TotalEnergies

1. La gestion de mes mots de passe

Une bonne pratique pour se prémunir :

- **De l'usurpation de mon identité** suite à la découverte ou au vol d'un de mes mots de passe.
- **Du vol de mes données**.
- **De la destruction de données** ou de systèmes d'information par des actions malveillantes réalisées avec mes autorisations.

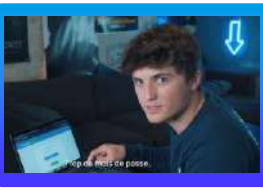
En chiffres

~ 890 000

Mots de passe volés par jour.
(source : Hasso Plattner Institute)

10 millisecondes

Temps nécessaire pour déchiffrer un mot de passe de 6 lettres minuscules.
(source : howsecureismypassword.net)



Vidéo

MICODE #1
LA GESTION DE MES MOTS DE PASSE

Voilà l'exemple à ne pas suivre

LA BONNE PRATIQUE EST AU VERSO ▶

Cette histoire est une parodie, toute ressemblance avec des personnes ou des situations existantes ou ayant existé ne serait que pure coïncidence.

1. La gestion de mes mots de passe

J'utilise des mots de passe **robustes et différents** pour chacun de mes comptes.

Je les garde secrets en les stockant dans un **gestionnaire de mots de passe.**

En pratique

Je crée un mot de passe robuste

- Composé d'au moins 12 caractères.
- En évitant de définir mon mot de passe à partir d'informations rendues publiques sur les réseaux sociaux.
- Je protège l'accès à mon Smartphone en utilisant un code PIN à 6 chiffres minimum, même si j'utilise la fonctionnalité Touch ID ou Face ID.

Je choisis des mots de passe différents selon les services utilisés

- En cas d'attaque informatique, cela évitera aux cybercriminels d'accéder aux autres services utilisés.
- En particulier, je n'utilise pas les mêmes mots de passe dans ma vie privée et professionnelle.

Je protège mes mots de passe

- Je les conserve dans le logiciel de stockage de mots de passe recommandé par la Compagnie (KeePass). Je ne les inscris pas ailleurs.
- Je ne les communique à personne.
- Je les change immédiatement si je suspecte une compromission.
- Je ne divulgue jamais (réseaux sociaux,…) les questions « secrètes » et leurs réponses permettant de les réinitialiser.

Liens utiles

KEEPASS vous aide à construire des mots de passe robustes et les retient pour vous **en savoir plus et l'utiliser**

En savoir plus sur la gestion de mes moyens d'authentification

voir la page Infosec

Vidéo

CYBERSECURITY MOMENT
What's your password ?

Edité par DSI/CYB – sept. 2021

2. L'hygiène informatique de mes équipements

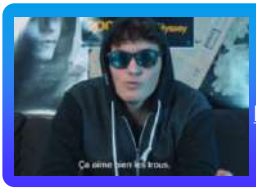
Une bonne pratique pour se prémunir :

De vulnérabilités sur mes équipements.
Cela me garantit une protection efficace.

En chiffres

En moyenne, dans le monde
11 vulnérabilités
critiques sont découvertes chaque jour !
(source : cvedetails.com)

Pour plus de 50 %
des vulnérabilités des applications web, il existe un code d'exploitation rendant possible une attaque.
(source : Imperva report)



Vidéo
MICODE #2
L'HYGIÈNE INFORMATIQUE DE MES ÉQUIPEMENTS

Voilà l'exemple à ne pas suivre

LA BONNE PRATIQUE EST AU VERSO ▶

Cette histoire est une parodie, toute ressemblance avec des personnes ou des situations existantes ou ayant existé ne serait que pure coïncidence.

2. L'hygiène informatique de mes équipements

Je veille à la **mise à jour** de mes ressources informatiques dès la mise à disposition de correctifs.

En pratique

Sur les terminaux fournis par TotalEnergies

- J'applique dans les plus courts délais les mises à jour proposées par les services IT de la Compagnie.
- J'utilise les services mis à disposition par la Compagnie. Pour un nouveau besoin, je sollicite le support informatique.

Sur mes terminaux personnels

- Je mets à jour sans tarder l'ensemble de mes appareils (fixes et mobiles) et logiciels.
- Je télécharge les mises à jour uniquement depuis les sites officiels.
- J'active l'option de téléchargement et d'installation automatique des mises à jour.
- Lorsque je me sépare d'un de mes équipements, je le réinitialise aux paramètres d'usine (effacement de toutes mes données).

Fiche INFOSEC

SÉCURISER SON SMARTPHONE ET SA TABLETTE

Vidéo

REX RANÇONGICIEL HUTCHINSON

Vidéo

CYBERSECURITY MOMENT
Security Updates

3.
La Cybersécurité de mes projets

Une bonne pratique pour se prémunir :

- **D'une potentielle Cyberattaque** sur un produit / service non sécurisé (et des amendes pour non-conformité).
- **D'une atteinte à la réputation de la Compagnie** (perte de confiance clients).
- **De coûts et de délais supplémentaires** pour sécuriser à posteriori.

En chiffres

84 % des organisations
exploitant des objets connectés ont connu des incidents de Cybersécurité liés à ces derniers.
(source : safeatlast.co)

575 millions d'Euros
d'amende pour Equifax après un vol massif de données, lié à une application mal sécurisée.
(source : csoonline.com)

Voilà l'exemple à ne pas suivre

LA BONNE PRATIQUE EST AU VERSO ▶

Cette histoire est une parodie, toute ressemblance avec des personnes ou des situations existantes ou ayant existé ne serait que pure coïncidence.

3. La Cybersécurité de mes projets

J'intègre la **Cybersécurité** dans mes **projets** et dans les critères de **choix de mes fournisseurs.**

En pratique

Je n'installe aucun logiciel moi-même

Le service WeCare ou un appel au Help-Desk garantissent l'installation de logiciels habilités dont la mise à jour est contrôlée. Tout logiciel provenant d'une source externe peut représenter une menace pour la Compagnie. Solliciter le Help-Desk pour l'installation de logiciels externes non habilités est également une menace pour la Compagnie !

J'intègre la Cybersécurité dans les critères de choix de mes fournisseurs

Pour tout nouveau projet, je prends contact avec mon correspondant informatique (ou Cybersécurité) habituel pour **intégrer la Cybersécurité** dès la conception et tout au long de la vie du projet.

Une **Analyse Sécurité Projet** est réalisée afin de maîtriser les risques de Cybersécurité du projet. Les fournisseurs intervenant dans le projet portent des risques qui doivent être identifiés et traités. Les engagements de cybersécurité de ces fournisseurs devront être formalisés dès la phase d'appel d'offre et contractualisés dans un Plan d'Assurance Sécurité.

Je contrôle mes fournisseurs

Avant la contractualisation, le Plan d'Assurance Sécurité (PAS) est validé par un contrôle effectué par mon correspondant Cybersécurité habituel

Au cours du projet :

- Le PAS est à mettre à jour avant toute évolution du périmètre de la prestation.
- Les mesures de sécurité du PAS sont contrôlées régulièrement.

Mes responsabilités en tant que « Métier »

- Je qualifie les impacts métier des risques cyber identifiés.
- Je m'assure de l'implémentation des mesures de Cybersécurité.
- Je suis responsable du niveau de risque cyber résiduel du projet.

Vidéo

REX ATTAQUES VIA UN FOURNISSEUR - COGNIZANT

Vidéo

MICODE #3 LES INCIDENTS DE CYBERSÉCURITÉ

TotalEnergies

4. La protection de mes données

Une bonne pratique pour se prémunir :

- **Du vol de mes données** professionnelles et personnelles.
- **Un vol de données expose TotalEnergies à**
  - ✓ Des pertes financières et des pertes d'opportunité business ;
  - ✓ Des contentieux juridiques ;
  - ✓ Des sanctions financières ;
  - ✓ Une dégradation de l'image de la Compagnie.

En chiffres

4,2 M$

C'est le coût annuel moyen d'un vol de données pour une entreprise.
(source : IBM – 2021 Cost of a Data Breach Study : Global Overview)

38 milliards

de données seront exposées à des fuites de données en 2021.
(source : securitymagazine.com)

Vidéo

MICODE #4
LA PROTECTION DE MES DONNÉÉS

Voilà l'exemple à ne pas suivre

LA BONNE PRATIQUE EST AU VERSO ▶

Cette histoire est une parodie, toute ressemblance avec des personnes ou des situations existantes ou ayant existé ne serait que pure coïncidence.

4. La protection de mes données

Je **protège** mes données en fonction de **leur niveau de confidentialité** et je maîtrise leur **diffusion**.

En pratique

Je classifie

Mes informations sont-elles sensibles ?

- Le niveau de confidentialité des informations que je manipule (transmission, stockage,…) détermine l'outil de protection que je dois utiliser.
- la Compagnie fournit **un guide** listant les types d'informations sensibles au sein de la Compagnie et par périmètre métier.

Je sécurise

Mes informations non-sensibles

La fonction « Protéger » de LIFT / Office 365 me permet de choisir si mon mail ou mon document est « Public » ou « Restreint », les mécanismes de marquage s'appliquent alors automatiquement.

Mes informations sensibles

Pour stocker et partager des informations sensibles au sein d'un groupe projet, j'utilise le services iExtranet.

Pour échanger sur des sujets professionnels sensibles, j'utilise l'application Signal (disponible sur mobile ou ordinateur).

Pour mes informations sensibles et non secrètes, je peux utiliser certains des outils LIFT / Office 365 (Outlook, Word, Excel, Powerpoint) avec la fonction « Protéger » positionnée sur « Confidentiel ». Les mécanismes de protection s'appliquent automatiquement.

Liens utiles

La protection des informations et données sensibles dans LIFT / Office 365 et dans le cloud

Page Infosec « Je protège mes informations »

E-Learning

INFOSEC

CLASSIFICATION DE L'INFORMATION

InfoRules

J'UTILISE LES BONS OUTILS POUR PROTÉGER MES INFORMATIONS

Vidéo

REX FUITES DE DONNÉES TOTALENERGIES

TotalEnergies

5. La formation en Cybersécurité

Une bonne pratique pour garantir :

- L'acquisition des bons réflexes ;
- L'application des procédures internes ;
- L'utilisation des outils adaptés à mes besoins.

En chiffres

80% des incidents cyber
sont attribuables à l'erreur humaine.
(source : ObserveIT)
L'investissement dans la formation et la sensibilisation à la Cybersécurité a

72% de chance
de réduire l'impact business d'une cyberattaque.
(Source : 2015 Aberdeen Group & Wombat Security Technologies)

Vidéo

MICODE #5
LA FORMATION EN CYBERSÉCURITÉ

Voilà l'exemple à ne pas suivre

LA BONNE PRATIQUE EST AU VERSO ▶

Cette histoire est une parodie, toute ressemblance avec des personnes ou des situations existantes ou ayant existé ne serait que pure coïncidence.

5. La formation en Cybersécurité

Je suis les **formations Cybersécurité** de la Compagnie

En pratique

Je me forme à la Cybersécurité car tout un chacun y contribue.

Dès mon arrivée, je m'informe des enjeux de Cybersécurité, des règles à respecter et des bons comportements à adopter :

- Je prends connaissance des « Conditions générales d'utilisation des Systèmes d'Information de la Compagnie » (DIR-GR-INF-001).
- J'applique les 12 bonnes pratiques de la Cybersécurité.

Pour démarrer

Je me forme aux modules suivants accessibles à tous :

- « Phishing: to click or not to click, that is the question! » depuis l'application Touch&Learn (application web et mobile).
- « Cybersécurité : panorama et enjeux » disponible sur Lizzy.

Au quotidien

- Je suis les e-learnings et j'applique les fiches pratiques disponibles sur le site INFOSEC.
- Je pense aux Cybersecurity Moments pour mes réunions.

E-Learning
LIZZY
CYBERSÉCURITÉ : PANORAMA ET ENJEUX

Vidéos
DÉCOUVREZ NOTRE BIBLIOTHÈQUE DE CYBERSECURITY MOMENTS

E-Learning
INFOSEC
LA PROTECTION DES INFORMATIONS

Teaser

E-LEARNING PANORAMA & ENJEUX

6. La navigation sur Internet

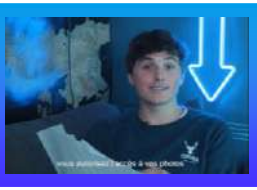
Une bonne pratique pour se prémunir :

- **D'une infection virale** rendant inopérant mes équipements (téléchargement de logiciels malveillants, fausses mises à jour urgentes via des fenêtres intempestives…).
- **D'une fuite de données sur Internet** suite à l'utilisation de services inadaptés.

En chiffres

4 minutes !
C'est le temps pour infecter un ordinateur non sécurisé et connecté à Internet.
(source : SANS Institute)

En 4 partages successifs,
une information devient visible par plusieurs centaines de millions d'utilisateurs !
(source : INFOSEC)



Vidéo

MICODE #6
LA NAVIGATION
SUR INTERNET

Voilà l'exemple à ne pas suivre

LA BONNE PRATIQUE EST AU VERSO ▶

Cette histoire est une parodie, toute ressemblance avec des personnes ou des situations existantes ou ayant existé ne serait que pure coïncidence.

6. La navigation sur Internet

Je navigue sur Internet avec prudence et **j'utilise les services mis à disposition par la Compagnie** (stockage, échange, collaboration…).

En pratique

Quand je navigue sur Internet :

- J'utilise exclusivement les services autorisés par la Compagnie pour stocker ou échanger des documents professionnels.
- Je vérifie l'adresse affichée du site et s'il est sécurisé (commence par « https:// ») notamment pour les opérations sensibles (banque en ligne, site e-commerce…).
- Je ne communique pas mes coordonnées professionnelles (téléphone, mail) sur des sites non professionnels.

SUR LES RÉSEAUX SOCIAUX

Je protège mes comptes

- Je crée un mot de passe robuste (cf. règle #1).
- Je gère la confidentialité de mon compte. Pour cela, je m'aide des guides définis par la Compagnie et disponibles sur **INFOSEC**.

Je choisis mes contacts avec soin

- J'accepte uniquement des invitations des personnes que je connais ou bien je me renseigne sur ces personnes avant de les accepter comme contact.

J'évalue la sensibilité des informations que je publie

- Je ne communique pas d'informations qui pourraient être utilisées au détriment de la Compagnie.
- Je ne détaille pas mes activités professionnelles.
- Je ne renseigne que les informations utiles.

E-Learning
INFOSEC
LES DANGERS D'INTERNET

Vidéo

CYBERSECURITY MOMENT
The Fortune Teller

D'une façon générale, JE NE PUBLIE PAS sur Internet ce que JE NE DIRAIS PAS à un inconnu dans la rue.

7. La connexion Internet en dehors des sites TotalEnergies

Voilà l'exemple à ne pas suivre

En chiffres

73 %

des consommateurs n'utilisent jamais un VPN pour sécuriser leurs connexions wifi, même si c'est la meilleure solution pour protéger leurs informations. (source : idtheftcenter.org)

Une bonne pratique pour se prémunir :

- **D'une fuite de mes données professionnelles et personnelles** (interception des données par l'attaquant placé entre l'utilisateur ciblé et le point d'accès WiFi. Les WiFi publics sont particulièrement concernés par cette attaque appelée « Man in the Middle »).

LA BONNE PRATIQUE EST AU VERSO ▶

Cette histoire est une parodie, toute ressemblance avec des personnes ou des situations existantes ou ayant existé ne serait que pure coïncidence.

7. La connexion Internet en dehors des sites TotalEnergies

J'utilise **mon VPN** quand je me connecte à un réseau WiFi public.

En pratique

Pour toute connexion en dehors des sites de la Compagnie et surtout depuis un réseau WiFi public (aéroports, hôtels,…), j'utilise le VPN pour me connecter à partir de mon terminal TotalEnergies.

Qu'est-ce qu'un VPN ?

Un VPN ou Virtual Private Network (réseau privé virtuel) est un service permettant de naviguer sur Internet et d'accéder à distance au Système d'Information TotalEnergies de façon confidentielle et sécurisée.

Comment utiliser le VPN sur mon laptop TotalEnergies ?

- Mon VPN Zcaler se lance automatiquement.
- Je m'assure en ouvrant l'application Zscaler que les statuts des services sont bien sur « ON ».

Et sur mon smartphone TotalEnergies ?

- Je n'ai aucune action à réaliser : le VPN se lance automatiquement.

Et pour mes travaux personnels ?

- Pour mes terminaux personnels, ils existent de multiples solutions sur le marché. Veillez à vérifier et recouper la réputation du fournisseur que vous choisirez.

Vidéo

MICODE #7 CONNEXION INTERNET EN DEHORS DES SITES TOTALENERGIES

8. La vigilance sur les terminaux publics

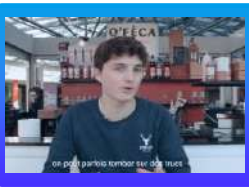
Une bonne pratique pour se prémunir :

- **D'une fuite de mes données auxquelles j'accède depuis un terminal public** (sessions laissées ouvertes sur des postes publics ; mots de passe enregistrés dans le navigateur d'un terminal public…).
- **D'une infection de mes fichiers** à partir d'un terminal non sécurisé et préalablement compromis.

En chiffres

x2

Le nombre de failles de sécurité enregistrées par an a plus que doublé depuis 2016.
(source : cvedetails.com)



Vidéo

MICODE #8
LA VIGILANCE SUR LES TERMINAUX PUBLICS

Voilà l'exemple à ne pas suivre

LA BONNE PRATIQUE EST AU VERSO ▶

Cette histoire est une parodie, toute ressemblance avec des personnes ou des situations existantes ou ayant existé ne serait que pure coïncidence.

8. La vigilance sur les terminaux publics

J'accède aux données TotalEnergies depuis **mes terminaux professionnels et personnels** et j'évite d'utiliser des terminaux publics.

En pratique

Avec LIFT (Office 365), vous avez désormais accès à vos informations professionnelles (Outlook, OneDrive…) depuis tout poste de travail n'appartenant pas à la Compagnie.
Ces nouveaux modes d'accès impliquent le respect de quelques règles d'usage.

Sur les terminaux publics et personnels :

- Je considère que tout ce que je fais sur un terminal public pourrait être rendu public.
- Je ne consulte pas d'informations confidentielles.
- Je sélectionne « non » quand il m'est proposé de « rester connecté ».
- Quand j'ai terminé de travailler, je me déconnecte de mon compte puis je ferme le navigateur Internet.
- Je ne télécharge pas de fichiers localement.

NB : sur mes terminaux personnels, le téléchargement de fichiers est toléré. Je les supprime une fois mon travail terminé.

Je sépare mes activités personnelles et professionnelles :

- Je choisis des mots de passe différents pour tous les services / applications personnelles et professionnelles que j'utilise ;
- Je ne mélange pas ma messagerie professionnelle et personnelle ;
- Je n'utilise pas de services de stockage en ligne personnels à des fins professionnelles.

E-Learning
INFOSEC
TRAVAILLER DEPUIS UN ÉQUIPEMENT NON TOTAL ENERGIES

Les terminaux publics se trouvent dans les cybercafés, les hôtels, les aéroports et plus généralement dans tous les lieux publics, UN TERMINAL PRÊTÉ PAR UN TIERS EST ÉGALEMENT CONSIDÉRÉ COMME PUBLIC.

9. La sauvegarde de mes fichiers importants

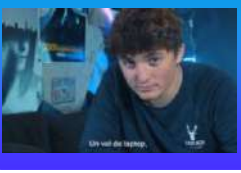
Une bonne pratique pour se prémunir :

- **D'une perte de mes données non sauvegardées** suite à une infection par un logiciel malveillant.
- **D'un arrêt de l'activité** suite à l'indisponibilité de mes données vitales.

En chiffres

En 2017, le malware NotPetya a paralysé l'activité de nombreuses organisations. Les pertes cumulées de ces acteurs ont dépassé

1 milliard de dollars



Vidéo

MICODE #9
LA SAUVEGARDE DE MES FICHIERS IMPORTANTS

Voilà l'exemple à ne pas suivre

LA BONNE PRATIQUE EST AU VERSO ▶

Cette histoire est une parodie, toute ressemblance avec des personnes ou des situations existantes ou ayant existé ne serait que pure coïncidence.

9. La sauvegarde de mes fichiers importants

Je m'assure de la **sauvegarde** régulière de mes **fichiers importants** dans un **espace sécurisé**.

En pratique

En cas de perte, de vol, de panne, de piratage ou de destruction de vos appareils ou systèmes numériques, vous perdrez les données enregistrées sur ces supports.

Il peut s'agir de données auxquelles vous accordez une importance particulière ou considérées comme essentielles dans le cadre de vos activités personnelles ou professionnelles.

Il est essentiel de s'assurer que vos données et fichiers importants sont sauvegardés dans un espace sécurisé.

Pour mes données non sensibles :

- Je les stocke dans les dossiers Desktop, Documents ou Favorites de mon terminal TotalEnergies qui sont sauvegardés.
- Je les stocke dans mes espaces LIFT (OneDrive – SharePoint) qui sont sauvegardés.

Pour mes données confidentielles :

- Je les stocke dans iExtranet : mes données sont alors protégées et sauvegardées.

Pour toute demande sur les solutions mentionnées ci-dessus, n'hésitez pas à contactez votre correspondant informatique habituel.

Vidéo

CYBERSECURITY MOMENT
Sécurité des données
Sauvegarde des données et restauration

Vidéo

CYBERSECURITY MOMENT
Cybermalveillance.gouv.fr

TotalEnergies

10. L'usage des supports amovibles

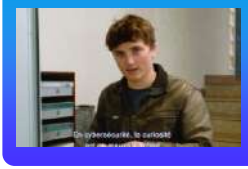
Une bonne pratique pour se prémunir :

- **D'une infection ou une destruction des données** de mon poste de travail suite à l'insertion d'un support amovible infecté.
- **D'une fuite de mes informations confidentielles** suite à la perte ou au vol d'un support amovible.

En chiffres

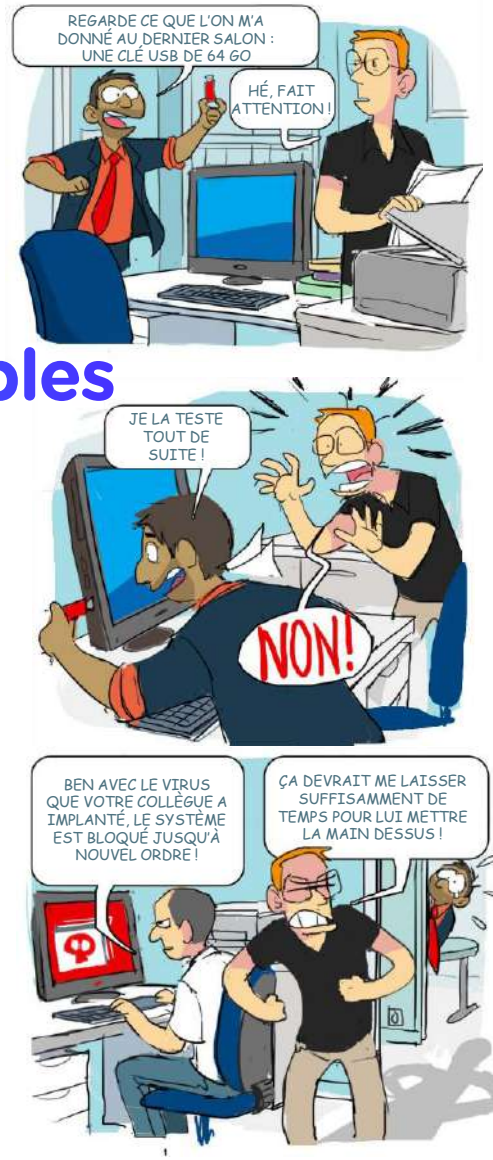
98 %
des clés USB abandonnées sont ramassées.

45 %
d'entre elles sont explorées avec ouverture des fichiers.
(source : Google's anti-abuse research team)



Vidéo

MICODE #10
L'USAGE DES SUPPORTS AMOVIBLES



Voilà l'exemple à ne pas suivre

Cette histoire est une parodie, toute ressemblance avec des personnes ou des situations existantes ou ayant existé ne serait que pure coïncidence.

LA BONNE PRATIQUE EST AU VERSO ▶

10. L'usage des supports amovibles

Je ne connecte **pas de supports amovibles appartenant à des tiers** à mes équipements professionnels et personnels.

En pratique

Les supports amovibles peuvent être utilisés afin de propager des virus, voler des informations sensibles et stratégiques ou encore compromettre le réseau de l'entité.

- De tels agissements peuvent avoir des conséquences désastreuses pour l'activité de la structure ciblée.
- Je ne connecte jamais de supports amovibles appartenant à des tiers à mon environnement de travail.
- Je privilégie les outils d'échange et de partage de fichiers préconisés par la Compagnie à l'usage d'un support amovible.
- Si je dois utiliser un support amovible, je le dédie à un usage strictement professionnel.
- Pour des informations sensibles, j'utilise les supports amovibles sécurisés habilités par la Compagnie (clés ou disques durs avec chiffrement).
- En cas de doute, je lance un scan antivirus sur le support amovible depuis mon poste de travail ou depuis une borne de décontamination USB si mon site en est équipé.

Exigences complémentaires sur un réseaux industriel

- Je dédie un support amovible à un usage exclusif sur le réseau industriel et distinct de celui utilisé sur le réseau bureautique.
- Avant utilisation, j'analyse tout support amovible à l'aide d'un dispositif habilité.

Liens utiles

Page INFOSEC

GÉRER LES SUPPORTS AMOVIBLES

E-Learning

INFOSEC

GÉRER LES SUPPORTS AMOVIBLES

11. Les incidents de Cybersécurité

Une bonne pratique pour se prémunir :

- **De la propagation et de l'aggravation d'un incident** suite à une absence de signalement ou un signalement tardif, retardant la réaction des services compétents.

En chiffres

6 000 Milliards $

Coût global estimé des cyber attaques dans le monde en 2021
(source : CyberSecurity Ventures)

Voilà l'exemple à ne pas suivre

Cette histoire est une parodie, toute ressemblance avec des personnes ou des situations existantes ou ayant existé ne serait que pure coïncidence.

LA BONNE PRATIQUE EST AU VERSO ▶

11. Les incidents de Cybersécurité

Je signale **tout incident, anomalie ou sollicitation abusive** à mon support informatique ou à mon correspondant habituel.

En cas de :

Comportement inhabituel de mes terminaux (ordinateur, smartphone, tablette) ou des applications que j'utilise

- Exemples : impossibilité de se connecter, lenteurs, activité importante, connexions ou activités inhabituelles, fichiers créés, modifiés ou supprimés sans autorisation,…

Comportements ou sollicitations inhabituels, abusifs et présentant un caractère urgent :

- Tentative de phishing ;
- Tentative de fraude au président ;
- Arnaque au faux support technique.

RQ : Ces arnaques font appel au manque de vigilance des cibles (Cf. Ingénierie sociale).

Vidéo

MICODE #11
LES INCIDENTS DE CYBERSÉCURITÉ

Perte / vol / confiscation d'informations ou de matériels

- Je ne cède pas à la panique.
- Je contacte mon support informatique ou mon correspondant informatique habituel.

Vidéo

CYBERSECURITY MOMENT
Signalement des évènements de sécurité

TotalEnergies

12. La vigilance face au phishing

Une bonne pratique pour se prémunir :

- **D'une infection ou d'une destruction** des données de mon poste de travail pouvant s'étendre à celles de la Compagnie.
- **D'une fuite de données confidentielles**.
- **D'une fuite de mes identifiants / mots de passe professionnels et personnels.**

En chiffres

Au mois de Juin 2020

660 448

E-mails de phishing ont été bloqués par les systèmes de protection de la Compagnie.
(Source : Indicateurs internes)

95 %

Des malwares sont véhiculés par email.
(source : CSO Online)

Vidéo

MICODE #10
L'USAGE DES SUPPORTS AMOVIBLES

Voilà l'exemple à ne pas suivre

Cette histoire est une parodie, toute ressemblance avec des personnes ou des situations existantes ou ayant existé ne serait que pure coïncidence.

LA BONNE PRATIQUE EST AU VERSO ▶

12. La vigilance face au phishing

Je ne clique **ni sur les liens ni sur les pièces jointes** des mails suspects que je signale.

En pratique

Je me protège en apprenant à détecter les tentatives de phishing. En cas de doute, plusieurs indices peuvent m'alerter sur le caractère frauduleux du mail :

- L'adresse e-mail de l'expéditeur imite une adresse légitime (en alternant ou substituant certains caractères similaires, par exemple « @tolalenergies.com » au lieu de «@totalenergies.com »).
- Contient des fautes d'orthographe, de grammaire, de syntaxe.
- Contient une notion d'urgence, de sanction, ou de gain.
- Recours à des menaces irréalistes ou tente de générer un
- sentiment d'urgence (appel à l'action immédiate, ton insistant).
- Provient d'un expéditeur inconnu ou suspect.
- Utilise des formulations impersonnelles et généralistes.
- Renvoie vers une URL/domaine suspect.

Détecter les mails suspects

- Je ne clique pas sur les liens et n'ouvre pas les pièces jointes contenues dans ce type d'email !
  - ✓ Dans le cas contraire, j'informe immédiatement mon support informatique pour stopper l'infection.
- Je contacte mon interlocuteur en cas de doute :
  - ✓ même si l'expéditeur est bon, si le contenu est inhabituel ou suspect.
  - ✓ sa messagerie a peut-être été piratée.
- Je ne réponds jamais.
- Je signale tout email suspect :
  - ✓ Soit à l'aide du bouton anti-phishing de ma messagerie.
  - ✓ Soit en contactant mon support informatique.

Liens utiles

Article Infosec sur l'usage du bouton anti-phishing

Page Infosec sur le Phishing

Je suis LA FORMATION SUR LE PHISHING sur CLICK&LEARN

E-Learning

INFOSEC

DÉTECTER ET FAIRE FACE AU PHISHING

Vidéos

REX PHISHING TOTALENERGIES MEXICO