|  |  |
| --- | --- |
| Mission 6 – Sensibiliser le personnel à la sécurité des échanges(Entraînement à l’épreuve au 6) | Une image contenant disque compact, cercle, Graphique, graphisme  Description générée automatiquement |
| Durée : 50’ | Homme avec un remplissage uni | Une image contenant symbole, Bleu électrique, Police, Graphique  Le contenu généré par l’IA peut être incorrect. | Source |

**Contexte professionnel**

L’entreprise CATADOM est spécialisée dans l’anodisation de l’aluminium, un procédé de traitement de surface par électrochimie qui permet de modifier les propriétés du métal afin de renforcer sa résistance à la corrosion, tout en améliorant son aspect esthétique.

Reconnue pour son savoir-faire et sa réactivité, CATADOM collabore principalement avec des décolleteurs et des emboutisseurs de pièces en aluminium, au service de secteurs exigeants tels que l’automobile, la parfumerie, le luxe, le sport ou encore l’industrie navale.

Mme Gonzalez (directrice) a récemment rencontré,le directeur de la société Etesia, qui lui a fait part des graves conséquences d’une cyberattaque subie par son entreprise. Cette attaque a fortement perturbé son fonctionnement et entraîné des pertes importantes (**document 1**).

**Travail à faire**

Ces témoignages ont sensibilisé Mme Gonzalez à l’importance de la cybersécurité et de la prévention des risques liés aux rançongiciels. Elle souhaite alerter et mobiliser l’ensemble du personnel sur ce sujet crucial.

1. Elle vous charge de rédiger une note, d’une page, destinée au personnel afin de les sensibiliser à ces risques.
2. Elle souhaite organiser une formation du personnel. Vous devez rédiger la demande de devis qui sera envoyée à différents organismes de formation (20 salariés sont concernés par la formation).

**Doc. 1 Espaces verts : Etesia tente de se relever de sa cyberattaque**

*Source : https://www.lesechos.fr/ - avr. 2024 - Bénédicte Weiss*

**Le spécialiste alsacien du matériel professionnel d'entretien des espaces verts a été placé en redressement judiciaire, après avoir subi une cyberattaque en février. Son activité se remet progrès-sivement en place.**

En ce matin de février 2024, ne parvenant pas à accéder à leurs mails ni à téléphoner, les équipes d'Etesia ont d'abord cru à une panne informatique. Dans les heures qui ont suivi, tous les services, de la production à l'administratif, peinant à lancer leurs machines, ce spécialiste du matériel d'entretien des espaces verts basé à Wissembourg (Bas-Rhin) a dû se rendre à l'évidence : il avait été victime d'une attaque informatique. Toutes les données de ses serveurs ont été cryptées, y compris celles de ses serveurs de secours.﻿

Près de deux mois après, l'enquête suit son cours et aucune rançon n'a été versée aux pirates. Thomas Meyer, le président de cette PME qui réalise 48 millions d'euros de chiffre d'affaires, ﻿a bon espoir que l'activité reprenne pleinement dans les prochaines semaines. Mais étant dans l'incapacité d'honorer les créances de la fin février, l'entreprise a été placée début mars en redressement judiciaire pour six mois, soit jusqu'au 1er août. De quoi espérer reconstituer la trésorerie grâce à la reprise des expéditions, avec la volonté affichée de ne se séparer d'aucun de ses quelque 200 salariés. **[…]**

**Doc. 2 3Fuite de données : une autre grande entreprise française touchée**

*Source : https://www.cafebabel.fr/*

Depuis le début de l’année 2024, il ne se passe pas un seul mois sans qu’une institution publique ou une entreprise privée ne soit victime d’une cyberattaque. Après SFR en septembre et Free en octobre, une autre grande enseigne vient d’être victime d’une fuite de données massive, en ce mois de novembre.

**385 000 cas de cyberattaques recensés en France chaque année**

Picard vient d’être ajouté à la longue liste des victimes de cette interminable vague de **cyberattaques** qui cible les administrations et les entreprises françaises depuis plusieurs mois. Chaque année, pas moins de 385 000 cas de cyberattaques sont recensés un peu partout en France, selon un rapport réalisé par l’*école de cybersécurité Jedha Bootcamp*.

**Entreprises et institutions victimes de cyberattaque en 2024**

Une situation qui ne fait que s’intensifier au fil du temps. Cette année 2024, les **cybercriminels** ne chôment pas. Depuis janvier, le nombre d’entités victimes ne cesse d’augmenter : le CHU de Nantes, le Conseil départemental de la Sarthe, Viamedis, Almerys, Etesia, Sidaction, Centre hospitalier d’Armentières, Caisse d’Allocations Familiales, 800 services de l’État français en ligne, Lycées d’Île-de-France, France Travail (ex-Pôle emploi), Fédération Française de Football (FFF), etc.

**45 000 données volées :** c’est à présent l’enseigne de surgelés Picard qui a été visée par les pirates informatiques. Une fuite de données personnelles qui concerne, selon le dernier communiqué de l’entreprise française en date du mardi 12 novembre 2024, 45 000 de ses clients inscrits dans son programme fidélité. « *Nous avons détecté, […] un accès non autorisé par des tiers* », informe l’entreprise dans un message envoyé par e-mail aux clients concernés. En effet, les pirates ont réussi à siphonner les noms et prénoms, les dates et lieu de naissance, avec des adresses postales, des e-mails, des coordonnées téléphoniques ainsi que les identifiants de carte de fidélité. […]

**Doc.3 Cinq conseils pour se prémunir contre les rançongiciels**

*Source :  Bercy Infos, le 11/10/2024*

Vous avez reçu un message douteux contenant des pièces jointes ? Vous avez retrouvé une clé USB ? Gare aux rançongiciels ! Vos données peuvent-être chiffrées et prises en otage contre rançon. Voici cinq conseils pour minimiser les risques.

**Qu’est-ce qu'un rançongiciel ?** Les rançongiciels, ou *ransomware*, désignent des programmes informatiques malveillants. Il s’agit de mettre votre ordinateur ou votre système d’information hors d’état de fonctionner de manière réversible en chiffrant vos données. L’objectif ? Vous inciter à envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.

**Conseil n°1 : n’ouvrez pas les messages dont la provenance ou la forme est douteuse.** Ne vous laissez pas tromper par un simple logo. Les pirate*s (hacker)* peuvent avoir récupéré certaines de vos données préalablement (les noms de vos clients par exemple) et créé des adresses de messagerie ressemblant à un détail près à celles de vos interlocuteurs habituels**.** Restez donc très vigilants, car certains messages paraissent tout à fait authentiques. Vous avez un doute ? Contactez l'expéditeur par un autre canal de communication, par un appel téléphonique par exemple.

**Conseil n°2 : apprenez à identifier les extensions douteuses des fichiers :** Vous recevez habituellement des fichiers en .doc ou .mp4 (par exemple) et le fichier du message dont vous avez un doute se finit par un autre type d’extension ? Ne les ouvrez surtout pas ! Voici quelques exemples d'extensions douteuses : .pif, .com, .bat, .exe, .vbs, .lnk, etc. Attention également à l’ouverture de pièces jointes de type .scr ou .cab. il s’agit d’extensions de logiciels malveillants .

**Conseil n°3 : effectuez des sauvegardes régulières de vos données :** Pensez à régulièrement sauvegarder les données de vos différents appareils. Vous pourrez ainsi les récupérer en cas d'attaque.

**Conseil n° 4 : mettez à jour régulièrement vos principaux outils :** Traitement de texte, lecteur PDF, navigateur mais aussi antivirus…. Si possible, désactivez les macros des solutions de bureautique qui permettent d’effectuer des tâches de manière automatisée. Ceci évite la propagation des rançongiciels *via* les vulnérabilités des applications. En générale, les systèmes d'exploitation qui ne sont plus mis à jour, donnent aux attaquants un moyen d'accès plus facile à vos systèmes.

**Conseil n° 5 : utilisez un compte « utilisateur » plutôt qu’un compte « administrateur » :** Évitez de naviguer depuis un compte administrateur. L’administrateur d’un ordinateur dispose de droits supplémentaires sur celui-ci, comme réaliser certaines actions ou accéder à des fichiers cachés de votre ordinateur. En privilégiant l’utilisation d’un compte utilisateur, cela ralentira, voire dissuadera le voleur dans ses actions malveillantes.

**Doc. 4 Recommandations de l’ANSSI : Comment se prémunir d’une cyberattaque ?**

*Source : https://www.info.gouv.fr/*

**Soyez vigilant** : les demandes autoritaire ou intimidante, par email ou *SMS*, dissimulent parfois des tentatives d’arnaques.

- Vous recevez un email du Trésor public vous demandant de fournir vos coordonnées bancaires pour un remboursement.

- Un service de transport vous demande par *sms*de cliquer sur un lien pour régler les taxes douanières d’un colis.

- Vous recevez un email de la gendarmerie vous accusant d’un délit et vous demandant de répondre sous peine de poursuites.

**1. Utilisez des mots de passe robustes :** L’un des premiers réflexes consiste à définir des **mots de passe robustes,** à la fois difficiles à trouver par un système automatisé et à deviner pour une tierce personne. Privilégiez des mots de passe longs, complexes et composés avec différent types de caractères (chiffres, majuscules, minuscules et caractères spéciaux).

**2. Préservez votre identité numérique :** Préservez votre identité numérique en vous **montrant vigilant en ligne et les réseaux sociaux**: prenez soin de vos données personnelles et ne communiquez pas vos informations sensibles (numéro de téléphone, adresse ou numéro de carte bleue).

**3. Protégez votre messagerie :** vous recevez un message d’un partenaire, dont le contenu est étonnant (un titre en anglais ou dans une autre langue, une demande inhabituelle, des fautes d’orthographe), Soyez prudent. L’identité de l’expéditeur peut être usurpée. Soyez attentif aux indices mettant en doute l’origine d’un courriel : incohérence de forme ou de fond avec les messages habituels. Dans le même sens, ne répondez pas aux demandes suspectes d’expéditeurs inconnus.

* Les demandes d’informations confidentielles sont rarement faites par courriel. Soyez donc attentifs à ces tentatives dites d’hameçonnage, aussi appelées *phishing*. (exemple, le règlement de vos impôts se fait sur le site impots.gouv.fr : le Trésor public ne vous demandera jamais vos coordonnées bancaires par courriel.
* Vérifiez les liens qui figurent dans vos courriels avant de cliquer dessus. Si vous avez un doute, saisissez vous-même l’adresse du site dans la barre d’adresse du navigateur.
* Assurez-vous également qu’en passant la souris au-dessus du lien proposé, l’adresse du site soit conforme à l’expéditeur annoncé. Souvent, le contenu des sites frauduleux comporte des fautes de français, mais de plus en plus, les tentatives d’hameçonnage emploient un français correct.
* Soyez vigilant avant d’ouvrir les pièces jointes. Elles constituent le principal vecteur d’attaque et peuvent véhiculer des programmes malveillants.

**4. Mettez à jour vos équipements :** Votre ordinateur doit être équipé d’un antivirus efficace, ainsi que d’un système d’exploitation et de logiciels à jour pour se protéger des cyberattaques. Les hackers ciblent les ordinateurs utilisant des logiciels qui ne sont pas à jour pour exploiter les vulnérabilités non corrigées.

**5. Évitez la connexion aux réseaux non sécurisés :** Évitez les réseaux publics ou inconnus. En déplacement, privilégiez la connexion de votre abonnement téléphonique (3, 4 ou 5G). Les réseaux Wi-Fi publics sont souvent mal sécurisés, et peuvent être contrôlés ou usurpés par des pirates qui peuvent lire et capturer vos informations personnelles ou confidentielles (mots de passe, numéro de CB...). Si vous n’avez d’autre choix que d’utiliser un Wi-Fi public, veillez à ne jamais y réaliser d’opérations sensibles et utilisez si possible un réseau privé virtuel (VPN).

**6. Sauvegardez régulièrement vos données :** Enfin, il faut penser à sauvegarder vos fichiers régulièrement sur un support externe à votre équipement (clé ou disque USB) que vous débranchez une fois la sauvegarde effectuée. En cas de piratage de votre ordinateur, vous risquez de perdre des données (photos, fichiers, contacts, messages…).