



**CONCOURS EXTERNE
DE CONTRÔLEUR DES FINANCES PUBLIQUES DE 2ÈME CLASSE
AFFECTÉ AU TRAITEMENT DE L'INFORMATION EN QUALITÉ DE PROGRAMMEUR**

ANNÉE 2024

ÉPREUVE ÉCRITE D'ADMISSIBILITÉ N° 3

Durée : 1 heure 30 – Coefficient : 1

Traduction d'un texte en anglais issu d'une revue ou d'une documentation informatique.

Seuls sont pris en compte les points obtenus au-dessus de 10/20.

*Le candidat trouvera au verso la manière de servir la copie dédiée.
Il devra obligatoirement se conformer aux directives données.*

NOTE AUX CANDIDATS

→ Passation de l'épreuve :

1. Sur les copies :

- vous devrez **composer lisiblement sur les copies avec un stylo foncé** : bleu ou noir. Toute copie illisible lors de la numérisation du fait d'une encre trop claire **ne sera pas corrigée (l'usage de stylo à encre effaçable est fortement déconseillé)** ;
- l'usage du surligneur et des stylos de couleurs est interdit ;
- pour toute correction, il est recommandé de privilégier **un correcteur type ruban** plutôt que liquide.

2. Vous devrez numéroté votre composition correctement dans l'encadré en haut de la copie.

Chaque numérotation doit contenir le numéro de la feuille et le nombre total de feuilles de votre composition. (Ex : 01/05 ; 02/05 ... 05/05).

3. Vous devrez, sur chaque feuille A3, remplir en **MAJUSCULES** toutes vos informations d'identification : Nom de naissance, Premier prénom, Numéro de candidature, rempli de gauche à droite, et Date de naissance.

Nom de naissance :	N	O	M																	
Premier prénom :	P	R	E	N	O	M														
Numéro candidature :	0	0	0	0	1	2	3	4		Né(e) le :	0	1	/	0	7	/	1	9	9	2
<small>(Le numéro est celui qui figure sur la convocation ou la feuille d'embarquement)</small>																				
<small>(Remplir cette partie à l'aide de la notice)</small>																				
Concours / Examen : Contrôleur programmeur externe des Finances publiques															Session : 2024					
Epreuve n° : 3										Matière : Anglais										
CONSIGNES															Feuille : <input type="text"/> / <input type="text"/>					
<ul style="list-style-type: none">• Remplir soigneusement, sur CHAQUE feuille officielle, la zone d'identification en MAJUSCULES.• Ne pas signer la composition et ne pas y apporter de signe distinctif pouvant indiquer sa provenance.• Numéroté chaque feuille A3 dans le cadre à droite et placer les feuilles dans le bon sens et dans l'ordre.• Rédiger avec un stylo à encre foncée (bleue ou noire) et ne pas utiliser de stylo plume à encre claire.• N'effectuer aucun collage ou découpage de sujets ou de feuille officielle. Ne joindre aucun brouillon.																				

4. Il ne doit pas y avoir de rature dans le pavé d'identification. Si nécessaire, vous pouvez demander une feuille vierge au responsable de salle.

5. Vous devrez composer uniquement sur les supports de composition officiels de l'épreuve : les feuilles de format A3 comportant le bandeau d'identification.

6. Notez que dans tous les cas, les feuilles ne doivent être ni découpées, ni agrafées, ni collées.

Les copies sont anonymisées lors des opérations de scannage. Ainsi, les correcteurs n'ont aucune information sur l'identité du candidat.

→ Lors de la collecte des copies :

Vous devrez rendre **uniquement les feuilles de composition officielles**. Tout autre support (sujet, brouillon) sera écarté de la correction.

ANGLAIS

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.

Genomics firm 23andMe investigates theft of sensitive customer data

Attackers stole personal data by guessing login credentials

Genetics firm 23andMe has initiated an investigation into an incident in which hackers leaked a substantial list of individuals with Ashkenazi Jewish ancestry, obtained without their consent from individual accounts on the platform.

The company claimed its systems remained uncompromised, and that the attackers acquired the data by guessing login credentials for a specific group of users.

Subsequently, they scraped additional information from a feature called DNA Relatives. This particular feature enables any account holder to search for potential genetic matches, regardless of how distant they may be. Users have the option to voluntarily share their information through DNA Relatives for others to access.

23andMe is a biotechnology and genomics firm based in the US. It provides popular genetic testing services to customers who submit a saliva sample to their laboratories, receiving in return a comprehensive report on their ancestry and genetic predispositions.

"We recently learned that certain 23andMe customer profile information that they opted into sharing through our DNA Relatives feature, was compiled from individual 23andMe.com accounts without the account users' authorisation," the firm stated in a post on its website.

"After learning of suspicious activity, we immediately began an investigation. While we are continuing to investigate this matter, we believe threat actors were able to access certain accounts in instances where users recycled login credentials - that is, usernames and passwords that were used on 23andMe.com were the same as those used on other websites that have been previously hacked."

In the initial data leak, the threat actor published one million lines of data specifically pertaining to individuals of Ashkenazi Jewish descent on dark-web site BreachForums. Later, on 4th October, the threat actor offered to sell data profiles in bulk at prices ranging from \$1 to \$10 per 23andMe account, depending on the quantity purchased.

The data exposed in this incident comprises complete names, usernames, profile pictures, gender, date of birth and geographic location. Additionally, it includes genetic ancestry information, such as individuals being identified as "broadly European" or "broadly Arabian" in descent.

Credential stuffing technique is widely used by hackers for compromising user accounts. It

enables them to infiltrate accounts by exploiting credentials that have been exposed in previous data breaches, especially when those same login credentials are reused.

The company is now urging its customers to take proactive measures to enhance the security of their accounts and passwords.

"Confirm you have a strong password, one that is not easy to guess and that is unique to your 23andMe account," it says.

Users are also being strongly recommended to enable multifactor authentication (MFA) for their 23andMe accounts.

"Review our Privacy and Security Checkup page with additional information on how to keep your account secure," 23andMe urged.

Dev Kundaliya, 09 October 2023, *Computing*

