Sujet zéro n°6

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS
Sous-épreuve E12- Expression et communication en langue anglaise
Session 2021

Coefficient 1

Durée maximale de l'épreuve : 20 minutes
Préparation : 20 minutes

Déroulement de l'épreuve :

1) Expression orale en continu (5 minutes maximum)

   Présentation en anglais de l'analyse du dossier

2) Expression orale en interaction (15 minutes maximum)

   Échange en anglais avec l'examinateur à partir de l'analyse du dossier et des réponses apportées au questionnement accompagnant la mise en situation

L'usage d'un dictionnaire n'est pas autorisé.

Composition du dossier du candidat

Document A	**Texte :** Dumping passwords can improve your security – really?
Document B	**Capture d'écran** : OnlyKey
Document C	**Vidéo** : How to make a strong password
Mise en situation et questionnement	

Ce sujet comporte 4 pages. Il est conseillé au candidat de vérifier que le sujet est complet.

DOSSIER DU CANDIDAT : Passwords

Document A

Dumping passwords can improve your security – really?

Security keys, biometrics and a technology called FIDO are upgrading today's feeble security foundation.

Passwords suck.

They're hard to remember, hackers exploit their weaknesses and fixes often bring their own problems. Dashlane, LastPass, 1Password and other password managers generate strong and unique passwords for every account you have, but the software is complex. Services from Google, Facebook and Apple allow you to use your passwords for their services at other sites, but you have to give them even more power over your life online. Two-factor authentication, which requires a second passcode sent by text message or retrieved from a special app each time you log in, boosts security dramatically but can still be defeated.

A big change, however, could eliminate passwords altogether. The technology, called FIDO, overhauls the log-in process, combining your phone; face and fingerprint recognition; and new gadgets called hardware security keys. If it delivers on its promise, FIDO will make cringeworthy passwords like "123456" relics of a bygone age.

"A password is something you know. A device is something you have. Biometrics is something you are," said Stephen Cox, chief security architect of SecureAuth. "We're moving to something you have and something you are."

[…]

www.cnet.com 7 May 2020

Document B

OnlyKey

Image: Amazon

This key stores up to 24 passwords and can serve as a security key for an unlimited number of sites. It uses a pin number for access, so if you lose the physical key, no one can use the key to access sensitive information. OnlyKey automatically locks after a set period of time when it is plugged. If the key is stolen, all data is erased after 10 attempts to enter the pin. The key works with most websites, including Twitter, Facebook, GitHub, and Google and with Windows, macOS, and Linux devices.

$46 AT AMAZON

www.techrepublic.com

DOCUMENT C

How to make a strong password (1'37)

ESET, 2 June 2017

MISE EN SITUATION

You are an IT technician in a middle-sized company. Your manager is concerned about computer security. Discuss the different solutions.

QUESTIONNEMENT

- Strong passwords *vs* security keys?
- What solutions would you recommend?