FINANCES PUBLIQUES

CONCOURS EXTERNE
POUR L'ACCÈS AU GRADE D'INSPECTEUR DES FINANCES PUBLIQUES AFFECTÉ AU TRAITEMENT DE L'INFORMATION EN QUALITÉ D'ANALYSTE

ANNÉE 2022

ÉPREUVE ÉCRITE D'ADMISSION N° 3

Durée : 1 heure 30 – Coefficient : 1

Version anglaise à partir d'un texte issu d'une revue ou d'une documentation informatique

---

Seuls sont pris en compte les points obtenus au-dessus de 10.

Recommandations importantes

Le candidat trouvera au verso la manière de servir la copie dédiée.

Sous peine d'annulation, en dehors du volet rabattable d'en-tête, les copies doivent être totalement anonymes et ne comporter aucun élément d'identification tels que nom, prénom, signature, paraphe, localisation, initiale, numéro ou toute autre indication, même fictive, étrangère au traitement du sujet.

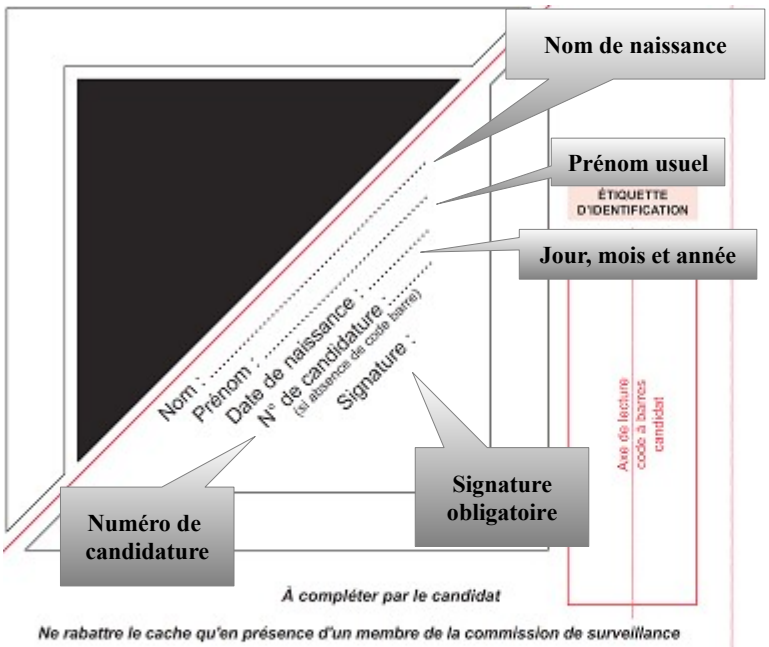
Sur les copies, les candidats devront écrire et souligner si nécessaire au stylo bille, plume ou feutre de couleur noire ou bleue uniquement. De même, l'utilisation de crayon surligneur est interdite.

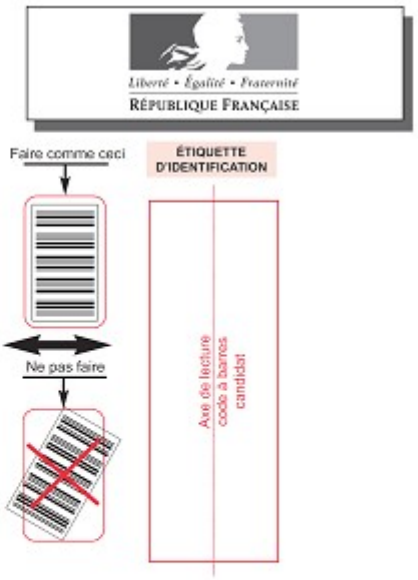
Il devra obligatoirement se conformer aux directives données.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Tournez la page S.V.P.

Le candidat complétera l'intérieur du volet rabattable des informations demandées et se conformera aux instructions données





Concours externe - interne - professionnel - ou examen professionnel (1)
(1) Rayer les mentions inutiles

Externe

Pour l'emploi de : **Inspecteur des Finances Publiques affecté au traitement de l'information en qualité d'analyste**

Épreuve n° : **3**

Matière : **051 - Version anglaise**

Date : **16/11/2021**

Nombre d'intercalaires supplémentaires :

Préciser éventuellement le nombre d'intercalaires supplémentaires

À L'ATTENTION DU CANDIDAT

En dehors de la zone d'identification rabattable, les copies doivent être totalement anonymes et ne comporter aucun élément d'identification tel que nom, prénom, signature, paraphe, localisation, initiale, numéro, ou toute autre indication même fictive étrangère au traitement du sujet.

Il est demandé aux candidats d'écrire et de souligner si nécessaire au stylo bille, plume ou feutre, de couleur noire ou bleue uniquement. Une autre couleur pourrait être considérée comme un signe distinctif par le jury, auquel cas la note de zéro serait attribuée. De même, l'utilisation de crayon surligneur est interdite.

Les étiquettes d'identification codes à barres, destinées à permettre à l'administration d'identifier votre copie, ne doivent être détachées et collées dans les deux cadres prévus à cet effet qu'en présence d'un membre de la commission de surveillance.

Suivre les instructions données pour les étiquettes d'identification

NOTE / 20 ,

RÉSERVÉ À L'ADMINISTRATION

À L'ATTENTION DU CORRECTEUR

Pour remplir ce document :
Utilisez un stylo ou une pointe feutre de couleur NOIRE ou BLEUE.

EXEMPLE DE MARQUAGE : Faire comme ceci — Ne pas faire

Pour porter votre note, cochez les gélules correspondantes.

Reportez la note dans les zones NOTE / 20 et dans le cadre A

En cas d'erreur de codification dans le report des notes cochez la case erreur et reportez la note dans le cadre B.

Cadre A réservé à la notation		
20	19	18
17	16	15
14	13	12
11	10	09
08	07	06
05	04	03
02	01	00
Décimales		
,00	,25	,50 ,75

Cadre B réservé à la notation rectificative		
20	19	18
17	16	15
14	13	12
11	10	09
08	07	06
05	04	03
02	01	00
Décimales		
,00	,25	,50 ,75
Erreur		

NOTE / 20 ,

EN AUCUN CAS, LE CANDIDAT NE FERMERA LE VOLET RABATTABLE AVANT D'Y AVOIR ÉTÉ AUTORISÉ PAR LA COMMISSION DE SURVEILLANCE

FINANCES PUBLIQUES

SUJET
Code matière : 051

Les candidates et les candidats peuvent avoir à leur disposition sur la table de concours le matériel d'écriture, une règle, un correcteur, des surligneurs.

NCSC offers teachers free cyber security training

The UK's National Cyber Security Centre (NCSC) has released a free cyber security training package for teachers and other school staff, setting out steps to take to help mitigate cyber-attacks and drawing on real-life case studies to demonstrate the impact of such incidents.

The resources are the newest addition to a widening package of support measures offered up by the NCSC as schools and universities across the UK reel from a spate of cyber-attacks, which began to surge as lockdowns forced the education sector to transition to remote learning, and have not let up even with the return of face-to-face teaching.

Sarah Lyons, NCSC deputy director for economy and society engagement, said: "It's absolutely vital for schools and their staff to understand their cyber risks and how to better protect themselves online. That's why we've created an accessible, free training package offering practical steps on cyber security to help busy professionals boost their defences.

The training package is designed to be accessible by any staff member, regardless of role or level of technical knowledge, and also comes as a scripted presentation. It can be accessed via the NCSC's website and shines a light on the most dangerous threats schools face, and outlines the impact successful cyber-attacks can have.

One of the case studies highlights an incident in which a successful voice phishing – or vishing – attack in which cyber criminals impersonated the Department for Education (DfE) to obtain the email details of the target's head of finance and headteacher. This was then used to target the headteacher with a personalised phishing email that, when opened, downloaded ransomware that spread across the network, encrypting the school's data. The ransomware gang demanded £8,000 for the decryption key.

In another example, cyber criminals targeted an independent school receptionist using phishing emails to steal the contact details of parents. The cyber criminals posed as an audit and compliance specialist. They then emailed the parents posing as the school itself, asking the parents to change the bank details to which they paid the school fees to those of an account controlled by the gang.

However, the incidents that affect schools are not always the work of malicious cyber criminals. In another case highlighted in the training package, a teacher left their system password written down on a post-it note, from where a pupil stole it and used it to access their laptop, and change their grades. The school was sanctioned for a breach of the Data Protection Act.

The package highlights four key steps school staff should take :

1. To defend themselves against phishing attempts by cutting down the amount of information on them publicly available on, for example, social media, being alert to suspicious emails, and seeking help if unsure of a request.
2. To use strong passwords that differ between accounts, protected by two-factor authentication where possible.
3. To secure devices, apply needed security updates, only download software from official sources, and lock screens when not in use.
4. To report suspicions as soon as possible.

***Computer Weekly*, 21 April 2021**