Les
BONNES PRATIQUES
du télétravail

Sécurisez votre connexion internet

- **Assurez-vous du bon paramétrage de votre box Internet.** Vérifiez son mot de passe d'accès administrateur, changez-le s'il est faible et mettez à jour son logiciel interne. Le site web de votre opérateur (par exemple celui de Bouygues SFR, Orange et Free), vous accompagnera dans la bonne mise en œuvre de ces étapes.

- **Si vous utilisez le Wi-Fi**, activez l'option de chiffrement WPA2 ou WPA3 avec un mot de passe long et complexe (l'Agence nationale de la sécurité des systèmes d'information (ANSSI) recommande par exemple une vingtaine de caractères). Désactivez la fonction WPS et supprimez le Wi-Fi invité. Ne vous connectez qu'à des réseaux de confiance et évitez les accès partagés avec des tiers.

Si vous devez utiliser un ordinateur personnel, assurez-vous qu'il est suffisamment sécurisé

Cela doit passer par :

- l'installation d'un antivirus et d'un pare-feu. Si vous êtes sur le système d'exploitation *Windows 10*, vérifiez l'état de vos systèmes de protection au moyen du centre de sécurité ;

- l'utilisation d'un compte dédié au travail avec des droits limités, protégé par un mot de passe fort et non partagé avec d'autres personnes (par exemple avec d'autres membres de votre famille) et sur lequel les applications installées sont uniquement nécessaires pour le travail ;

- la mise à jour régulière du système d'exploitation et des logiciels utilisés, notamment le navigateur web et ses extensions. Supprimez ou passez au plus vite à une version récente des logiciels dont le support ou la mise à jour sont abandonnés, comme le système d'exploitation *Windows 7* (et les versions antérieures comme *Windows XP*) dont la sécurité n'est plus assurée depuis le 14 janvier 2020 ;

- des sauvegardes régulières de votre travail sur un support externe de type clé USB ou disque dur externe. Si vous êtes sur le système d'exploitation *Windows 10*, configurer vos sauvegarde en suivant l'assistance Windows. Si vous utilisez un ordinateur Mac, consultez l'assistance Apple ;

- l'utilisation de mots de passe forts pour ouvrir votre compte, mais aussi pour accèder aux services/logiciels à distance, et l'activation de l'authentification à deux facteurs (clef d'authentification, SMS) dès que cela est proposé par le service. Les gestionnaires de mots de passe, par exemple les logiciels KeePass ou ZenyPass, vous permettront de sécuriser leur stockage et leur gestion.

La CNIL propose un outil pour créer rapidement des mots de passe robustes ainsi qu'un tutoriel pour utiliser le gestionnaire de mots de passe Keepass.

Communiquez en toute sécurité

Évitez de transmettre des données confidentielles via des services grand public de stockage, de partage de fichiers en ligne, d'édition collaborative ou via des messageries. À défaut, chiffrez les données avant de les transmettre et transmettez les clés de chiffrement par un canal de communication distinct (par exemple, communication du mot de passe par téléphone ou SMS). Des logiciels grand public comme 7-zip pour *Windows* et 7zX pour *Mac OSX* permettent de chiffrer les données avec des algorithmes réputés fiables.

Utilisez une adresse de messagerie dédiée pour votre activité diocésaine/ sanctuaire, distincte de votre messagerie personnelle. Si le diocèse/sanctuaire ne peut pas vous fournir un compte de messagerie de type prénom.nom@diocèse.fr, créez-vous un compte chez Google ou Hotmail (réputés pour la sécurité), non partagé avec les personnes de votre entourage.

Si vous devez utiliser votre téléphone personnel, protégez vos données et limitez les accès

Parce qu'ils vous accompagnent partout, les téléphones portables sont particulièrement exposées à la perte et aux vols:

Évitez d'y enregistrer des informations confidentielles: codes secrets, codes d'accès, coordonnées bancaires, etc ;

Activez le code PIN et mettez en place un délai de verrouillage automatique du téléphone
Évitez les codes trop faciles (date de naissance, 0123, etc.) ;

Activez le chiffrement des informations sur votre téléphone lorsque c'est possible ;

Notez le numéro « IMEI » du téléphone pour le bloquer en cas de perte ou de vol ;

N'installez des logiciels que depuis les plateformes officielles et évitez à tout prix les applications de sources inconnues ;

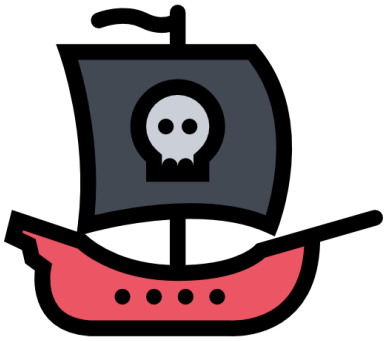
Lorsque vous installez de nouvelles applications sur votre appareil, **lisez les conditions d'utilisation et la politique de confidentialité et limitez les données auxquelles elles peuvent avoir accès au strict nécessaire** ;

Réglez les paramètres de géolocalisation afin de toujours contrôler **quand et par qui être géolocalisé**.

Si vous en avez la possibilité, utilisez l'ordinateur mis à votre disposition par le diocèse/sanctuaire

Privilégiez l'emploi d'un VPN (Virtual Private Network ou réseau privé virtuel) pour vous connecter au serveur du diocèse/sanctuaire. Renseignez-vous auprès de l'économe ou du responsable informatique.

Veillez à la sécurité de l'ordinateur. Eteignez-le et rangez-le à la fin de votre travail.



Soyez particulièrement vigilant sur les tentatives de piratage

Les pirates profitent des périodes de crise ou de trouble pour inventer de nouvelles escroqueries et tirer profit de ces événements. Soyez vigilant à tout contact :

de personnes que vous ne connaissez pas, surtout si elles vous invitent à cliquer sur des liens ou à ouvrir un fichier;

d'une personne connue vous envoyant une communication inhabituelle. Essayez de vérifier cette information par un autre canal (téléphone, SMS, mail);

de personnes cherchant à créer un sentiment d'urgence, de danger ou de secret. Le cas échéant, toujours utiliser un autre canal pour vérifier les informations communiquées, par exemple en effectuant une recherche sur Internet.

En cas de doute, demandez de l'aide à votre éconme ou au responsable informatique du diocèse.