**BTS SERVICES INFORMATIQUES AUX ORGANISATIONS**
**Sous-épreuve U12- 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** | **Vidéo :** Hack Attacks Rise During Coronavirus Crisis, Says Crowdstrike CEO (1'33) |
| **Document B** | **Texte :** Businesses believe the pandemic will change the security landscape forever |
| **Document C** | **Capture d'écran** : Phishing notice |
| **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 : Covid 19, Teleworking and Cybersecurity

## DOCUMENT A

Hack Attacks Rise During Coronavirus Crisis, Says Crowdstrike CEO (1’33)

Bloomerg Technology 26 March 2020

## DOCUMENT B

### Businesses believe the pandemic will change the security landscape forever

Remote workers could pose a serious threat to cybersecurity.

[...]

The pandemic has forced many workers to embrace the home office, and a large proportion are expected to continue working in that manner even after the pandemic subsides.

With this in mind, examining how remote employees approach cybersecurity will become paramount if an organisation is to maintain a strong security posture.

A third of respondents said they worry employees may feel more relaxed about cybersecurity than when they are working out of the office. Employees may also be less likely to follow protocol at home, particularly when it comes to identifying and flagging suspicious activity.

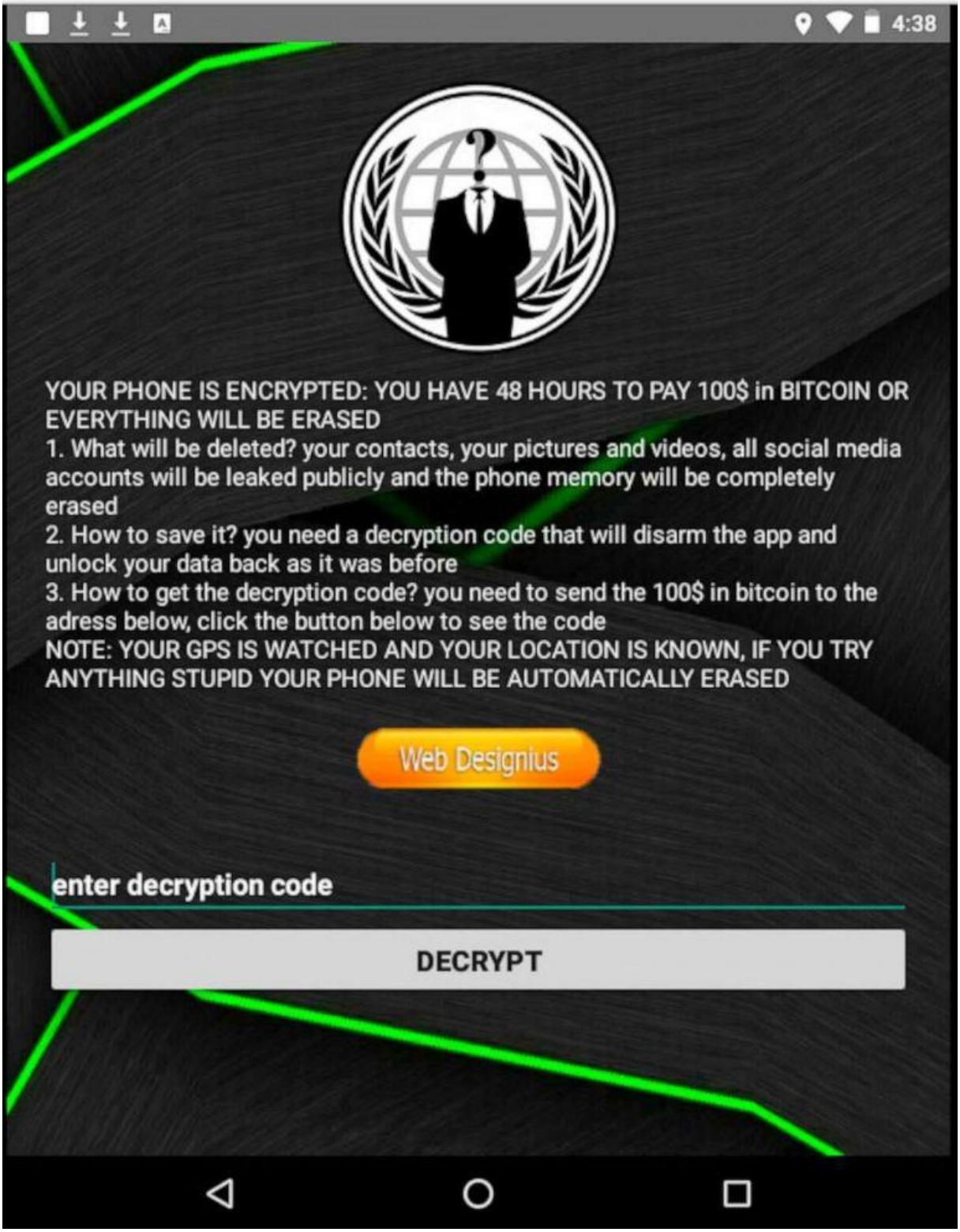
Further, almost a third (31 percent) fear employees might unintentionally leak sensitive data or fall prey to a phishing scam and a quarter are afraid staff might fall victim to malware attacks.

Of the largest risks associated with remote working, respondents singled out “using untrusted networks” as the most significant. Other people accessing employees' company devices, the use of personal messaging services for work, and the unintentional sharing of company data are also high on the list of risks.

Sead Fadilpašić, www.itproportal.com 19 June 2020

**DOCUMENT C**

*Cybersecurity experts have identified a new app that masquerades as a coronavirus tracker in order to infect devices with ransomware.*




www.abcnews.go.com 19 March 2020

**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?
- What about data security when the staff are working from home?
- How efficient is an antivirus?