

Maintenez votre environnement aussi sûr que possible

Ne laissez pas de tiers non autorisés vous approcher lorsque vous accédez au DEP.

Utilisez une connexion réseau sécurisée.

Verrouillez systématiquement votre session dès que vous vous absentez, même pour un court instant.

N'utilisez pas de support externe (par exemple un disque dur ou une clé USB) de provenance inconnue sur votre poste.

Utilisez un poste de travail, une tablette ou un smartphone à jour

Utilisez un logiciel antivirus à jour et activez le pare-feu.

Mettez systématiquement à jour vos logiciels, en particulier le système d'exploitation (Windows, MacOS, Android, iOS) et le navigateur internet utilisé pour accéder au DEP afin de corriger les failles de sécurité.

Ne vous connectez pas au DEP depuis un poste de travail que vous ne maîtrisez pas.



Créez de mots de passe uniques et complexes

Créez des mots de passe uniques et complexes combinant majuscules, minuscules, chiffres, caractères spéciaux, pour chacun de vos comptes.

Ne communiquez pas vos mots de passe et ne les inscrivez pas sur un support physique (post-it, calepin, etc.).

Restez vigilant

Ne vous laissez pas tromper ou distraire: si quelque chose vous paraît anormal ou inhabituel, agissez avec prudence.

N'ouvrez pas les pièces jointes d'emails dont vous doutez de la provenance.

Ne répondez jamais aux demandes de transmission d'informations sensibles.

CARA ne vous demandera jamais de transmettre vos identifiants de connexion au DEP.

