**MENTION COMPLÉMENTAIRE**

**SERVICES NUMÉRIQUES AUX ORGANISATIONS**

**SESSION 2023**

**ÉPREUVE E3**

**ACCOMPAGNEMENT DES UTILISATEURS**

**AUX USAGES DU NUMÉRIQUE**

**Phase A : Production d’une ressource**

Durée : 2 h

L’usage de tout modèle de calculatrice avec mode examen actif est autorisé.

L’usage de la calculatrice sans mémoire « type collège » est autorisé.

Aucun document n’est autorisé.

**Une ressource numérique sous format pdf doit être rendue à l’issue de l’épreuve sur clef avec un nommage de fichier permettant d’identifier le candidat.**

Ce sujet se compose de 5 pages numérotées de 1/5 à 5/5

Dès que le sujet vous est remis, assurez-vous qu'il est complet.

L’entreprise Channel Logistics est spécialisée dans le transport de marchandises entre la France et l’Angleterre.

L’effectif de 52 salariés est réparti entre la société mère située à Londres et la succursale basée à Calais.

Ces localisations sur territoire anglais et français permettent un maillage logistique optimal et un accès stratégique aux grands axes autoroutiers.

Elle dispose de moyens techniques et d’outils logistiques parmi les plus innovants : camions de nouvelle génération, plusieurs entrepôts de stockage, outils informatiques performants…

L’entreprise est équipée d’un logiciel métier type PGI (Progiciel de Gestion Intégré) permettant de gérer l’ensemble des processus. Le module TMS *(Transport Management System)* y est intégré. Ce module supervise l’ensemble du transport : planification des flux, plan de transport, gestion des tournées, matériel roulant, temps de conduite, etc.

Les salariés reçoivent régulièrement dans leur messagerie professionnelle des tentatives d'hameçonnage (*phishing*) et des rançongiciels (*ransomware)*. La direction craint des vulnérabilités pour son système d’information.

Des salariés ont transmis récemment au service informatique des courriels pour lesquels ils émettent des doutes.

Aussi, la direction souhaite alerter et faire adopter les bons gestes à ses collaborateurs sur les règles d’hygiène numérique concernant la gestion des courriels.

Vous êtes sous la responsabilité de Madame Maude DUVAL chargée de projets informatiques et déléguée à la protection des données au sein du service informatique. Vous avez en charge l’élaboration d’un guide de bonnes pratiques à destination des collaborateurs français. Vous avez à votre disposition une documentation, en anglais, envoyée par la société mère ainsi que des courriels reçus par les salariés.

**Travail à faire :**

* **Réaliser ce guide à destination des utilisateurs dans un format pdf**

**Documents du sujet à votre disposition :**

* Document 1 : Don’t be that employee: How to avoid ransomware attacks at work
* Document 2 : Courriels reçus par des salariés

**Documents numériques à disposition :**

* Images des documents 1 et 2 au format numérique (.png)

**Document 1 : Don’t be that employee: How to avoid ransomware attacks at work**

[…]

Ransomware, which locks down a target’s computers and data, can infect a network a few different ways, including through employee accounts. Click the wrong link, open the wrong attachment or log into the wrong website, and you could put your company in a perilous position. (…)

If an email arrives promising a bonus you didn’t know you were receiving, you probably aren’t receiving it. Hackers use whatever is most likely to get clicks, so get familiar with some classic phishing lures [[1]](#_ftn1), like an “accidental” email from HR with an attachment titled “**Companywide salaries.**” Fake Amazon gift cards and DocuSign links are also popular, says Peter Quach, director of client relations at security firm Polito. (…)

Hackers also prey on[[2]](#_ftn2)people’s tendency to defer to authority. Fake emails from CEOs or senior executives asking for account credentials[[3]](#_ftn3)— or wire transfers — are a common tactic.

This is an emergency. I need you to send it. But you can’t tell anybody because it’s a very secret project, and I only trust you.’ Using the typical con[[4]](#_ftn4)tactics to make you feel like, ‘Okay, I’m in on something really special,’ ” says Allan Liska, a senior threat analyst at cybersecurity firm Recorded Future. (…)

Cybercriminals might also just pick up the phone, pose as a colleague and ask you for account information. Always authenticate requests[[5]](#_ftn5)through another channel, or check with IT.

What if you’ve already opened a phishing link or attachment?

You might feel tempted to pretend like nothing happened and hope no one notices. But don’t do that.

“That is often the first reaction, and it is not ideal,” Kalember says. “When you fall for something, the attacker still has some window of time where they have to figure out what they’ve just got and whether it’s even worth taking advantage of.”

That gap[[6]](#_ftn6)— or dwell time, in industry lingo — is incredibly valuable for your company’s IT team. If you report what happened right away, odds[[7]](#_ftn7)are you’re in line with your company’s security policies and have little to worry about. Phishing emails are common, and it’s tough to expect employees to get it right 100 percent of the time.

But if you brush the incident under the rug[[8]](#_ftn8), it could come back to haunt you. When ransomware attackers use phishing to access company networks, they do so through a compromised employee account. By reporting your encounter with a phishing email, you distance yourself from any subsequent malicious activity coming from your accounts.

As far as repercussions for clicking on malicious links and attachments — and potentially opening up the company to ransomware — things get stickier. If the company hasn’t taken steps to train employees and protect its network, it’s tough to pin an attack on any one employee, Quach says. When that kind of scapegoating[[9]](#_ftn9)does happen, it’s usually reserved for high-level executives or IT professionals. (…)

Companies want to incentivize[[10]](#_ftn10)employees to report malicious emails and security mistakes, and if there are any consequences, it might look more like attending extra training or losing administrative privileges on your device.

Keep a copy of your IT team’s email address somewhere easy to find, and contact the team if something seems fishy. Don’t delete the email you clicked on, and don’t unplug your computer or turn off WiFi.

Source : washingtonpost.com – Ransomware attack avoid

|  |  |
| --- | --- |
| [[1]](#_ftnref1) Lures: appâts  [[2]](#_ftnref2) Prey on : s’attaquer  [[3]](#_ftnref3)Credentials: références  [[4]](#_ftnref4) Con: escroquerie  [[5]](#_ftnref5)Requests: demandes | [[6]](#_ftnref6) Gap: intervalle  [[7]](#_ftnref7) Odds: probabilité  [[8]](#_ftnref8) Rug: tapis  [[9]](#_ftnref9)Scapegoating: désigner comme bouc émissaire  [[10]](#_ftnref10)Incentivize : encourager |

**Document 2 : Courriels reçus par des salariés**

