Soyez Vigilants !

Bonnes Pratiques Sécurité

Le travail collaboratif et à distance ont connu un développement particulièrement important depuis le début de la crise sanitaire. Cela est une expérience très enrichissante pour la Fédération comme pour de nombreuses entreprises, mais un désastre pour celles qui sont victimes de cyberattaques.

La Fédération met à votre disposition différents moyens collaboratifs à travers les applications d'Office 365 pour faciliter vos activités et mener à bien vos projets ; le courrier électronique (Outlook), applications de visio-conférences (Teams), des applications de création et de stockage de documents (OneDrive). Ces moyens collaboratifs qui constituent en partie notre système d'information*, peuvent à tout instant être compromis par ces cyberattaques

Système d'Information* : l'ensemble des moyens et ressources d'une entreprise qui permettent la gestion de l'information et des données professionnelles et personnelles (RGPD) ; leur disponibilité, intégrité, confidentialité et traçabilité

Il est donc indispensable de protéger notre système d'information et de vous sensibiliser aux bonnes pratiques sécurité à adopter pour un meilleur usage de vos PC et téléphones mobiles

Les principales menaces informatiques qui existent à l'heure actuelle - Soyez vigilant et remontez immédiatement tout incident à l'adresse office365@ffradonnee.fr ; capture d'email douteux, dysfonctionnement ou blocage anormal d'Office 365, etc.

- **Phishing (hameçonnage)** : cette menace se présente sous la forme d'emails incitants l'utilisteur à cliquer sur un lien ou à ouvrir une pièce jointe. Le but des auteurs de phishing est d'obtenir des informations personnelles de leurs victimes. On reconnaît souvent un email de phishing à son orthographe douteuse et à sa mise en forme bâclée ; voir ci-dessous le chapitre sur la gestion des emails pour plus d'explications
- **Les malwares dont les plus dangereux sont ransomwares (rançongiciels**). Ces derniers sont particulièrement sophistiqués et néfastes. Ils s'installent tout seuls et peuvent désactiver l'anti-virus. Les téléchargements sur des sites à risque constituent l'une des pratiques qui exposent le plus aux ransomwares

De nouvelles variantes de logiciels malveillants et intrusifs* apparaissent régulièrement. Protégez vos appareils professionnels en installant un logiciel anti-virus et vérifiant souvent les mises à jour pour rester à l'abri de ces menaces

Ci-après quelques noms de logiciels reconnus ; Trend Micro, Bitdefender, Avast

Assurez que vos logiciels PC et navigateurs internet sont à jour. Les mises à jour incluent régulièrement des correctifs qui résolvent des vulnérabilités sécurité nouvellement identifiées

Usages pro-perso : - Ne mélangez pas votre messagerie professionnelle et personnelle

Ce serait, en effet, le meilleur moyen de ne plus vous y retrouver et de faire des erreurs, notamment des erreurs de destinataires ; par exemple, envoyer par erreur des informations confidentielles de la fédération à des contacts personnels qui pourraient en faire un mauvais usage, ou à l'inverse voir un message trop personnel circuler dans votre environnement professionnel alors que vous ne le souhaitez pas.

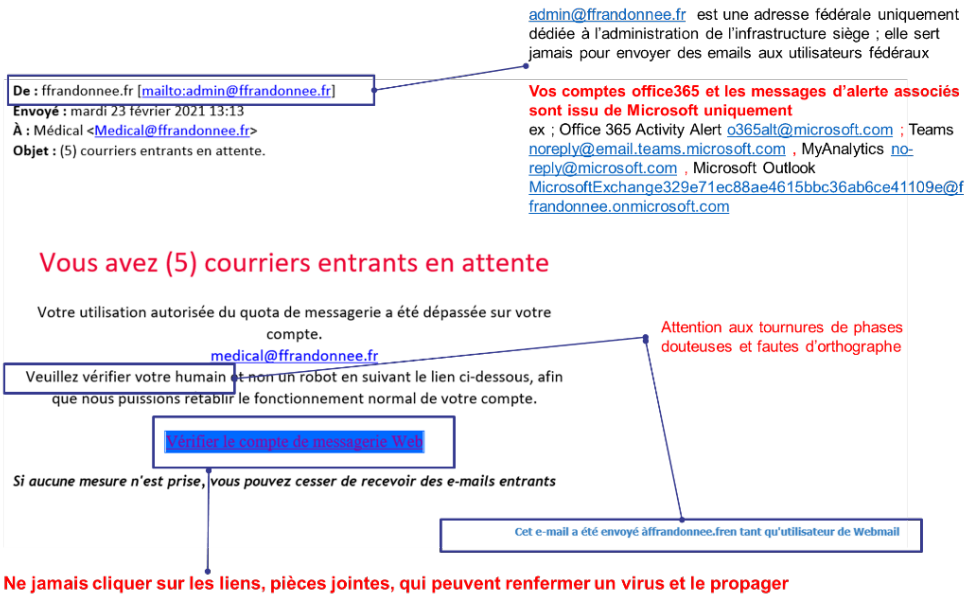
De plus, votre messagerie personnelle est généralement bien moins sécurisée que votre messagerie professionnelle, Vous faire pirater votre email personnel pourrait mettre en danger les activités métiers & numériques de la Fédération

Les emails constituent la principale méthode d'infection. Soyez attentifs aux emails reçus, surtout s'ils contiennent des liens et/ou des pièces jointes. Ces faux emails reprennent les noms et logos de vraies sociétés connues et comportent souvent des erreurs d'orthographe ou de syntaxe.

- Vérifiez l'adresse de l'expéditeur qui peut ressembler à la véritable adresse mais va différer par un petit détail, ex. l'expéditeur n'est pas de la forme « *adressemail@société.com* »
- Ne pas cliquer sur un lien dans un email : allez sur le web et saisissez vous-même l'adresse dans le navigateur pour vérifier le lien.

Si vous avez un doute, **NE TRANSFÉRER JAMAIS CES EMAILS à des destinataires** ; préférer envoyer une capture écran de l'email reçu à l'adresse office365@ffrandonnee.fr car ils peuvent contenir des virus, infecter leur PC, voir se propager à tout le réseau fédéral

Méfiez-vous particulièrement des emails concernant vos comptes office 365 avec pièces jointes ou des liens vous conseillant d'activer des macros pour les visualiser.



La sauvegarde des données importantes représente la méthode la plus efficace pour combattre les infections par les Ransomware

- Sauvegardez vos données professionnelles sur plusieurs supports ; 3 minimum tels qu'un disque externe dédié exclusivement à cette opération. Vous pouvez utiliser OneDrive ou SharePoint dont les données sont stockées sur les serveurs Microsoft mais ne garantissent pas leurs sauvegardes en cas de perte de fichiers
- Évitez les clés USB déjà utilisées sur d'autres PC
- Pour vos contacts, sauvegarder les régulièrement en effectuant un export depuis votre Outlook. Ceci permettra de prévenir rapidement vos contacts en cas d'usurpation d'identité

La sécurité de vos données passe aussi par la complexité et la longueur de vos mots de passe ; cela concerne tous vos outils informatiques (PC, tél. mobile, wifi, accès aux sites internet, etc.). Vos mots de passe doivent comporter à minima une combinaison alphanumérique de 8 caractères ou plus pour mieux vous protéger. Vous pouvez composer des mots de passe avec des phrases difficiles à pirater (ex : F@d1haev2! - "Face au danger un homme averti en vaut deux !").

IMPORTANT : - Fin février 2021 nous vous avons informé du piratage de près de 3,2 milliards d'emails et mots de passe dans le monde entier; ci-joint deux liens pour vérifier si vos comptes emails ont été touchés, https://haveibeenpwned.com/ , https://cybernews.com/personal-data-leak-check/

Vous pouvez tester vos comptes emails personnels avec ces mêmes liens

Si l'un de vos comptes office365 est corrompu, contactez rapidement le office365@ffrandonnee.fr pour modifier votre mot de passe

- Pour stocker vos mots de passe, privilégiez des logiciels dédiés tels que Keepass. Éviter d'enregistrer vos mots de passe sur Internet, qui n'est pas suffisamment sécurisé pour les protéger

Votre téléphone mobile peut aussi être vecteur d'attaques dont les plus répandues sont les applications malveillantes, « fausses Apps » assez bien réalisées pour se faire passer pour des vraies. Leur but : - Endommager et/ou détruire un système d'information, voler, modifier ou supprimer des données, mais aussi afficher des publicités

Voici quelques bons réflexes à adopter :

- Choisissez un mot de passe complexe ;
- Effectuez toutes les mises à jour demandées par le système d'exploitation de votre mobile ou les applications téléchargées
- Ne pas télécharger d'applications hors des Apps Store officiels
- Ne jamais communiquer vos données personnelles par email ou sms, même aux instances officielles, tout simplement parce qu'elles ne le demandent jamais
- Contrôlez les autorisations de vos applications et désactivez les options trop intrusives et inutiles au fonctionnement de l'application

Si vous avez un doute ou des questions, veuillez envoyer un email à l'adresse office365@ffrandonnee.fr

Nous vous communiquons un lien vers le site cybermalveillance.gouv.fr , qui a créé un kit de sensibilisation aux questions numériques afin de partager les bonnes pratiques dans les usages personnels et professionnels