Page Principale

Cybersécurité, tous concernés !

Sécurité Informatique, tous concernés !

Avec la transition numérique, nos métiers et nos usages ont évolués ! Il s'agit certes d'un progrès incontestable mais qui s'accompagne également d'une cybercriminalité en forte croissance.

La sécurité informatique ou cybersécurité a pour mission de protéger les données informatiques de l'entreprise contre toute violation, intrusion, dégradation ou vol de données.

Vous trouverez, ici, les conseils et bonnes pratiques, articles pour protéger votre environnement Professionnel (et du coup votre environnement personnel :)

Si vous avez identifié des situation à risque ou pour toute autre question ou remontée, n'attendez pas :

Contacter :

Mettre les coordonnées du rôle à contacter au niveau de D&A

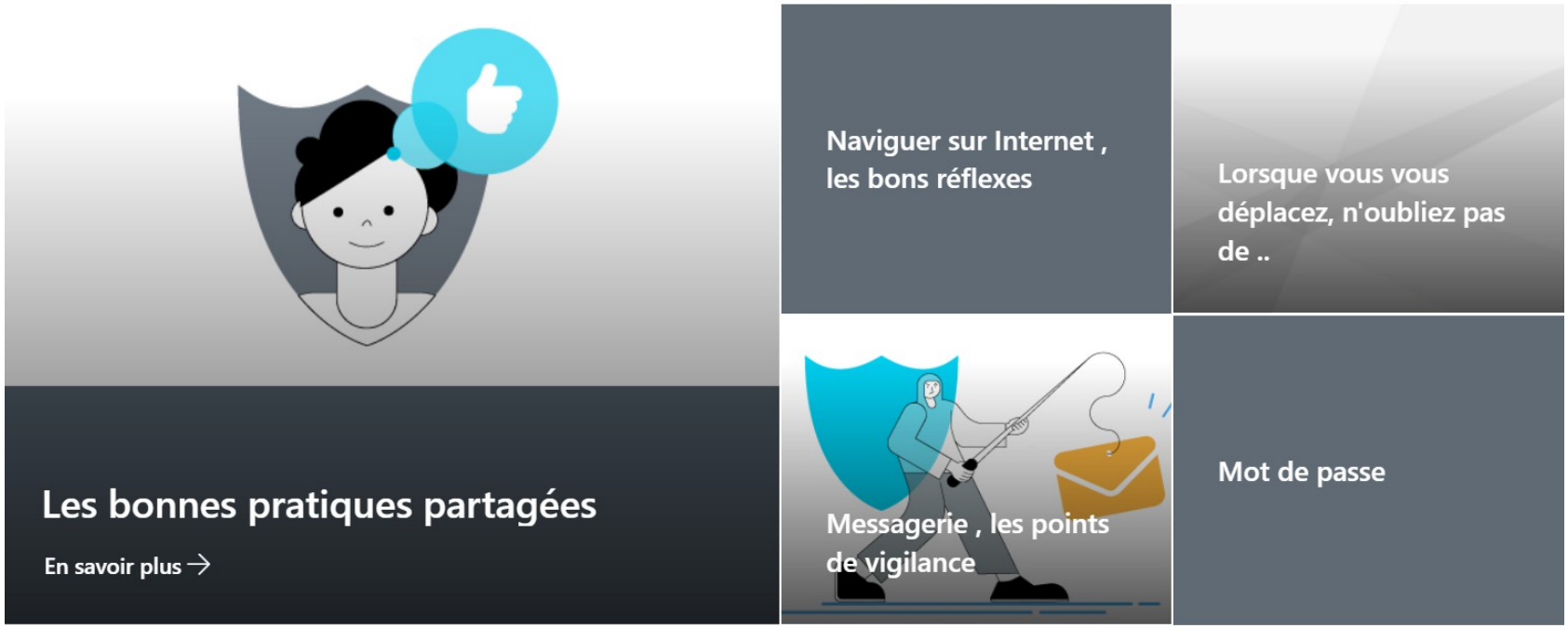
1. Identifiez les situations à risques et réagissez !

Votre vigilance aidera à arrêter les attaques et à réduire l'impact de celles qui se produisent malgré tout.

Quand réagir ?

- Vous pensez que vos mots de passe ont été utilisés
- Votre PC commence à agir de manière suspecte ou inhabituelle
- Vous rencontrez un comportement informatique suspect ou un logiciel défectueux
- Votre PC ou votre smartphone est perdu ou volé

2. Gardez en tête les bonnes pratiques :



Pages de renvoi quand l’utilisateur va cliquer sur les 5 domaine des images ci-dessus

Page 1 " Les bonnes pratiques partagées"

BONNES PRATIQUES-SECURITE INFORMATIQ...

Gardez en tête les bonnes pratiques partagées

ACCUEIL D2ID > CYBERSECURITE > BONNES PRATIQUES PARTAGEES

Mot de passe :
Choisissez un mot de passe complexe, sécurisé et gardez le secret !

Équipements :
Sécurisez vos équipements au bureau et conservez-les avec vous lorsque vous travailler en mobilité

Protection des données :
Protégez vos données avec les outils d'entreprise dont vous disposez et adoptez le bon comportement

E-mail :
Faites attention lors de l'envoi ou de la réception d'un e-mail

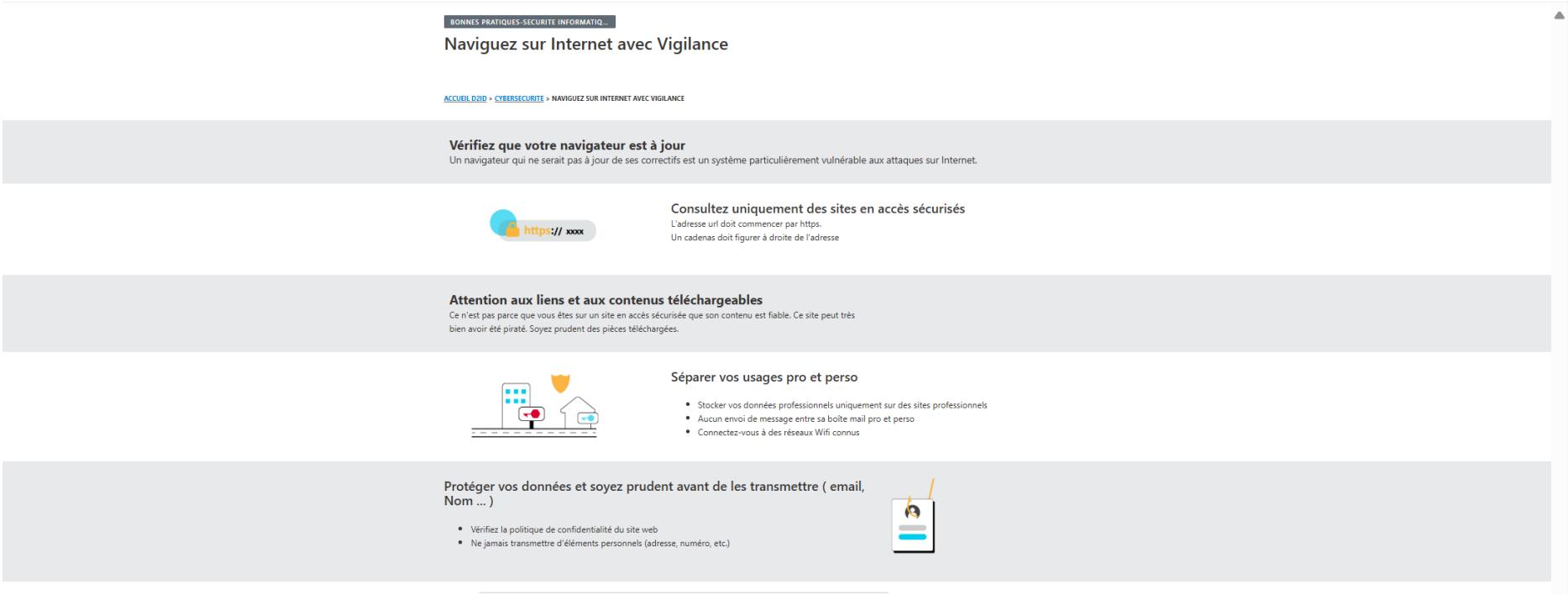
Internet :
évitez les comportements à risque et n'installez pas de logiciels interdits

Outils de protection :
Respecter les politiques et les outils de sécurité GSF et garder vos ordinateur personnel et professionnel pour des utilisations distinctes

Conformité - Réglementation :
Agissez conformément aux lois et règlements auxquels vous soumettez

Ingénierie sociale :
Ne fournissez pas d'informations à des étrangers sans preuve de leur identité et restez discret quant vos activités professionnelles

Page 2 " Naviguez sur Internet avec Vigilance "



Page 3 " Messagerie"

BONNES PRATIQUES-SECURITE INFORMATIQ...

Messagerie

ACCUEIL D2ID > CYBERSECURITE > MESSAGERIE

L'email est le canal privilégié par les cyber-délinquants. **65% des incidents** de cybercriminalité ont utilisé l'email comme porte d'entrée : Phishing, SPAM, La fraude au président...

N'ayez pas une confiance aveugle dans le nom de l'expéditeur

- Répondez seulement aux e-mails ayant un expéditeur connu et de confiance.
- Soyez attentif à tout indice mettant en doute l'origine réelle du courriel :
  - notamment si le message comporte une pièce jointe ou des liens
  - Une incohérence de forme ou de fond entre le message reçu et ceux que votre interlocuteur légitime vous envoie d'habitude
  - En cas de doute, contactez votre interlocuteur pour vérifier qu'il est à l'origine du message.

Méfiez-vous des pièces jointes

Elles peuvent contenir des virus ou des espiogiciels.
Ouvrir uniquement les pièces jointes provenant de sources connues et dignes de confiance
Si votre poste a un comportement anormal (lenteur, écran blanc sporadique, etc.), contacter l'assistance.

Ne répondez jamais à une demande d'informations confidentielles

Les demandes d'informations confidentielles, lorsqu'elles sont légitimes, ne sont jamais faites par courriel (mots de passe, code PIN, coordonnées bancaires, etc.). En cas de doute, là encore, demandez à votre correspondant légitime de confirmer sa demande car vous pouvez être victime d'une tentative de filoutage, ou phishing.

Soyez vigilants sur le contenu envoyé

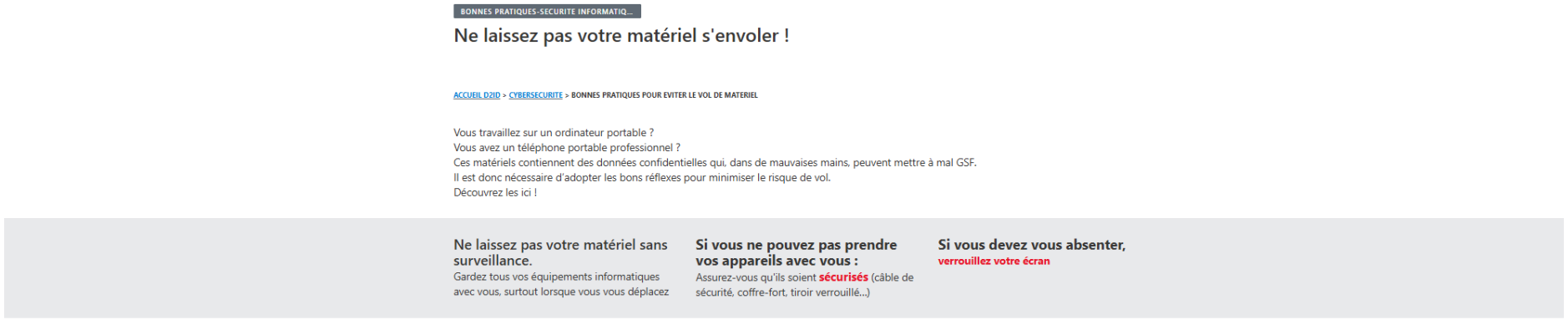
- Envoyez des messages dont le contenu ne porte pas atteinte à l'image de GSF ni à sa réputation
- Vérifiez l'identité de vos destinataires et soyez vigilants aux homonymies et aux listes de diffusion

J'aime Commentaire 74 vues Enregistrer pour plus tard

Commentaires

Ajoutez un commentaire. Tapez @ pour mentionner une personne Publier

Page 4 " Ne laissez pas votre matériel s'envoler ! "



Page 5 " Mot de passe "

BONNES PRATIQUES-SECURITE INFORMATIQ...

Mot de passe

Les mots de passe mal choisis constituent un point faible du SI : Prêtés, Notés, Trop courts, Trop simples, etc.

Les principaux risques : Accès frauduleux aux S.I. GSF, Usurpation d'identité, Vol de données sensibles, Atteintes aux données personnelles, Fraudes et détournements.

Séparer vos environnements PRO et PERSO.

Il est important de définir des mots de passe différents entre vos usages Pro et Perso.
En gardant des mots de passe identiques, vous facilitez la tâche des pirates ...

Exemple : mail pro et mail perso = 2 mots de passe

Renouvelez régulièrement vos mots de passe !

Conseil:

Choisissez un mot de passe complexe!
Evitez les structures classiques...

Longueur minimum : 12 caractères
Complexité : 4 types de caractères minimums parmi minuscule, majuscule, chiffre, caractères spéciaux

Evitez toutes références à des informations personnelles (ex: Date de naissance, prénom etc ...

Ne partagez jamais vos identifiants, un mot de passe est personnel!

Ne communiquez ou ne partagez jamais vos mots de passe
Evitez les post-it visibles, etc...