduction des délais de livraison promis aux clients. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Dommages à la réputation de l'entreprise et création d'une image négative dans les médias. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Exposition à des sanctions pécuniaires imposées par les autorités régulatrices ou judiciaires. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Indisponibilité du site internet de l'entreprise pour ses clients. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Risques d'une paralysie totale des systèmes d'information. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Des coûts accrus liés à la remédiation et à l'investigation. | ☐ | ☐ | ☐ | ☐ | ☐ |
| L'obligation de notifier l'incident | ☐ | ☐ | ☐ | ☐ | ☐ |

Q20 Quelles seraient les meilleures stratégies pour développer quotidiennement la prévention en matière de sécurité et de cybersécurité **au sein d'une entreprise** ?

| | Tout à fait d'accord | Plutôt d'accord | Ni d'accord ni pas d'accord | Plutôt pas d'accord | Pas du tout d'accord | Ne sait pas |
|---|---|---|---|---|---|---|
| Parier sur une formation personnalisée pour les employés. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Se préparer à la création d'une équipe d'intervention d'urgence. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Vérifier l'existence d'un Plan de Reprise d'Activité (PRA). | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Appliquer des mises à jour et correctifs aux logiciels et aux systèmes d'exploitation (OS). | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Gérer les droits d'accès des administrateurs. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Réaliser des sauvegardes régulières afin de restaurer les données et logiciels. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Utiliser un VPN uniquement pour les salariés cadres. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Défendre, surveiller les passerelles Internet, isoler les applications Web. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Assurer une veille constante sur les Threat Intelligence pour être informé des menaces actuelles et émergentes spécifiques à l'industrie. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Intégrer un framework de gestion des risques cybersécuritaires, comme le NIST, pour structurer et orienter les efforts. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

Q21 Vous sentez-vous concerné(e) par les recommandations de sécurité formulées **par votre entreprise** ?

| | Tout à fait d'accord | Plutôt d'accord | Ni d'accord ni pas d'accord | Plutôt pas d'accord | Pas du tout d'accord |
|---|---|---|---|---|---|
| Suivre les recommandations | ☐ | ☐ | ☐ | ☐ | ☐ |

| | | | | | |
|---|---|---|---|---|---|
| de l'ANSSI. | | | | | |
| Protéger et identifier les données sensibles. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Vérifier la vigilance lors de l'ouverture d'e-mails et la vérification des destinataires. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Sensibiliser les collaborateurs aux risques en ligne. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Adopter une 'hygiène informatique' quotidienne rigoureuse. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Télécharger les applications sur les sites ou magasins officiels ou non. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Utiliser un gestionnaire de mots de passe recommandé. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Autoriser l'accès de votre PC professionnel à vos enfants. | ☐ | ☐ | ☐ | ☐ | ☐ |

# Page 8

Q22 Selon vous, se former à la sécurité/cybersécurité pour développer **ses compétences en entreprise** c'est :

| | Tout à fait d'accord | Plutôt d'accord | Ni d'accord ni pas d'accord | Plutôt pas d'accord | Pas du tout d'accord | Ne sait pas |
|---|---|---|---|---|---|---|
| Mener régulièrement des audits de sécurité pour identifier les failles. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Maîtriser des outils pointus pour repérer les intrusions. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Organiser des simulations d'attaque pour tester les défenses (Red Teaming). | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Élaborer des stratégies de sécurité informatique. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Utiliser des techniques de cryptographie sophistiquées. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Préparer un plan de continuité des opérations (type PRA). | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Acquérir des ressources spécialisées du darknet. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Adopter la norme ISO 27001 dans la gestion de la sécurité. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Gérer les identités et les accès efficacement (IAM). | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Prévenir les fuites de données (DLP). | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Opérer des systèmes de gestion de la sécurité de l'information (ISMS). | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Configurer des outils de cryptographie comme DSA et RSA. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

| | | | | | | |
|---|---|---|---|---|---|---|
| Naviguer entre les rôles de Gray Hat Hacker. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Isoler les applications avec sandboxing et conteneurisation. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Comprendre la réalisation d'une Analyse d'Impact relative à la Protection des Données (AIPD). | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Chasser proactivement les menaces numériques (Threat Hunting). | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

Q23 Selon vous, quelles stratégies pourraient être mises en œuvre pour **stimuler l'intelligence collective** en matière de cybersécurité au sein d'une équipe, qu'elle soit dédiée à la sécurité, constituée de salariés ou d'un service spécifique ?

| | Tout à fait d'accord | Plutôt d'accord | Ni d'accord ni pas d'accord | Plutôt pas d'accord | Pas du tout d'accord |
|---|---|---|---|---|---|
| Instaurer une culture d'entreprise qui valorise la sécurité et la cybersécurité. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Développer des programmes de formation en cybersécurité adaptés au profil de chaque employé. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Sensibiliser spécifiquement chaque service de l'entreprise à la cybersécurité. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Tisser des liens solides entre les équipes dédiées à la sécurité et tous les salariés. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Assurer une veille technologique et réglementaire constante pour l'équipe de sécurité. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Mettre en place une cellule de crise inter-départementale et interfiliale. | ☐ | ☐ | ☐ | ☐ | ☐ |

| | | | | | |
|---|---|---|---|---|---|
| Promouvoir le partage de savoir-faire en matière de sécurité avec les fournisseurs et partenaires. | ☐ | ☐ | ☐ | ☐ | ☐ |
| S'engager en faveur de la formation continue des équipes de sécurité et des prestataires externes. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Encourager une ouverture d'esprit via des visioconférences dédiées à la sécurité. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Stimuler la curiosité intellectuelle pour les meilleures pratiques en informatique. | ☐ | ☐ | ☐ | ☐ | ☐ |

Q24 Toujours pour **stimuler l'intelligence collective**, quelles autres stratégies pourraient être mises en œuvre ?

| | Tout à fait d'accord | Plutôt d'accord | Ni d'accord ni pas d'accord | Plutôt pas d'accord | Pas du tout d'accord |
|---|---|---|---|---|---|
| Inculquer une vigilance permanente lors de l'utilisation de réseaux connectés. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Clarifier les risques et conséquences liés aux différents usages informatiques. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Établir des mesures de sécurité de base à mettre en place au domicile des employés. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Concevoir des formations en cybersécurité qui intègrent les aspects de l'intelligence artificielle. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Former les équipes en fonction des applications utilisées et de leur environnement | ☐ | ☐ | ☐ | ☐ | ☐ |

| | | | | | |
|---|---|---|---|---|---|
| numérique. | | | | | |
| Organiser des simulations d'attaques de phishing pour tester la réactivité des employés. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Instituer une heure annuelle de 'blackout' par service pour sensibiliser au risque de dépendance au numérique. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Prévoir des journées dédiées à la sensibilisation à la sécurité et à la cybersécurité. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Proposer des sessions informelles de formation à la sécurité pendant le déjeuner en télétravail (choix libre). | ☐ | ☐ | ☐ | ☐ | ☐ |
| Diffuser un podcast sur la sécurité et les cyberattaques, accessible lors des trajets quotidiens (choix libre). | ☐ | ☐ | ☐ | ☐ | ☐ |

# Page 9

Q25 Comment évaluez-vous **l'importance** des propositions ci-dessous ?

Plusieurs réponses possibles

| | Très important | Moins important |
|---|---|---|
| Formaliser sa politique de sécurité informatique | ☐ | ☐ |
| Sensibiliser les utilisateurs du parc informatique | ☐ | ☐ |
| Mettre à jour les systèmes d'exploitation (OS) sur tous les matériels (ordinateurs, tablettes, smartphones...) | ☐ | ☐ |
| Mettre à jour les logiciels, navigateurs, plugins, Java, etc. | ☐ | ☐ |
| Changer régulièrement de mots de passe | ☐ | ☐ |
| Faire des sauvegardes ordinateurs/ smartphones régulières | ☐ | ☐ |
| Surveiller la présence éventuelle de ses données personnelles sur le darknet et autres plateformes | ☐ | ☐ |
| Réaliser des audits de sécurité pour vérifier l'intégrité de son écosystème informatique | ☐ | ☐ |
| Respecter les règles relatives aux réseaux sociaux | ☐ | ☐ |
| Respecter les règles de mot de passe WIFI | ☐ | ☐ |
| Respecter les règles de paiement en ligne | ☐ | ☐ |
| Respecter les chartes Internet utilisateurs | ☐ | ☐ |
| Faire attention en ouvrant les e-mails (phishing, virus) | ☐ | ☐ |
| Utiliser un firewall et/ou VPN | ☐ | ☐ |
| Protéger vos données en déplacement | ☐ | ☐ |
| Protéger son identité numérique en ligne | ☐ | ☐ |

Q26 Reprenons les mêmes propositions. Comment évaluez-vous leur **facilité technique** ?

Plusieurs réponses possibles

| | Facile techniquement | Difficile techniquement |
|---|---|---|
| Formaliser sa politique de sécurité informatique | ☐ | ☐ |
| Sensibiliser les utilisateurs du parc informatique | ☐ | ☐ |
| Mettre à jour les systèmes d'exploitation (OS) sur tous les matériels (ordinateurs, tablettes, smartphones...) | ☐ | ☐ |
| Mettre à jour les logiciels, navigateurs, plugins, Java, etc. | ☐ | ☐ |
| Changer régulièrement de mots de passe | ☐ | ☐ |
| Faire des sauvegardes ordinateurs/ smartphones régulières | ☐ | ☐ |
| Surveiller la présence éventuelle de ses données personnelles sur le darknet et autres plateformes | ☐ | ☐ |
| Réaliser des audits de sécurité pour vérifier l'intégrité de son écosystème informatique | ☐ | ☐ |
| Respecter les règles relatives aux réseaux sociaux | ☐ | ☐ |
| Respecter les règles de mot de passe WIFI | ☐ | ☐ |
| Respecter les règles de paiement en ligne | ☐ | ☐ |
| Respecter les chartes Internet utilisateurs | ☐ | ☐ |
| Faire attention en ouvrant les e-mails (phishing, virus) | ☐ | ☐ |
| Utiliser un firewall et/ou VPN | ☐ | ☐ |
| Protéger vos données en déplacement | ☐ | ☐ |
| Protéger son identité numérique en ligne | ☐ | ☐ |

Q27 Encore une fois sur les mêmes propositions, comment évaluez-vous **votre niveau de maîtrise** ?

Plusieurs réponses possibles

| | Maîtrisé | A approfondir |
|---|---|---|
| Formaliser sa politique de sécurité informatique | ☐ | ☐ |
| Sensibiliser les utilisateurs du parc informatique | ☐ | ☐ |
| Mettre à jour les systèmes d'exploitation (OS) sur tous les matériels (ordinateurs, tablettes, smartphones...) | ☐ | ☐ |
| Mettre à jour les logiciels, navigateurs, plugins, Java, etc. | ☐ | ☐ |
| Changer régulièrement de mots de passe | ☐ | ☐ |
| Faire des sauvegardes ordinateurs/ smartphones régulières | ☐ | ☐ |
| Surveiller la présence éventuelle de ses données personnelles sur le darknet et autres plateformes | ☐ | ☐ |
| Réaliser des audits de sécurité pour vérifier l'intégrité de son écosystème informatique | ☐ | ☐ |
| Respecter les règles relatives aux réseaux sociaux | ☐ | ☐ |
| Respecter les règles de mot de passe WIFI | ☐ | ☐ |
| Respecter les règles de paiement en ligne | ☐ | ☐ |
| Respecter les chartes Internet utilisateurs | ☐ | ☐ |
| Faire attention en ouvrant les e-mails (phishing, virus) | ☐ | ☐ |
| Utiliser un firewall et/ou VPN | ☐ | ☐ |
| Protéger vos données en déplacement | ☐ | ☐ |
| Protéger son identité numérique en ligne | ☐ | ☐ |

# Page 10

Q28 Merci de précisez votre statut

☐ Je suis étudiant, indépendant

☐ Je suis salarié

# Page 11

Q29 Avez-vous actuellement un rôle de manager ou occupez-vous un poste d'encadrement dans votre entreprise ou centre de formation ?

☐ Oui

☐ Non

Q30 Dans votre entreprise, à quel service ou département appartenez-vous ?

☐ 1 ere à 4 eme année d'étude

☐ 5 eme année et plus

☐ DIRECTION

☐ COMPTABILITE

☐ RESSOURCES HUMAINES

☐ VENTES

☐ MARKETING

☐ FINANCE

☐ LOGISTIQUE

☐ PRODUCTION

☐ ACHATS

☐ INFORMATIQUE

☐ COMMUNICATION

☐ SERVICE CLIENT

☐ SUPPORT DES VENTES

☐ MAINTENANCE

☐ SECRETARIAT

☐ QUALITE

☐ R&D

☐ SERVICES GENERAUX

☐ ASSURANCE

☐ FORMATION

☐ ORGANISATION

☐ DOCUMENTATION

☐ JURIDIQUE

☐ BUREAU D ETUDES

☐ CONTRÔLE DE GESTION

☐ GESTION DE PROJETS

☐ E-COMMERCE

☐ NTERNATIONAL

☐ [IMMOBILIER

☐ TRAVAUX

☐ SECURITE

☐ RELATIONS PUBLIQUES

☐ AUTRES

# Page 12

Q31 Quelles sont les actions à privilégier pour renforcer la culture de la cybersécurité **au sein de votre entreprise** ?

...../ Partager avec pédagogie la vision cybersécurité de l'entreprise auprès de l'ensemble des salariés.

...../ Utiliser la prévention pour se protéger face aux menaces en tous genres.

...../ Alerter l'ensemble du personnel sur les risques potentiels informatiques et cybermenaces.

...../ Appliquer les recommandations de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) afin de sensibiliser les salariés.

...../ Améliorer les moyens mis en oeuvre pour l'éducation et la sensibilisation des salariés.

...../ Impliquer l'ensemble des salariés, l'équipe sécurité de l'entreprise et pas uniquement les actions du RSSI.

...../ Consacrer du temps par l'équipe de sécurité afin de s'assurer que le personnel est toujours idéalement informé.

...../ Engager l'écosystème de l'entreprise, aussi bien les collaborateurs que les prestataires, les fournisseurs et les partenaires.

...../ Informer le personnel lorsqu'une attaque intervient, pour tenter de l'amener à comprendre et à agir de manière appropriée.

Q32 Dans le développement de a cybersécurité dans la société, diriez-vous que votre entreprise met en place une culture de la cybersécurité ?

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| ☐ | ☐ | ☐ | ☐ | ☐ |

Q33 Est-ce important pour vous d'être immédiatement informé par SMS en cas d'attaque informatique visant votre entreprise, incluant des instructions à suivre ?

☐ Oui, indispensable

☐ Oui, très important

☐ Oui, assez important

☐ Non

# Page 13

Q34 En cas d'attaque informatique, de fraude, de vol, de phishing et autres incidents similaires, diriez-vous que :

Plusieurs réponses possibles

| | Oui, tout à fait | Oui, en partie | Non, pas vraiment | Non, pas du tout | Ne sait pas |
|---|---|---|---|---|---|
| Vous avez les informations nécessaires pour comprendre la situation et agir de manière appropriée. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Vous êtes au courant des premières mesures à prendre. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Vous avez confiance en la capacité de réaction de l'équipe en charge de la sécurité informatique. | ☐ | ☐ | ☐ | ☐ | ☐ |

Q35 En fonction de vos expériences personnelles et/ou professionnelles passées, quel serait votre niveau de stress ?

☐ Pas du tout stressé

☐ Peu stressé

☐ Modérément stressé

☐ Très stressé

☐ Extrêmement stressé

Q36 Selon vous, est-il nécessaire que le service informatique ou la DSI mette en place des <u>simulations de cyberattaques</u> pour sensibiliser efficacement les employés, évaluer les mesures de sécurité et tester leurs réflexes numériques ?

☐ Oui, indispensable

☐ Oui, par précaution

☐ Non

☐ Ne sait pas

Q37 Considérez-vous comme nécessaire de signaler à votre service informatique ou à votre DSI en cas de piratage d'un ordinateur, d'une tablette ou d'un smartphone **dans votre environnement familial** ?

☐ Oui, indispensable

☐ Oui, par précaution

☐ Non

☐ Ne sait pas

# Page 14

Q38 Disposez-vous des outils adéquats tels qu'un cahier de notes, des fichiers informatiques, des services en ligne, etc., pour organiser et planifier efficacement votre politique de sécurité (y compris une liste de plans d'action basés sur un processus) dans votre environnement domestique ?

☐ J'ai déjà les outils adéquats

☐ Je suis en phase de recherche de solution

☐ Je n'ai pas ce type d'outils

Q39 Pour qu'une approche de sensibilisation à la sécurité informatique /cybersécurité soit pertinente et efficace, quelle serait la bonne répartition à adopter entre :

| | | |
|---|---|---|
| La sensibilisation liée à l'environnement professionnel | | % |
| La sensibilisation liée à l'environnement personnel | | % |
| **Total à répartir** | **100** | **%** |

Q40 Dans votre entreprise, quels sont **les freins** à la sensibilisation à la sécurité informatique /cybersécurité ?

Plusieurs réponses possibles

| | 1 Pas un frein | 2 | 3 | 4 | 5 Frein très important |
|---|---|---|---|---|---|
| La malveillance | ☐ | ☐ | ☐ | ☐ | ☐ |
| L'erreur humaine | ☐ | ☐ | ☐ | ☐ | ☐ |
| Le manque de temps en entreprise | ☐ | ☐ | ☐ | ☐ | ☐ |
| Le manque d'investissement dans la création et/ou l'achat de supports de formation | ☐ | ☐ | ☐ | ☐ | ☐ |
| Le manque d'implication des salariés | ☐ | ☐ | ☐ | ☐ | ☐ |
| Le manque de volonté d'apprendre dans le cadre de la formation continue | ☐ | ☐ | ☐ | ☐ | ☐ |

Q41 Si vous deviez signaler un incident de sécurité ou une activité suspecte :

Plusieurs réponses possibles

| | Oui | Non | Ne sait pas |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Je serais à l'aise pour signaler un incident de sécurité. | ☐ | ☐ | ☐ |
| Je serais à l'aise pour signaler une activité suspecte. | ☐ | ☐ | ☐ |
| Je sais comment faire pour signaler un incident de sécurité. | ☐ | ☐ | ☐ |
| Je sais comment faire pour signaler une activité suspecte. | ☐ | ☐ | ☐ |

Q42 Dans votre entreprise, l'information pertinente concernant la sensibilisation à la sécurité informatique /cybersécurité est-elle diffusée ?

Plusieurs réponses possibles

| | Toujours | Souvent | Parfois | Jamais |
|---|---|---|---|---|
| Aux bons destinataires | ☐ | ☐ | ☐ | ☐ |
| Dans le bon timing, au bon moment | ☐ | ☐ | ☐ | ☐ |
| De façon claire et compréhensible par tous | ☐ | ☐ | ☐ | ☐ |
| De façon utilisable par tous | ☐ | ☐ | ☐ | ☐ |
| Permettant l'apprentissage tout au long du contrat de travail | ☐ | ☐ | ☐ | ☐ |
| En alliant la théorie et la pratique | ☐ | ☐ | ☐ | ☐ |

Q43 Dans quelle mesure vous sentez-vous engagé(e) envers votre politique de sécurité entreprise ?

☐ Très peu engagé(e) : Je ne suis pas du tout concerné par la politique de sécurité et je ne pense pas que ce soit important pour mon travail.

☐ Peu engagé(e) : Je suis conscient de la politique de sécurité, mais je ne la considère pas comme une priorité dans mon travail quotidien.

☐ Modérément engagé(e) : Je comprends l'importance de la politique de sécurité et je m'efforce de respecter ses règles autant que possible.

☐ Engagé(e) : Je prends la politique de sécurité au sérieux et je suis attentif à respecter toutes ses règles dans mon travail.

☐ Très engagé(e) : La politique de sécurité est une priorité pour moi. Je suis toujours à jour avec ses exigences et j'encourage également mes collègues à la respecter.

Q44 La politique de sécurité de votre entreprise/organisation est-elle efficace pour prévenir les incidents de cybersécurité ?

☐ Pas du tout efficace : Je pense que notre politique de sécurité n'a aucun effet sur la prévention des incidents de cybersécurité.

☐ Peu efficace : Notre politique de sécurité pourrait avoir un effet mineur sur la prévention des incidents de cybersécurité, mais je pense qu'il y a beaucoup d'améliorations à faire.

☐ Modérément efficace : Notre politique de sécurité a un certain impact sur la prévention des incidents de cybersécurité, bien qu'il y ait encore des domaines à améliorer.

☐ Efficace : Je crois que notre politique de sécurité est en grande partie efficace pour prévenir les incidents de cybersécurité.

☐ Très efficace : Je suis convaincu que notre politique de sécurité est extrêmement efficace et joue un rôle crucial dans la prévention des incidents de cybersécurité.

# Page 16

Q44 Si vous deviez suivre une formation à l'IA dans les 6 prochains mois, que préféreriez-vous ?

Plusieurs réponses possibles

☐ Une formation en présentiel

☐ Une formation en e-learning

☐ Aucun des deux

☐ Ne sait pas

Q45 Pour améliorer la sécurité et la conformité des données dans votre entreprise dans le cadre du RGPD (Règlement Général sur la Protection des Données), quelles sont les actions les plus importantes ?

...../ Sensibiliser les salariés à la conformité RGPD (note d'information interne, réunion d'information par service, e-learning de 30 à 45 minutes...)

...../ Limiter l'accès aux données par : MFA, VPN, mail chiffré, cryptage des disques, gestionnaire de mot de passe

...../ Identifier les données dites sensibles (données sensibles interdites en entreprise et les données sensibles obligatoires)

...../ Planifier la politique de sécurité des données (Autorisation de contrôle d'accès, Accès aux réseaux, Responsabilités des utilisateurs)

...../ Prévoir et faire face aux demandes d'accès aux données des intéressés (utilisateurs, clients, fournisseurs, etc.)

...../ Vérifier l'application des mises à jour et sauvegarder régulièrement les données de votre entreprise

Q46 Dans votre travail quotidien, quel pourcentage de votre temps consacrez-vous à l'application du RGPD ?

☐ 100%

☐ 75%

☐ 50%

☐ 25%

☐ Non concerné

Q47 Avez-vous participé à une formation à la cybersécurité au cours de l'année écoulée ?

☐ Oui, en présentiel

☐ Oui, en e-learning

☐ Non, ni en présentiel ni en e-learning

Q48 Si vous deviez suivre une formation à la cybersécurité dans les 6 prochains mois, que préféreriez-vous ?

☐ Une formation en présentiel

☐ Une formation en e-learning

☐ Aucun des deux

☐ Ne sait pas

Q49 Quelle serait pour vous la durée idéale d'une formation en cybersécurité ?

☐ 2 heures

☐ 4 heures

☐ 1 journée

☐ 2 journées

☐ Plus de 2 journées

Q50 Pour vous former à la cybersécurité, êtes-vous favorable à :

| | Oui, plutôt | Non, plutôt pas |
|---|---|---|
| Utiliser votre Compte Personnel de Formation (CPF) | ☐ | ☐ |
| Suivre la formation dispensée par mon entreprise | ☐ | ☐ |
| Suivre une formation certifiante | ☐ | ☐ |
| Vous former sur votre temps libre | ☐ | ☐ |

Q51 Dans le domaine de la recherche et du développement (R&D), l'Innovation ouverte ou Open Innovation en anglais, désigne des modes d'innovation fondés sur le partage, la collaboration. Diriez-vous que votre environnement de travail favorise le développement de l'innovation ouverte ?

☐ Oui, tout à fait

☐ Oui, plutôt

☐ Ni oui, ni non

☐ Non, plutôt pas

☐ Non, pas du tout

Q52 Vous arrive-t-il de prendre l'initiative de partager des connaissances, des conseils sur la cybersécurité et d'encourager des pratiques cyber pour booster la cybersécurité dans votre entreprise ?

☐ Très souvent

☐ Parfois

☐ Rarement

☐ Jamais

Q53 Avec l'évolution des cyberattaques, il est important d'établir des points de contact au sein des

entreprises pour sensibiliser à la sécurité informatique /cybersécurité. Seriez-vous prêt(e) à participer à cette initiative en tant qu'**ambassadeur** de la sécurité ?

☐ Oui

☐ Non

☐ Ne sait pas

Q54 Comment évaluez-vous l'efficacité de vos managers en tant qu'ambassadeurs de la cybersécurité dans votre service ?

Plusieurs réponses possibles

| | Très efficace | Plutôt efficace | Neutre | Plutôt pas efficace | Pas du tout efficace |
|---|---|---|---|---|---|
| Leur niveau de sensibilisation à l'importance de la cybersécurité. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Leur compréhension des menaces cybernétiques. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Leur capacité à distinguer entre des comportements sécurisés et risqués. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Leurs efforts pour sensibiliser les employés aux mesures de sécurité. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Leur implication dans la planification et la mise en œuvre de projets, avec une attention particulière aux risques de cybersécurité. | ☐ | ☐ | ☐ | ☐ | ☐ |
| La qualité de leur coopération avec l'équipe de sécurité informatique. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Leur leadership influent et leur capacité à fournir des conseils pertinents en matière de cybersécurité. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Leur aptitude à répondre aux interrogations des employés ou à les orienter vers des | ☐ | ☐ | ☐ | ☐ | ☐ |

| | | | | | |
|---|---|---|---|---|---|
| experts. | | | | | |
| Leur engagement continu envers les valeurs de la cybersécurité. | ☐ | ☐ | ☐ | ☐ | ☐ |

Q55 Quelles sont les stratégies à privilégier pour stimuler l'intelligence collective en matière de cybersécurité ?
5 réponses possibles

...../ Instaurer une culture d'entreprise qui valorise la sécurité et la cybersécurité.

...../ Développer des programmes de formation en cybersécurité adaptés au profil de chaque employé.

...../ Sensibiliser spécifiquement chaque service de l'entreprise à la cybersécurité.

...../ Tisser des liens solides entre les équipes dédiées à la sécurité et tous les salariés.

...../ Assurer une veille technologique et réglementaire constante pour l'équipe de sécurité.

...../ Promouvoir le partage de savoir-faire en matière de sécurité avec les fournisseurs et partenaires.

...../ Mettre en place une cellule de crise interdépartementale et interfiliale.

...../ S'engager en faveur de la formation continue des équipes de sécurité et des prestataires externes.

...../ Encourager une ouverture d'esprit via des visioconférences dédiées à la sécurité.

...../ Stimuler la curiosité intellectuelle pour les meilleures pratiques en informatique.

...../ Inculquer une vigilance permanente lors de l'utilisation de réseaux connectés.

...../ Clarifier les risques et conséquences liés aux différents usages informatiques.

...../ Établir des mesures de sécurité de base à mettre en place au domicile des employés.

...../ Concevoir des formations en cybersécurité qui intègrent les aspects de l'intelligence artificielle.

...../ Former les équipes en fonction des applications utilisées et de leur environnement numérique.

...../ Organiser des simulations d'attaques de phishing pour tester la réactivité des employés.

...../ Instituer une heure annuelle de « blackout » par service pour sensibiliser au risque de dépendance au numérique.

...../ Prévoir des journées dédiées à la sensibilisation à la sécurité et à la cybersécurité.

...../ Proposer des sessions informelles de formation à la sécurité pendant le déjeuner en télétravail (choix libre).

...../ Diffuser un podcast sur la sécurité et les cyberattaques, accessible lors des trajets quotidiens (choix libre).

Q56 Les neurosciences cognitives sont le domaine de recherche dans lequel sont étudiés les mécanismes neurobiologiques qui sous-tendent la cognition (perception, motricité, langage, mémoire, raisonnement, émotions). Qu'en savez-vous ?

☐ Je connais bien ce sujet (connaissances précises)

☐ J'en ai entendu parler (connaissances vagues)

☐ Je ne sais pas de quoi il s'agit

Q57 Comment évaluez-vous l'efficacité des stratégies suivantes basées sur les neurosciences cognitives en matière de cybersécurité ?

| | Plutôt efficaces | Plutôt pas efficaces |
|---|---|---|
| Détection avancée des menaces : Comprendre les processus mentaux pour développer des modèles prédictifs qui identifient les comportements en ligne suspects. | ☐ | ☐ |
| Renforcement de la sensibilisation à la sécurité : Adapter les programmes de formation et de sensibilisation aux caractéristiques cognitives des individus. | ☐ | ☐ |
| Protection contre l'ingénierie sociale : Développer des stratégies basées sur la compréhension des tactiques de persuasion pour contrer les tentatives de manipulation. | ☐ | ☐ |
| Amélioration de l'expérience utilisateur sécurisée : Conception d'interfaces utilisateur intuitives pour réduire les erreurs humaines et les vulnérabilités en cybersécurité. | ☐ | ☐ |

Q58 Dans quelle mesure êtes-vous d'accord avec les affirmations suivantes concernant l'impact des neurosciences sur les programmes de formation en cybersécurité ?

| | Tout à fait d'accord | Plutôt d'accord | Ni d'accord ni pas d'accord | Plutôt pas d'accord | Pas du tout d'accord |
|---|---|---|---|---|---|
| Les programmes basés sur les neurosciences permettent une personnalisation plus efficace de l'apprentissage, améliorant la rétention des informations et des compétences en cybersécurité. | ☐ | ☐ | ☐ | ☐ | ☐ |
| L'utilisation des principes neuroscientifiques augmente l'engagement et la motivation des apprenants en | ☐ | ☐ | ☐ | ☐ | ☐ |

| | | | | | |
|---|---|---|---|---|---|
| cybersécurité. | | | | | |
| Les techniques inspirées des neurosciences améliorent les compétences de résolution de problèmes dans des situations de cybersécurité complexes. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Une meilleure compréhension du fonctionnement cérébral aide à réduire les erreurs humaines et les vulnérabilités comportementales en cybersécurité. | ☐ | ☐ | ☐ | ☐ | ☐ |

Q59 Dans quelle mesure êtes-vous satisfait du contenu des formations sur la cybersécurité proposé par les RH/DSI ?

☐ Oui, tout à fait satisfait

☐ Oui, plutôt satisfait

☐ Neutre

☐ Non plutôt pas satisfait

☐ Non, pas du tout satisfait

Q60 Dans votre quotidien, estimez-vous que vous mettez en oeuvre efficacement les bonnes postures de cybersécurité pour vous protéger (contre les virus, le piratage, les arnaques en ligne, etc.) ?

☐ Tout à fait d'accord

☐ D'accord

☐ Ni d'accord ni pas d'accord

☐ Pas d'accord

☐ Pas du tout d'accord

Q61 Comment évaluez-vous l'efficacité de votre service informatique / DSI en tant qu'ambassadeurs de la cybersécurité dans votre entreprise ?

| | Très efficace | Plutôt efficace | Neutre | Plutôt pas efficace | Pas du tout efficace |
|---|---|---|---|---|---|
| Leur niveau de sensibilisation à l'importance de la cybersécurité. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Leur compréhension des menaces cybernétiques. | ☐ | ☐ | ☐ | ☐ | ☐ |

| | | | | | |
|---|---|---|---|---|---|
| Leur capacité à distinguer entre des comportements sécurisés et risqués. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Leurs efforts pour sensibiliser les employés aux mesures de sécurité. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Leur implication dans la planification et la mise en œuvre de projets, avec une attention particulière aux risques de cybersécurité. | ☐ | ☐ | ☐ | ☐ | ☐ |
| La qualité de leur coopération avec l'équipe de sécurité informatique. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Leur leadership influent et leur capacité à fournir des conseils pertinents en matière de cybersécurité. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Leur aptitude à répondre aux interrogations des employés ou à les orienter vers des experts. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Leur engagement continu envers les valeurs de la cybersécurité. | ☐ | ☐ | ☐ | ☐ | ☐ |

Q62 Si vous travaillez dans le domaine de la cybersécurité, vous considérez-vous comme un expert légitime dans ce domaine ?

☐ Oui

☐ Non

☐ Je ne travaille pas dans le domaine de la cybersécurité

# Page 19

Q63 Quel est votre niveau d'anglais ?

☐ Débutant

☐ Intermédiaire

☐ Avancé

☐ Langue maternelle ou bilingue

Q64 Quel est le plus haut niveau de diplôme que vous avez obtenu ?

☐ Sans diplôme

☐ Diplôme National du Brevet (DNB)

☐ Baccalauréat

☐ Diplôme Universitaire de Technologie (DUT)

☐ Brevet de Technicien Supérieur (BTS)

☐ Licence (L1, L2, L3)

☐ Master (M1, M2)

☐ Doctorat

☐ Précisez :

Q65 Quelle est votre tranche d'âge ?

☐ 19 ans ou moins

☐ 20-39 ans

☐ 40-59 ans

☐ 60 ans ou plus

Q66 Etes-vous ?

☐ Un homme

☐ Une femme

Q67 Quel est le code postal de votre lieu de résidence ?

# Page 20

Q68 Dans quelle langue préfères-tu suivre la formation ?

☐ Français

☐ Anglais

Q69 Dans quel type d'établissement es-tu inscrit(e) ?

☐ École d'ingénieur

☐ École de commerce

☐ Université

☐ Autre :

☐ École spécialisée (design, communication, informatique…)

Q70 Quelle est ton année d'étude actuelle ?

☐ 1re année

☐ 2e année

☐ 3e année

☐ 4e année

☐ 5e année ou plus

Q71 Quelle est ta spécialisation / ton majeur principal ?

☐ Data / IA

☐ Informatique / cybersécurité

☐ Marketing / communication

☐ Autre :

☐ Finance / gestion

☐ Design / création

Q72 Avez-vous déjà réalisé un stage, une alternance ou une expérience freelance ?

☐ Non

☐ Oui, 1 expérience

☐ Oui, 2 expériences

☐ Oui, 3 ou plus

Q73 Quel format te motive le plus ?

☐ Exemples concrets et cas réels

☐ Concepts théoriques bien expliqués

☐ Démonstrations pas à pas

☐ Défis et mini-projets

Q74 En général, comment te décrirais-tu dans les formations en ligne ?

☐ Je décroche vite si ça ne m’intéresse pas

☐ J’avance, mais je zappe ce qui ne m’accroche pas

☐ Je suis les parcours jusqu’au bout

☐ Je vais plus loin que ce qui est demandé

# Page 21

Q75 Êtes-vous autonome dans votre apprentissage ?

☐ Peu

☐ Moyennement

☐ Oui

☐ Totalement

Q76 Quelle est ta motivation principale pour cette formation ?

☐ Réussir mes études

☐ Améliorer mon employabilité

☐ Autre :

☐ Curiosité personnelle

☐ C’est obligatoire dans mon cursus

Q77 Comment préfères-tu que l’IA te parle ?

☐ Très guidant, pas à pas

☐ Plutôt pédagogique et rassurant

☐ Direct et challengeant

☐ Peu importe, tant que c’est utile

Q78 Quel est ton objectif personnel pour ces 4 heures de formation ?

☐ Découvrir les bases

☐ Consolider ce que je sais déjà

☐ Aller plus loin que mon niveau actuel

☐ Préparer concrètement mon employabilité

Q79 Comment évaluez-vous votre niveau en IA ?

☐ Intermédiaire

☐ Avancé

☐ Expert

Q80 Comment évaluez-vous votre niveau en cybersécurité ?

☐ Intermédiaire

☐ Avancé

☐ Expert

Q81 Sur une échelle de 1 à 5, à quel point vous considérez-vous créatif ?

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| ☐ | ☐ | ☐ | ☐ | ☐ |

Q82 Passez-vous ce test pour la première fois ?

☐ Oui

☐ Non

# Page 22

Q83 Quelle est votre ancienneté dans votre entreprise ou votre établissement de formation ?

☐ Moins d'un an

☐ De 1 à 3 ans inclus

☐ De 3 à 5 ans inclus

☐ De 5 à 10 ans inclus

☐ Plus de 10 ans

Q84 Avec quelle version de langue avez-vous répondu à ce questionnaire ?

Plusieurs réponses possibles

☐ FR Version française (FR)

☐ GB Version anglaise (EN)

Q85 Date du passage de notre test d evaluation

...../...../.....

Q86 Combien de salariés compte votre entreprise (en France) ?

☐ Libellé du choix

☐ Auto entrepreneur / freelance

☐ Start up

☐ 0 à 9 salariés

☐ 10 à 49 salariés

☐ 50 à 249 salariés

☐ 250 à 499 salariés

☐ 500 à 999 salariés

☐ 1 000 à 2 499 salariés

☐ 2 500 à 4 999 salariés

☐ 5 000 salariés et plus

Q87 Merci pour votre évaluation sur ces test d’évaluation en cyber