CYBER TRANS LOG

Mémo Apprenant

L'essentiel à retenir



01 Votre rôle de bouclier



Votre parcours est terminé.
Ce mémo, c'est votre kit de réflexes. Casier, camion, sac : gardez-le à portée de main. Un doute ? Ouvrez-le.



Plannings, guidage, quais, badges, facturation :
tout passe par le numérique.



Une attaque numérique, des dégâts bien réels :
un camion détourné, un quai bloqué, des collègues et des usagers en danger.



Les pirates cherchent la facilité :
un clic trop rapide, un écran ouvert, une clé USB branchée par curiosité.



Vos gestes suffisent souvent à les arrêter.
Vos réflexes, ce sont vos EPI numériques.



Le premier rempart de votre entreprise, ce n'est pas un logiciel. C'est vous.

Dans ce mémo :



02 Les pièges que vous avez appris à déjouer

Vous les avez croisés dans les modules. Ils existent pour de vrai, tous les jours.

Sur la route et en entrepôt



La clé USB piégée (baiting)
Oubliée exprès sur un parking, elle n'attend que d'être branchée.

→ On ne branche pas, on la remet au référent.



Le mouchard GPS (cheval de Troie)
Un programme caché détourne le guidage vers une zone isolée.

→ Trajet incohérent ? On signale, on ne force pas.



Le robot devenu fou
Un pirate prend le contrôle d'un engin automatisé : danger physique sur les quais.

→ On stoppe, on s'éloigne, on alerte.



Le faux Wi-Fi (Man-in-the-Middle)
Un réseau gratuit qui lit et modifie tout ce qui passe.

→ Documents pro : jamais sur un Wi-Fi public.

Dans les ports et les gares



Les faux signaux (leurrage GNSS)
De faux signaux satellites trompent le navire sur sa position.

→ Position douteuse ? On recoupe, on signale.



Le sabotage des systèmes
Un intrus bloque la signalisation ou les portiques.

→ Comportement anormal = alerte immédiate.



L'arnaque sur mesure (spearphishing)
Un e-mail ultra précis : vrai nom du navire, vrai commandant.

→ Même crédible, on vérifie par téléphone.

Au bureau et à l'exploitation



La fausse urgence (phishing)
"Validez vos accès dans les 10 minutes !" Le lien vole vos mots de passe.

→ L'urgence, c'est le piège : on ne clique pas.



Le faux RIB
Une facture interceptée, un RIB changé, un client qui paie un pirate.

→ Nouveau RIB = contre-appel, pour vérifier.



Le poste resté ouvert (vol de session)
Une minute d'absence suffit pour valider un faux transport à votre place.

→ Je pars, je verrouille. Windows + L.

Le point commun de ces attaques ? À chaque fois, un geste humain pouvait les arrêter.

03 Vos 5 réflexes de protection



Zéro branchement inconnu
Jamais de clé trouvée ni de téléphone perso sur un outil pro.



Verrouillez avant de partir
Je pars, je verrouille. Windows + L.



Le contre-appel
Tout changement de RIB ou d'adresse se vérifie au numéro du répertoire.



Zéro Wi-Fi public pour le boulot
Documents pro : 4G/5G ou réseau officiel du site.



Stoppez, sécurisez, alertez
Machine bizarre, message louche ? Arrêt, mise en sécurité, alerte.



En cas de doute : on ne clique pas, on ne branche pas, on demande.

04 Le dico de la cybersécurité



Phishing : l'arnaque au faux client. Un message qui imite un partenaire de confiance pour vous faire cliquer.



Baiting : le piège de l'appât. Une clé USB abandonnée exprès, en espérant que quelqu'un la branche.



Man-in-the-Middle : le facteur invisible. Un pirate entre vous et le serveur, qui lit et modifie vos échanges.



Cheval de Troie : le mouchard. Un programme caché qui espionne ou manipule vos données.



Rootkit : le double de clés invisible. Un accès dérobé qui donne au pirate les pleins pouvoirs, sans se faire voir.



DDoS : l'embouteillage numérique. Des millions de fausses demandes qui saturent un serveur. Un péage envahi d'un coup.



Ransomware : le cadenas à rançon. Tout est verrouillé, et le pirate exige un paiement pour libérer.



OT : l'informatique qui agit. Les systèmes qui pilotent les machines réelles : portiques, aiguillages, grues, robots. Voilà pourquoi une attaque numérique fait des dégâts physiques.

05 Pour aller plus loin



Votre premier contact : votre formateur ou votre référent. Un doute, une situation bizarre ? Parlez-en.

Des ressources gratuites et officielles

Cybermalveillance.gouv.fr : fiches pratiques et parcours SensCyber, pour le travail et la maison.

SecNumAcadémie (ANSSI) : les bases de la cybersécurité.

Financeur principal

Co-financeurs

« Opération soutenue par l'État dans le cadre de l'AMI « Compétences et Métiers d'Avenir » du Programme France 2030, opéré par la Caisse des Dépôts ». Avec le soutien d'OPCO MOBILITÉS.

Partenaires du projet

Avec la participation de

Zelabo
E-SNCF Solutions
Alcyconie
France Cyber Maritime

Remerciements

Nous adressons nos sincères remerciements à :

- la DRANE ;
- l'École de la Deuxième Chance d'Amiens ;
- les établissements scolaires partenaires ;
- Euralogistic

Ce mémo accompagne le dispositif CyberTransLog, Sensibilisation à la cybersécurité dans les métiers du transport et de la logistique : route, ferroviaire, maritime et entrepôt.