Ce document a été mis en ligne par l'organisme FormaV®.

Toute reproduction, représentation ou diffusion, même partielle, sans autorisation préalable, est strictement interdite.

Pour en savoir plus sur nos formations disponibles, veuillez visiter :
formav.co/explorer

BTS SIO

Expression et communication en langue anglaise

Session 2019 • Code sujet : **19-SIE1ANG-ME1 (id 19AU)** • Durée : **2 h 00** • Coefficient : **2**

Sommaire

Cliquez sur une partie pour y accéder directement

1. Compte rendu en français sur les clés de sécurité et l'authentification multifacteur (1 question) **Page 3**

2. Courriel de conseil sur la protection des données professionnelles en déplacement (1 question) **Page 4**

3. Ce qu'il faut retenir & Questions fréquentes (FAQ) (Synthèse & Q&A Examen) **Page 6**

Sujet officiel (PDF) : https://coursbtssio.fr/assets/annales/bts-sio/E1.2 - Expression et communication en langue anglaise/2019/BTS SIO - E1.2 - Expression et communication en langue anglaise - Session 2019 - 1-Sujet.pdf

1. Compte rendu en français sur les clés de sécurité et l’authentification multifacteur

L’article de Patrick Howell O’Neill, publié dans CyberScoop le 25 juillet 2018, présente la clé de sécurité Titan de Google et l’usage de clés matérielles pour limiter les prises de contrôle de comptes. Il compare ces clés aux codes par SMS et aux applications mobiles, et souligne le rôle du phishing dans les cyberattaques.

Question 1. Rédigez en français un compte rendu du texte de 200 mots, avec une marge de plus ou moins 10 %. Introduisez brièvement la date, la source et le thème du document, puis synthétisez et reformulez ses idées essentielles. Ajoutez une brève conclusion personnelle sur l’intérêt du document dans une perspective professionnelle et indiquez impérativement le nombre de mots.

Publié le 25 juillet 2018 dans *CyberScoop*, l’article de Patrick Howell O’Neill présente la clé Titan de Google et le rôle des clés matérielles dans la protection des comptes en ligne.

Google a équipé ses 85 000 employés de clés USB et n’a confirmé aucun détournement de compte depuis plus d’un an. Elle lance désormais Titan, qui complète le mot de passe : il faut brancher et activer la clé pour accéder au service. Google la présente comme une protection simple et robuste, notamment pour les administrateurs. La clé bloque aussi certaines attaques dites « homme du milieu ». Le produit sera ensuite proposé au grand public. La console d’administration facilite son activation pour chaque application.

L’article rappelle que le phishing serait à l’origine d’environ 71 % des attaques ciblées. Les codes par SMS et les applications mobiles apportent un second facteur, mais sont plus faciles à intercepter ou pirater. Les clés physiques résistent mieux à ces menaces. De nombreuses grandes entreprises utilisent déjà des YubiKeys ; Google les a également distribuées à ses salariés.

Enfin, l’auteur recommande l’authentification multifacteur à tous les internautes. Pour les professionnels, le texte montre qu’une protection renforcée des comptes sensibles peut rester simple à déployer et à utiliser.

Nombre de mots : 199.

Repères de langue, hors compte rendu : « détournement de compte » et « authentification multifacteur » sont utiles pour parler de cybersécurité. Le présent sert à résumer les idées de l’article ; le conditionnel « serait » rapporte avec prudence le chiffre sur le phishing.

> **✓ RÉPONSE À RETENIR**
>
> Compte rendu modèle : 199 mots, dans la fourchette demandée de 180 à 220 mots.

2. Courriel de conseil sur la protection des données professionnelles en déplacement

Vous êtes consultant ou consultante informatique spécialisé(e) en protection des données. Peter Kelly, chef d'entreprise irlandais qui voyage régulièrement, souhaite accéder à des documents professionnels confidentiels et vous demande des conseils pour protéger leur stockage.

Question 1. Rédigez en anglais un courriel d'environ 150 mots à Peter Kelly. Indiquez les meilleures solutions pour protéger ses données et donnez des conseils techniques, ainsi que des conseils juridiques éventuels, afin que ses documents confidentiels soient stockés en toute sécurité et accessibles pendant ses déplacements.

Model email in English

Dear Mr Kelly,

Thank you for your message. To access confidential files while travelling, use a trusted business cloud service. Choose one that encrypts files in transit and at rest, and activate multi-factor authentication, preferably with a security key. Use an updated, company-managed laptop with a strong password and full-disk encryption. Avoid public Wi-Fi or connect through your company's VPN. Never use shared computers. Keep an encrypted backup in a separate, secure location.

Give employees access only to the files they need. Enable remote locking and erasing if a device is lost, and review access regularly. Before signing, check the provider's security measures, data-processing agreement and breach notification process. If your business is based in Ireland, ensure that it and the provider comply with the GDPR, especially when personal data is involved. Check that transfers outside the EEA have the required safeguards. These measures will help you work securely while travelling.

Kind regards,
Edwin Parker

Traduction française pédagogique

Cher Monsieur Kelly,

Merci pour votre message. Pour accéder à vos fichiers confidentiels pendant vos déplacements, utilisez un service cloud professionnel fiable. Choisissez-en un qui chiffre les fichiers pendant leur transfert et leur stockage, et activez l'authentification multifacteur, de préférence avec une clé de sécurité. Utilisez un ordinateur portable professionnel à jour, protégé par un mot de passe robuste et le chiffrement intégral du disque. Évitez les réseaux Wi-Fi publics ou connectez-vous par le VPN de votre entreprise. N'utilisez jamais d'ordinateurs partagés. Conservez une sauvegarde chiffrée dans un autre lieu sécurisé.

Donnez aux employés accès uniquement aux fichiers dont ils ont besoin. Activez le verrouillage et l'effacement à distance si un appareil est perdu, et vérifiez régulièrement les accès. Avant de signer, vérifiez les mesures de sécurité du fournisseur, son accord de traitement des données et sa procédure de notification des violations. Si votre entreprise est basée en Irlande, veillez à ce qu'elle-même et son fournisseur respectent le RGPD, en particulier lorsque des données personnelles sont concernées. Vérifiez que les transferts hors de l'EEE sont assortis des garanties requises. Ces mesures vous aideront à travailler en sécurité pendant vos déplacements.

Cordialement,
Edwin Parker

Vocabulaire et grammaire utiles : *in transit / at rest* : pendant le transfert / stocké ; *encrypt* : chiffrer ; *enable* : activer. L'impératif (*Use, Avoid, Check*) sert à donner des conseils. *If a device is lost* exprime une condition avec *if*.

✓ RÉPONSE À RETENIR

Conseiller un cloud chiffré, l'authentification multifacteur, des appareils sécurisés, des sauvegardes, des accès limités et le respect du RGPD.

Ce qu'il faut retenir de ce sujet (Session 2019)

Bilan de l'épreuve : Épreuve U12 d'expression et communication en langue anglaise du BTS Services informatiques aux organisations, session 2019, code 19-SIE1ANG-ME1, d'une durée de 2 h et de coefficient 2. Le sujet porte sur les clés Titan de Google, l'authentification multifacteur et le phishing. Il évalue la compréhension et la synthèse en français, puis la rédaction en anglais de conseils professionnels sur la protection des données confidentielles en déplacement.

Notions-clés, formules & règles à maîtriser

- L'authentification multifacteur ajoute une preuve d'identité à l'utilisation du mot de passe.
- Une clé de sécurité matérielle doit être activée lors de la connexion pour fournir un second facteur d'authentification.
- Le texte présente les clés de sécurité comme plus résistantes au phishing que les codes par SMS ou les applications mobiles.
- Le compte rendu doit reformuler les idées essentielles et indiquer la date, la source et le thème du texte.

Points de vigilance & attentes du jury

- Pour le compte rendu, respectez la longueur de 180 à 220 mots et indiquez le nombre de mots.
- Présentez la date, la source et le thème en introduction, puis reformulez les idées sans recopier le texte.
- Rédigez le courriel en anglais, en vous adressant à Peter Kelly et en tenant compte de ses déplacements.
- Proposez des conseils techniques pertinents et, si utile, juridiques, pour assurer le stockage sécurisé des documents.

Questions fréquentes sur cette épreuve (Q&A Examen)

Q : Comment organiser le compte rendu demandé dans la première partie ?

Commencez par indiquer la date, la source et le thème. Reformulez ensuite les idées essentielles du texte et terminez par une brève conclusion personnelle sur son intérêt professionnel. Le compte rendu doit compter entre 180 et 220 mots.

Q : Que faut-il expliquer sur les clés de sécurité et le phishing ?

Le texte présente les clés matérielles comme un second facteur de connexion, plus résistant au phishing que les codes par SMS ou certaines applications. Il souligne aussi que le phishing constitue une menace importante pour les comptes et les identifiants.

Q : Combien de temps consacrer à chaque partie ?

Le sujet prévoit deux heures au total, sans fixer de répartition entre les parties. Prévoyez du temps pour comprendre le texte, rédiger les deux productions et vérifier la langue, les consignes et les longueurs demandées.

Q : Quels critères sont explicitement attendus pour les deux productions ?

Le compte rendu doit présenter la date, la source et le thème, synthétiser les idées, inclure une conclusion personnelle et respecter 200 mots avec une marge de 10 %. Le courriel doit être en anglais et faire environ 150 mots.

Sujet officiel associé (PDF) : https://coursbtssio.fr/assets/annales/bts-sio/E1.2 - Expression et communication en langue anglaise/2019/BTS SIO - E1.2 - Expression et communication en langue anglaise - Session 2019 - 1-Sujet.pdf
Ressources BTS Services Informatiques aux Organisations : Toutes les annales & corrigés • Fiches de révision complètes • Simulateur de notes d'examen

Copyright © 2027 FormaV®. Tous droits réservés.

FormaV® est une marque déposée auprès de l'INPI sous le numéro 5227897.

Ce document a été élaboré par FormaV® avec le plus grand soin afin d'accompagner chaque apprenant vers la réussite de ses examens. Son contenu (textes, graphiques, méthodologies, tableaux, exercices, concepts, mises en forme) constitue une œuvre protégée par le droit d'auteur.

Toute copie, partage, reproduction, diffusion ou mise à disposition, même partielle, gratuite ou payante, est strictement interdite sans accord préalable et écrit de FormaV®, conformément aux articles L.111-1 et suivants du Code de la propriété intellectuelle. Dans une logique anti-plagiat, FormaV® se réserve le droit de vérifier toute utilisation illicite, y compris sur les plateformes en ligne ou sites tiers.

En utilisant ce document, vous vous engagez à respecter ces règles et à préserver l'intégrité du travail fourni. La consultation de ce document est strictement personnelle.

Merci de respecter le travail accompli afin de permettre la création continue de ressources pédagogiques fiables et accessibles.