Sujet n° 14

**BTS SERVICES INFORMATIQUES AUX ORGANISATIONS**
**Sous-épreuve E12- Expression et communication en langue anglaise**
**Session 2024**

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 de la mise en situation

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

**Composition du dossier du candidat**

| | |
|---|---|
| **Document A** | **Texte** : FBI warns consumers not to use public phone charging stations |
| **Document B** | **Vidéo** : Mobile security dangers |
| **Document C** | **Infographie** : Tips for getting a hacker off your phone |
| **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 : PHONE HACKING**

**Document A**

### FBI warns consumers not to use public phone charging stations

The FBI is warning consumers against using public phone charging stations in order to avoid exposing their devices to malicious software.

Public USB stations like the kind found at malls and airports are being used by bad actors to spread malware and monitoring software, according to a tweet last week from the FBI's Denver branch.

"Carry your own charger and USB cord and use an electrical outlet instead," the agency advised in the tweet. "Just by plugging your phone into a compromised power strip or charger, your device is now infected, and that compromises all your data."

The cord you use to charge your phone is also used to send data from your phone to other devices. For instance, when you plug your iPhone into your Mac with the charging cord, you can download photos from your phone to your computer.

If a port is compromised, there's no limit to what information a hacker could take. That includes your email, text messages, photos and contacts.

The Federal Communications Commission also updated a blog post on Tuesday warning that a corrupted charging port can allow a malicious actor to lock a device or extract personal data and passwords.

"In some cases, criminals may have intentionally left cables plugged in at charging stations," according to the FCC blog post. "There have even been reports of infected cables being given away as promotional gifts."

Jennifer Korn, *cnn.com*, April 12, 2023

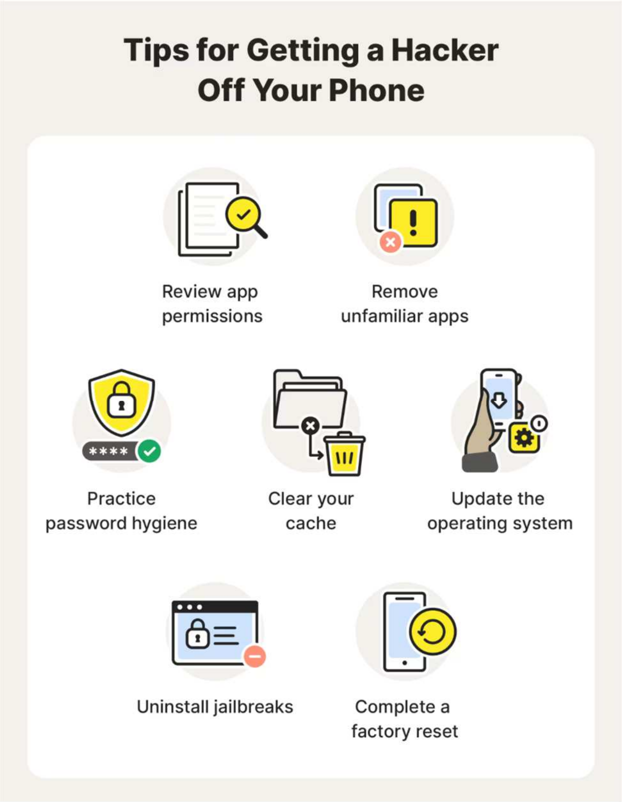
## Document B

**Vidéo** : Mobile security dangers

https://www.youtube.com/watch?v=L-9gmnwrba0

Cyber news, June 29, 2023

## Document C



Tips for Getting a Hacker Off Your Phone

Review app permissions

Remove unfamiliar apps

Practice password hygiene

Clear your cache

Update the operating system

Uninstall jailbreaks

Complete a factory reset

*us.norton.com*, July 12, 2023

## MISE EN SITUATION

You are an IT technician working for a small company. Your manager has allowed the employees to use their phones to work. He wants you to give him information about the security risks and how to protect the company's sensitive data.

## QUESTIONNEMENT

How can a phone be hacked?
How can you protect the company's data from cyberattacks?
What should you do if an employee's phone gets hacked?