Sujet n° 3

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS
Sous-épreuve E12- Expression et communication en langue anglaise
Session 2023

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 et de la situation en lien avec le secteur professionnel

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 <u>n'est pas</u> autorisé.

Composition du dossier du candidat

Document A	**Vidéo**: The passwordless future is here with Microsoft Security (1'25)
Document B	**Texte** : Small Businesses Are More Frequent Targets Of Cyberattacks Than Larger Companies
Document C	**Infographie** : Yubico review
Mise en situation et questionnement	

Ce sujet comporte 3 pages. Il est conseillé au candidat de vérifier que le sujet est complet.

DOSSIER DU CANDIDAT : CYBER ATTACKS ON SMALL BUSINESSES

Document A

Video: The passwordless future is here with Microsoft Security (1'25)

Microsoft Security, September 5, 2021

Document B

Small Businesses Are More Frequent Targets Of Cyberattacks Than Larger Companies: New Report

When it comes to avoiding cyberattacks, bigger is apparently better. At least that's according to a new report that shows small businesses are three times more likely to be targeted by cybercriminals than larger companies.

Between January 2021 and December 2021, researchers at cloud security company Barracuda Networks analyzed millions of emails across thousands of companies. They found that, on average, an employee of a small business with less than 100 employees will experience 350% more social engineering attacks than an employee of a larger enterprise.

According to the report, "Hackers target high-value accounts for takeover. Accounts of CEOs and CFOs are almost twice as likely to be taken over compared to average employees. Once they have access, cybercriminals use these high-value accounts to gather intelligence or launch attacks within an organization.

"Executive assistants are also a popular target as they often have access to executive accounts and calendars and usually can send messages out on behalf of executive teams."

Edward Segal, www.forbes.com, March 30, 2022

Document C

ReviewsPlus

yubico

ABOUT THE BRAND

Despite the increasing complexity of passwords, over 17 million login credentials are compromised every day! It's no wonder that many platforms, services, and servers encourage users to set up a second way to authenticate, such as email verification codes, text messages, one-time passwords, or biometric data.

Yubico Security Key. The YubiKey by Yubico makes accessing password-protected accounts a breeze. Simply hold the YubiKey up to your phone to enter instead of going through 2-Factor Authentication! Here, we'll get into the specifics about Yubico.

Yubico Review

PROS & CONS

- Makes managing multiple online accounts easier
- Provides password protection
- Budget-friendly options
- 1-year warranty
- Shipping not available to some countries
- Some users may experience difficulty in setting up & learning to use

PRODUCTS

YubiKey 5 NFC

$45.00

Security Key by Yubico

$20.00

YubiKey FIPS

$46.00

OVERALL RATING

4.5/5.0

YubiKeys from Yubico are a worthy choice for anyone looking for a little more security with their online accounts. They are small and discreet, but provide a wealth of value. Avoid 2-Factor Authentication and secure your passwords with one of the YubiKeys listed above. From budget options up to government-level security, Yubico has a security key for any level of use.

reviewsplus.co

MISE EN SITUATION

The manager of the small company where you work is worried about cyberattacks. He asks you to inform the staff about account protection.

QUESTIONNEMENT

What is the problem with passwords?

What are the main risks regarding computer security?

What measures can a company implement to face these threats?