CYBER SÉCURITÉ

POUR LES PETITES COLLECTIVITÉS

CDG 76

PARTIE 1

ÉTAT DE LA MENACE

TOUTES CONCERNÉES

- 1 collectivité normande par semaine est cyber attaquée selon la Gendarmerie Nationale pour la Région Normandie
- 1 collectivité sur 10 victime de cyberattaque en 2024 au niveau national

Toutes les communes, **même les plus petites**, sont exposées au risque de cyberattaque.

CDG 76

VOUS ÊTES UNE CIBLE CAR…

- Vous détenez des données personnelles de vos habitants qui peuvent être revendues et améliorer les gains du pirate
- Vous ne pensez pas être suffisamment « gros » pour intéresser
- Vous êtes souvent sous équipés en solutions basiques de cybersécurité

  ET/OU

  Vous n’avez pas de service informatique pour vous épauler

CDG 76

ATTAQUANTS

	OBJECTIFS
ÉTATIQUE →	Espionnage à des fins économiques, politiques ou militaires / déstabilisation / sabotage
HACKTIVISTES →	Déstabilisation / Atteinte à l'image de la collectivité
CYBERCRIMINELS →	Recherche de gains financiers
AMATEURS →	S'entraîner / saboter

CDG 76

PARTIE 2

LES PRINCIPALES ATTAQUES POUR LES PETITES COLLECTIVITÉS

MENACES LES + PRÉGNANTES POUR LES PETITES COLLECTIVITÉS

Source cybermalveillance.gouv.fr

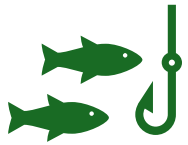
- Hameçonnage ou phishing
- Rançongiciels ou ransomwares
- Piratage de compte en ligne
- Arnaques au faux support technique

L'hameçonnage et/ou le piratage de compte sont utilisés pour réaliser des fraudes au Faux Ordre de Virement (FOVI)

CDG 76

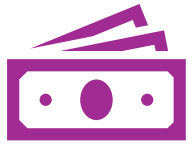
HAMEÇONNAGE

Technique qui leurre l'internaute pour l'inciter à communiquer des données personnelles ou professionnelles (identité / adresses / comptes / mots de passe / données bancaires…)



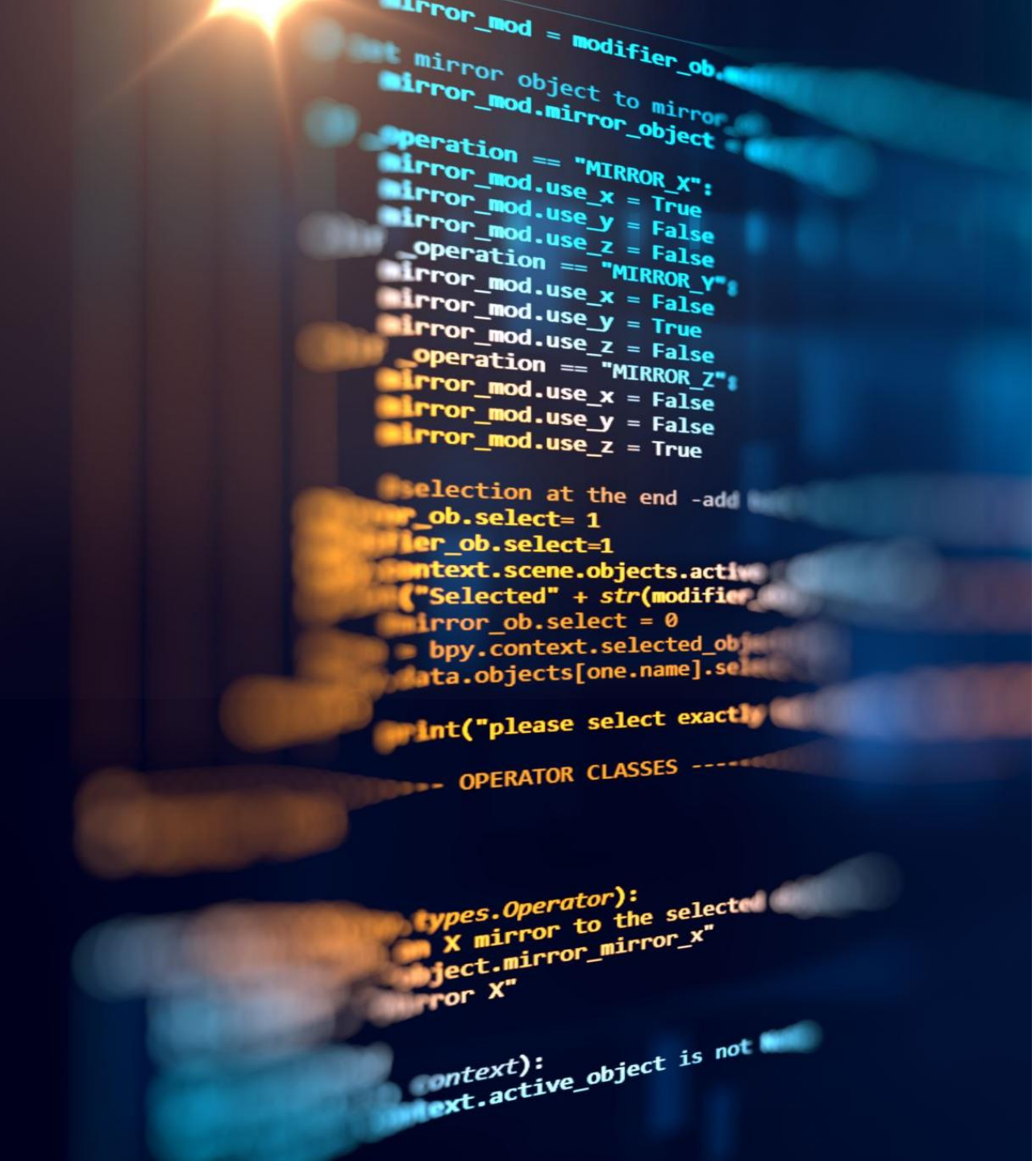
1 hameçon – 1 appât (sms, mail, téléphone, site frauduleux) – 1 victime

Usurpation de l'identité de l'organisme (Administration, Banque, Fournisseur…) – Mots clés pour détourner votre attention – Jouent sur l'urgence



But poursuivi : utilisation directe ou revente à des fins d'escroquerie / pour en faire un usage frauduleux

CDG 76



Rançongiciels

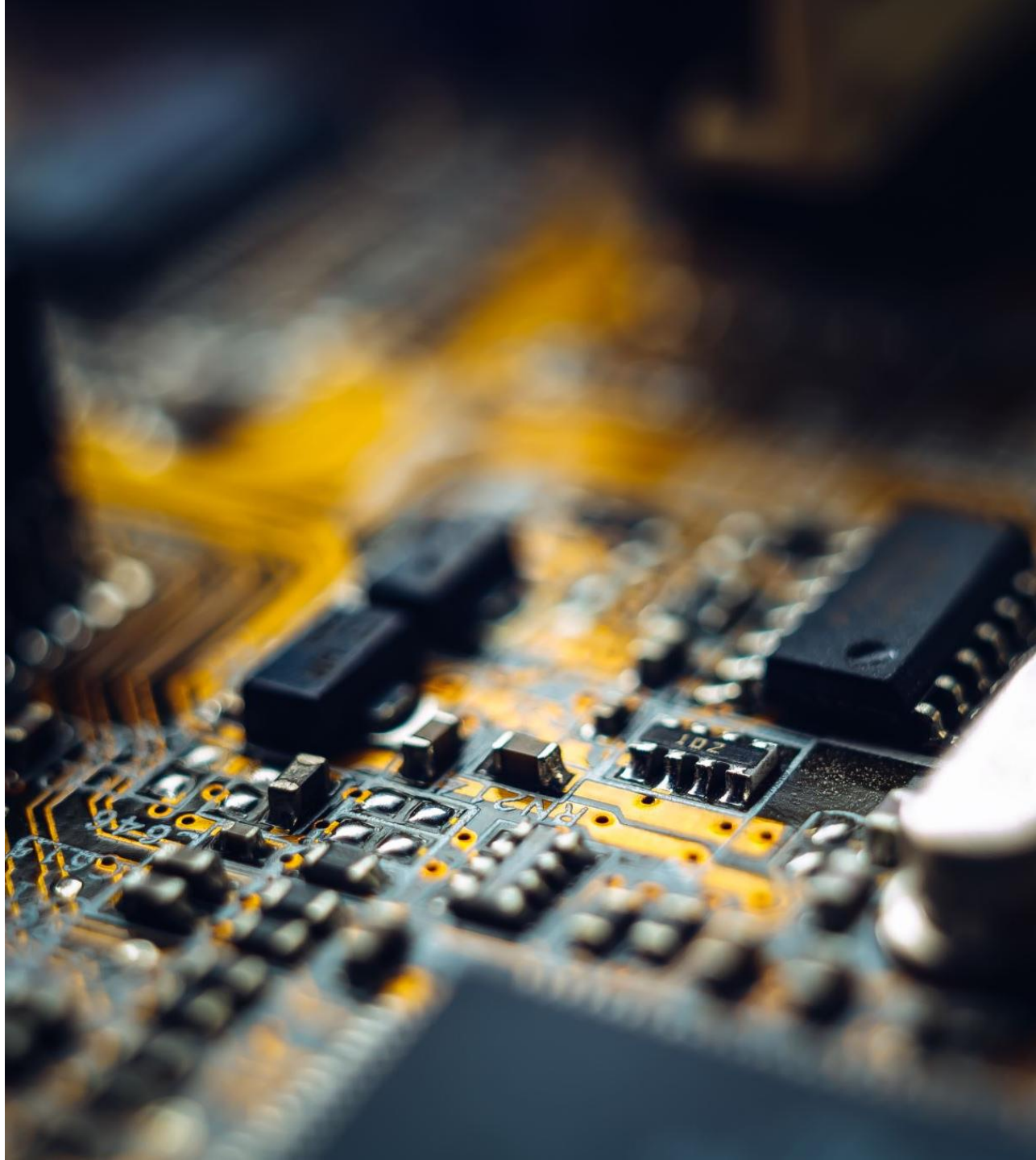
- Logiciel malveillant qui bloque l'accès à l'ordinateur et chiffre les fichiers
- Comment : l'infection passe par l'ouverture d'une pièce jointe et/ ou lien malveillant dans un courriel, la navigation sur des sites compromis ou l'intrusion dans le système par l'exploitation d'une vulnérabilité connue
- But poursuivi : extorsion de fonds ou endommagement du système de la victime pour générer des pertes d'exploitation ou porter atteinte à son image

Piratage de compte

- Prise de contrôle d'un compte (messagerie, administration, banque, e-commerce, réseau social) par un individu malveillant au détriment de son propriétaire légitime
- Comment : mot de passe trop simple / communication de votre mot de passe lors d'un hameçonnage / utilisation du même mot de passe sur plusieurs sites
- But poursuivi : usurpation d'identité, transactions frauduleuses / escroqueries, reventes de données personnelles et/ou professionnelles, spam

Arnaque au faux support technique

- Technique qui vise à vous effrayer prétextant un problème informatique grave et vous presse de rappeler un pseudo-service de dépannage
- Comment : via une fenêtre « pop-up », sms, tchat, courriel ou par téléphone
- But poursuivi : soutirer de l'argent pour un faux dépannage ou vous faire souscrire de faux abonnements, voire vous faire laisser prendre le contrôle de votre ordinateur



EXEMPLE

ACTIVITÉ Activités de service public diverses à mener (état civil, cimetière, voirie, espaces verts, cantines/distribution de repas, etc.)

PUBLIC Chaque citoyen de votre commune

DONNÉES Recueil de multiples données personnelles du fait des activités (administrés, agents, élus).

Protéger ces données est un enjeu majeur, notamment pour la confiance accordée par les citoyens à sa collectivité

Une cyberattaque induit une déclaration à la CNIL
En cas de violation des données → RGPD

CDG 76

RGPD
(Règlement Général sur la Protection des Données)

- Une **obligation règlementaire** en plusieurs étapes :
  1. **Désigner un Délégué à la Protection des Données** (sur le site de la CNIL)
  2. **Sensibiliser les agents et élus**
  3. **Réaliser le registre des traitements** de données personnelles
  4. **Ajouter des mentions d'information** sur les formulaires de collecte de DP
  5. Le cas échéant :
     - Répondre aux demandes d'exercice des droits (sous un mois)
     - Alerter la CNIL en cas de violation de Données Personnelles (sous 3 jours)

CDG 76

PARTIE 3

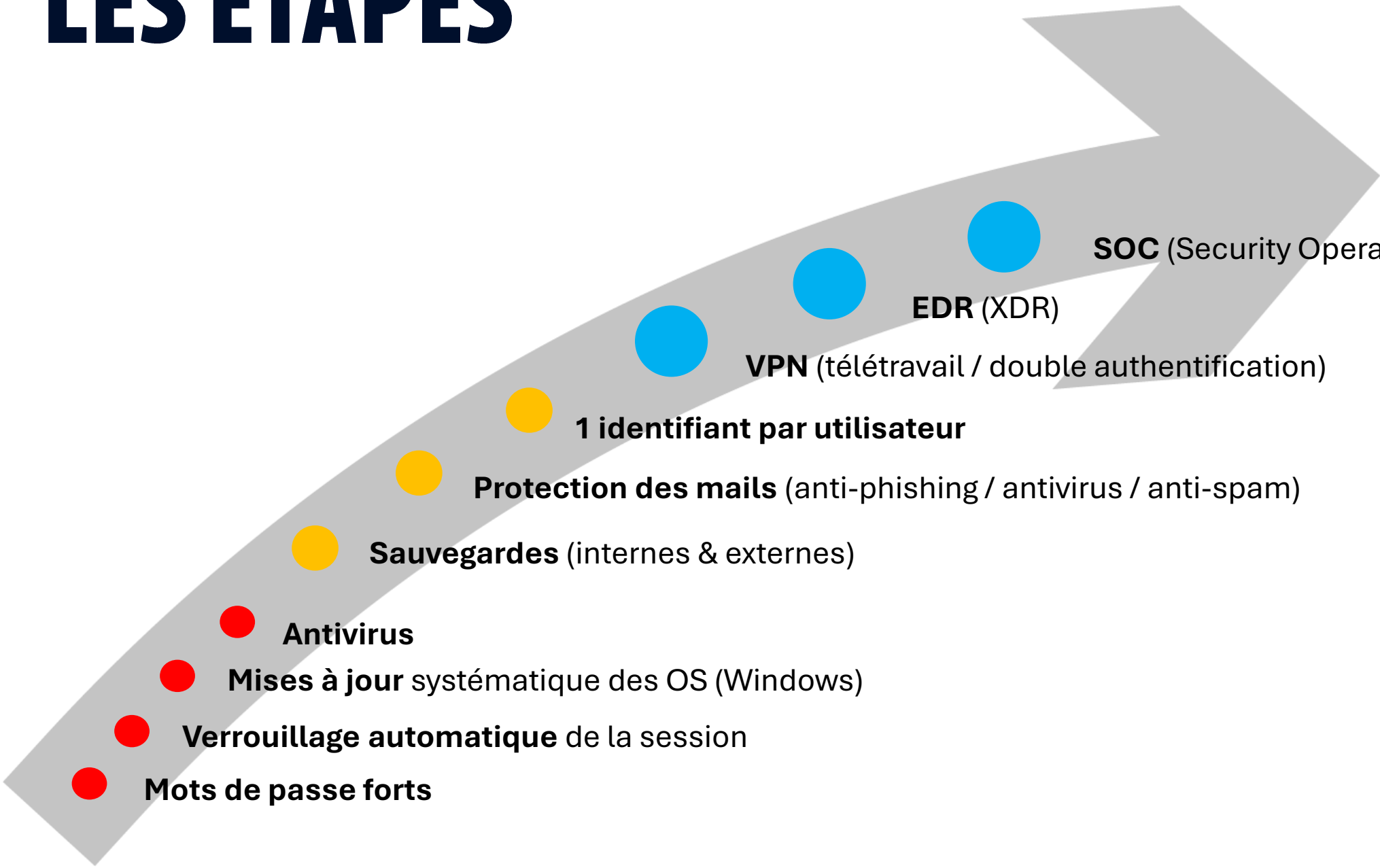
TÉMOIGNAGE

COMMUNE DE SEINE-MARITIME

PARTIE 4

TENDRE VERS UNE CYBERSÉCURITÉ DE QUALITÉ

LES ÉTAPES



CDG 76

CONTACTS

Magalie LANDEMAINE

07 88 64 45 35

cybercommunes@cdg76.fr

Raphaël FACCON

02 35 59 41 86

dpd@cdg76.fr

NOS SERVICES RESTENT
À VOTRE ÉCOUTE

CDG 76