

Esami di Stato 2009: la prova di lingua straniera

Un esempio di didattizzazione
della prova di francese



Patrizia Mauri

PL0A - ESAMI DI STATO DI LICEO LINGUISTICO

Tema di: LINGUA STRANIERA

TESTO DI ATTUALITÀ – LINGUA FRANCESE
(comprensione e produzione in lingua straniera)

Connaître les failles du numérique

Alors que le e-commerce et les puces électroniques ont envahi notre quotidien, plus de la moitié des Français se déclarent inquiets face aux risques liés aux nouvelles technologies.
Internet, le téléphone mobile, les cartes bancaires, la carte Vitale, les passeports biométriques

Le texte

Testo di attualità-lingua francese:

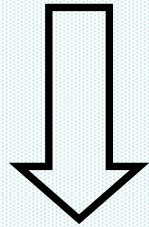
Connaître les failles du numérique

L'exercice

Le questionnaire

Étape 1

Observez le paratexte



- Le titre
- La source
- La date

pour situer ce que vous allez lire.

Étape 2

Lisez le questionnaire

- Il est important de lire d'abord toutes les questions pour qu'on puisse se faire une idée de ce qu'on demande et pour qu'on puisse faire une lecture sélective.
- Ne vous attardez pas sur des éléments du texte qui ne sont pas visés par les questions !



Étape 3

Lisez le texte

- Prenez votre temps pour lire le texte ! Essayez d'en comprendre le sens global.
- Ne cherchez pas dans le dictionnaire tous les mots qui ne sont pas clairs, bornez-vous plutôt aux mots-clés dont le sens est cryptique.
- Faites les repérages principaux sur le texte (à la lumière des questions lues à l'avance).



Étape 4



Posez-vous des questions
à propos du sens global
du texte.

Recherchez dans le
dictionnaire d'éventuels
mots obscurs.

- Qui ?
- Quoi ?
- Où ?
- Quand ?
- Comment ?
- Pourquoi ?

Étape 5

Considérez une
question après
l'autre:



Considérez la première question:

Expliquez l'expression « Le e-commerce et les puces électroniques ont envahi notre quotidien »

et faites des repérages dans le texte.

PL0A - ESAMI DI STATO DI LICEO LINGUISTICO

Tema di: LINGUA STRANIERA

TESTO DI ATTUALITÀ – LINGUA FRANCESE
(comprensione e produzione in lingua straniera)

Connaître les failles du numérique

Alors que le e-commerce et les puces électroniques ont envahi notre quotidien, plus de la moitié des Français se déclarent inquiets face aux risques liés aux nouvelles technologies.

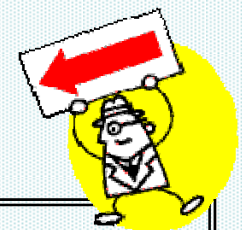
Internet, le téléphone mobile, les cartes bancaires, la carte Vitale, les passeports biométriques ... Toutes ces technologies véhiculent des informations, souvent confidentielles. Pourtant, à l'ère du commerce électronique (20 milliards d'euros de chiffre d'affaires en France en 2008) et de la banque en ligne, une nouvelle génération de malfaiteurs, les cybercriminels, tente d'intervenir dans les échanges pour s'enrichir. Avec un certain succès, semble-t-il ... 32 millions d'internautes dans notre pays et 56 millions de mobinautes sont concernés. Doivent-ils accorder une confiance aveugle à ces technologies, parfois difficiles à cerner, ou les refuser de peur d'être floués?

En découvrant les conclusions du panorama 2008 de la cybercriminalité présenté le 15 janvier 2009 par le Clusif (Club de la sécurité de l'information français, regroupant des professionnels de la sécurité numérique), il serait facile de céder à la panique. La multitude des failles de sécurité existantes (dont de nombreuses ont déjà été exploitées par des malfaiteurs), ainsi que les risques inhérents aux

Brouillon: prenez des notes qui constituent des éléments de réponse

- e-commerce → vente ou achat de biens et de services sur internet.
- puces électroniques → it : chip ; circuit intégré doté de capacité de connexions avec d'autres éléments
- envahir → connotation négative : occuper « brusquement, de vive force, de manière abusive »

Brouillon: rédigez votre réponse



- Faites des phrases courtes et claires pour mieux manipuler la langue étrangère.
- Veillez à ce que vos phrases soient cohérentes les unes après les autres.

Cette expression signifie que le e-commerce, c'est-à-dire la vente et l'achat sur Internet, et les puces électroniques, c'est-à-dire les microcircuits qui permettent de se connecter à un réseau, sont entrés de manière prépondérante dans notre vie, si bien qu'on ne peut plus s'en passer.

Vous pouvez ajouter des remarques plus fines sur la façon dont est écrit le texte :

L'emploi du verbe envahir donne une connotation négative à la phrase comme si le e-commerce et les puces électroniques s'étaient répandus de vive force, de manière abusive, sans qu'on s'en rende compte.

En effet, la plupart des français se préoccupent des dangers éventuels que les TICE pourraient cacher.



- Articulez vos réponses en paragraphes : allez à la ligne si vous passez à une idée nouvelle.
- Ne recopiez jamais le texte, mais paraphrasez et reformulez ! Si vous avez besoin de citer les mots du texte, mettez-les entre guillemets.



- Relisez le brouillon, corrigez les fautes de
 - Logique
 - Orthographe
 - Morphologie
 - Syntaxe
- Veillez aux choix lexicaux et, en cas de doute, cherchez dans le dictionnaire monolingue.



Considérez la quatrième question:

Court-on un risque lorsque l'on retire de l'argent dans un distributeur?

et faites des repérages dans le texte.

En découvrant les conclusions du panorama 2008 de la cybercriminalité présenté le 15 janvier 2009 par le C1usif (Club de la sécurité de l'information français, regroupant des professionnels de la sécurité numérique), il serait facile de céder à la panique. La multitude des failles de sécurité existantes (dont de nombreuses ont déjà été exploitées par des malfaiteurs), ainsi que les risques inhérents aux technologies émergentes, dessinent un portrait fragile de cette nouvelle économie bâtie autour du numérique. Sans oublier les bugs informatiques, comme celui du moteur de recherche Google qui, le 31 janvier, a indiqué pendant une heure que l'ensemble des sites mondiaux pouvaient «*endommager votre ordinateur*».

On peut distinguer deux types de circuits à risques: les circuits fermés (notamment les cartes bancaires) et les circuits ouverts (internet). Les premiers systèmes, utilisant des cartes à puce, apparaissent les moins sujets aux fraudes. En effet, les cartes bancaires, cartes Vitale, cartes SIM et passeports biométriques évoluent généralement en milieu fermé. La communication des informations intervient uniquement entre la carte et le lecteur et ne présente pas vraiment de faiblesse. Des tentatives pour «casser les codes» impliqueraient une dépense de temps et d'énergie trop importante, contre-productive pour le crime organisé. Il reste plus efficace de voler directement la carte bancaire d'une personne vulnérable avec ses identifiants. Certains malfaiteurs préfèrent d'ailleurs installer des caméras près des distributeurs pour enregistrer la saisie des codes.

Les menaces deviennent plus palpables lorsqu'on aborde le monde des réseaux, internet en première ligne. Tout le monde connaît l'existence de programmes malveillants, reçus par e-mail ou chargés sur des sites infectés, qui se glissent dans les ordinateurs pour subtiliser discrètement les codes et données confidentielles.

Mais de nombreuses autres techniques sont apparues, notamment les cartes de vœux piégées, les

Brouillon: prenez des notes qui constituent des éléments de réponse

- OUI on court des risques
→ Risque: danger éventuel
- Mots-clés: distributeur, caméra
- Saisie des codes → taper les codes
- Malfaiteur → criminel
- Enregistrer → filmer

Brouillon: rédigez votre réponse

Oui, on court des risques lorsqu'on retire de l'argent dans un distributeur puisque des criminels pourraient filmer le client qui tape son identifiant à l'aide d'une caméra cachée. Une fois le code secret obtenu, il ne leur reste qu'à voler la carte bancaire ou à la cloner.

Vous pouvez ajouter des remarques plus fines sur la façon dont est écrit le texte :

Pour échapper au danger il faut donc faire attention et protéger la saisie: on pourrait par exemple ériger à écran l'une des deux mains de façon à ce que la caméra ne puisse pas enregistrer les données sensibles du client.

Travaillez de cette manière pour toutes les questions, les unes après les autres.

Étape 6

Recopiez au propre!



- Écrivez de manière lisible. Celui qui vous lit ne doit pas se concentrer sur votre calligraphie, mais plutôt sur ce que vous avez écrit.
- Laissez une marge assez large pour les corrections.

Étape 7

Relisez encore une fois votre copie pour éliminer d'éventuelles fautes.



Parfois, quand on est fatigué, on ne voit plus les erreurs. Faites alors des lectures ciblées : une lecture pour vérifier les accords (sujet-verbe, article-substantif-adjectif), une pour vérifier les accents, une pour vérifier les relatifs et ainsi de suite. Laissez-vous guider par vos points faibles.

...et bon courage!