2025 année de la cybersécurité

GIFAS

Que ce soit dans un cadre professionnel ou personnel, l'utilisation des outils numériques ne cesse de croître et de se diversifier. Ordinateurs de bureau ou portables, téléphones mobiles, tablettes, objets connectés… Ils font de plus en plus partie de notre quotidien. Cette intensification des usages représente pour les cybercriminels une opportunité de développer leurs attaques. **Comment se protéger au mieux face à ces risques ?** Voici **10 bonnes pratiques** essentielles à adopter pour assurer votre cybersécurité, présentées dans de **courtes vidéos**.

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/10-mesures-essentielles-assurer-securite-numerique

Nous vous rappelons qu'AirCyber permet la mise en œuvre d'une gouvernance cyber et une bonne réponse opérationnelle pour faire face aux risques qui ciblent notre filière. Si vous souhaitez devenir membre d'AirCyber, inscrivez-vous ici :

https://boostaerospace.com/aircyber/contact-form/

L'actualité est également marquée par la recrudescence de faux e-mails et de tentatives de fishing. Retrouvez ci-après la **fiche réflexe rédigée par le CERT** qui détaille ce qu'il faut faire en cas de **réception d'un message suspect** (via SMS, e-mail ou outil de messagerie).

GIFAS - Direction des Affaires Industrielles/Commission Du Digital

Avril 2025

CERT Aviation France

FR 03	Un personnel reçoit un message suspect (via SMS, email ou outil de messagerie)	MàJ : 28/03/2025

Symptômes

- **Expéditeur inconnu ou adresse d'expédition étrange** :
  - Le message provient d'une adresse mail/numéro inconnu ;
  - L'adresse/le numéro de l'expéditeur est étrange : (ex : une adresse email officielle avec un domaine non professionnel / numéro étranger / numéro court).
- **Langue / Erreurs d'orthographe ou de grammaire** :
  - Le message contient des fautes, des phrases mal construites ou un style d'écriture inhabituel (ces erreurs peuvent indiquer que le message a été traduit automatiquement) ;
  - Le message est dans une langue étrangère.
- **Demandes urgentes ou menaces** :
  - Le message vous demande d'agir rapidement. On vous menace si vous ne répondez pas immédiatement.
- **Liens ou pièces jointes inattendus**
- **Demandes de renseignements personnels ou confidentiels** :
  - On vous demande de fournir des informations personnelles, financières ou de connexion (ex : mots de passe, numéros de carte bancaire, …).
- **Offres trop belles pour être vraies**
- **Détails qui semblent « anormaux » ou qui font « amateurs » / signes visuels inhabituels (mise en page, signature)**

Actions réflexes à l'attention du destinataire du mail :

- Ne pas suivre les liens : pour les emails, passer la souris sur les liens pour vérifier l'adresse (anomalie dans l'orthographe, …) ;
- Ne pas rappeler les numéros demandés ;
- Vérifier l'expéditeur. S'il est connu, comparer avec les emails précédemment reçus ;
- Ne jamais fournir d'informations personnelles. Si vous avez fourni des informations bancaires : contactez votre banque ;
- Utiliser une source tierce de vérification (appel téléphonique direct) ;
- Signaler l'email à la personne en charge dans votre entité : envoyer l'email en pièce jointe sans le transférer ;
- Supprimer le message et pour les emails, vider la corbeille ;
- Vérifier votre système (exécuter un scan antivirus et changer vos mots de passe).

Actions réflexes à l'attention du responsable informatique de l'entité :

En cas de doute ou si votre entité souhaite bénéficier de moyens d'investigation cyber supplémentaires, le responsable peut contacter le service de réponse à incident du CERT Aviation 24/7 :

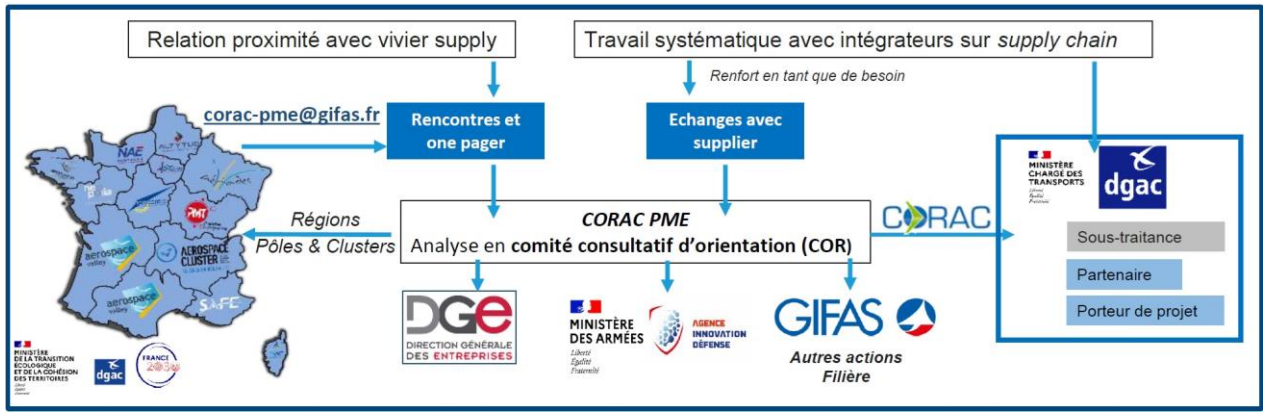
01.81.70.71.72 / assistance@cert-aviation.fr

CERT Aviation France

Sur l'ensemble de l'année, la CDD propose des livrables mensuellement pour sensibiliser et accompagner la supply chain

Composites TP : dispositifs d'accompagnement

Le groupe de travail **Composites ThermoPlastiques** du **Comité Industriel** a préparé ce document avec pour objectif de permettre aux PME et ETI de la filière de mieux connaitre les **dispositifs d'accompagnements** et de les aider à s'orienter vers les bons guichets d'innovation en fonction des types de projet : Régionaux, Nationaux, Européens, Projets Laboratoires / IRTs / Centres techniques.



➔ Livrable pour la filière :

Cartographie des projets subventionné

Livrables à l'attention des Pôles et Clusters ainsi que leurs adhérents

Cartographie des sujets digitaux

Le GT ESN propose de venir présenter ses travaux aux adhérents des pôles et clusters lors de leurs réunions en Régions

Accélérer sa digitalisation

Replays disponibles :

Retrouvez ici les replays de nos masterclasses :

- Présentation des Webinaires Comment accélérer sa digitalisation ?
- Pourquoi l'ERP est un levier de réussite pour l'entreprise dans un contexte de ramp up ?
- Comment valoriser ses données et les verrous à lever ?
- Quelles sont les tendances du digital en 2024 et leurs impacts sur nos métiers ?
- La collaboration digitale au service de l'Aéronautique et de la Défense
- Comment améliorer sa performance en exploitant les données du Shopfloor ?
- Visite au cœur de la collaboration et de la digitalisation du Manufacturing Engineering
- Le MES (Manufacturing Execution System) levier de performance du shopfloor
- Gestion des compétences au cœur des défis actuels de la filière

Replays accessibles directement via les liens ci-dessous