Sujet zéro n°1

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 :** Coronavirus stimulus scams are here. How to identify these new online and text attacks
Document B	**Vidéo** : Cyber security when working from home
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 : Cybersecurity

Document A

Coronavirus stimulus scams are here. How to identify these new online and text attacks

COVID-19 fears are fertile ground for malicious actors. Here's how to stay safe online.

As with any public crisis, the spread of the coronavirus has created a new crop of hackers targeting people […] who are working from home and who are just trying to stay healthy. […] You need to be on guard against all kind of scams and misinformation found online, in your email inbox and even in your text messages.

A recent release from the FBI's Internet Crime Complain Center offers some solid advice on what to watch out for. "Scammers are leveraging the COVID-19 pandemic to steal your money, your personal information, or both. Don't let them," the FBI said. "Protect yourself and do your research before clicking on links purporting to provide information on the virus; donating to a charity online or through social media; contributing to a crowdfunding campaign; purchasing products online; or giving up your personal information in order to receive money or other benefits."

[...]

Meanwhile, researchers at Trustwave found that ransomware attacks amounted to 18% of overall breach incidents observed in 2019, up from 4% in 2018. Researchers also found the amount of malware in traditional spam email declined to 0.2% from 6% the previous year, as attackers look for more effective infection vehicles. The biggest rise was in social engineering attacks, like phishing. In 2018, Trustwave analysts found 33% of all data breach incidents were the result of phishing or social engineering attacks. In 2019, that number rose to half.

Rae Hodge, www.cnet.com April 27, 2020

Document B

Cybersecurity practices when working from home, 41 Action news, www.kshb.com (1’40)

MISE EN SITUATION

You are an IT technician in an accounting firm whose 40 employees work from home because of Covid-19 lockdown. She worries they might be targeted by scammers and she wonders if there are software and hardware solutions to protect both the firm’s sensitive data and her employees.

QUESTIONNEMENT

- How can a company make sure its data is safe when the staff are working from home?
- How efficient is an antivirus?
- How useful can a data protection charter be?