Association Hospitalière de Bourgogne Franche-Comté

SÉCURITÉ NUMÉRIQUE

Adopter les bonnes pratiques...

LES MOTS DE PASSE

Votre mot de passe , comme votre compte, est le même pour la majorité des logiciels : *pensez à le changer au minimum tous les 6 mois.*
Il doit être suffisamment long (> 8 caractères), assez complexe (majuscule, minuscule, chiffre et caractères spéciaux) et impossible à deviner.
Ne le communiquez jamais à un tiers !

LES SAUVEGARDES

Les sauvegardes sont gérées par le service informatique pour tous les postes qui sont sur le réseau de l'AHBFC et pour l'ensemble des serveurs.
Sur chaque poste la sauvegarde est effectuée uniquement pour le dossier « Mes documents » : *il est donc impératif d'enregistrer ces données dans ce dossier spécifique*. En cas de doute, vous pouvez adresser un mail à hotline@ahbfc.fr

LES MISES À JOUR

Les mises à jour sont faites automatiquement sur chaque poste distant.
Pour qu'elles puissent être installées, il est impératif de redémarrer régulièrement les postes pour que ces mises à jour puissent être installées, y compris les PC portables !

LES USAGES PRO-PERSO

DISTINGUEZ LES :
Choisissez des mots de passe différents pour tous les services professionnels et personnels auxquels vous accédez ;
Ne mélangez pas vos messageries professionnelle et personnelle ;
N'utilisez pas de service de stockage en ligne personnel à des fins professionnelles, etc.

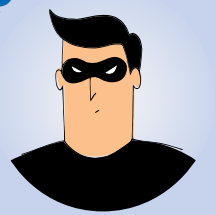
MAI 2022 - Infographie adaptée par l'AHBFC à partir du site **www.cybermalveillance.gouv.fr**

Association Hospitalière de Bourgogne Franche-Comté

SÉCURITÉ NUMÉRIQUE

Comprendre les risques et réagir

CYBERCRIMINEL



L'HAMEÇONNAGE

VOL DE DONNÉES

Vous recevez un message ou un appel inattendu, voire alarmant, d'une organisation connue et d'apparence officielle qui vous demande des informations personnelles ou bancaires ? Vous êtes peut-être victime d'une attaque par hameçonnage (*phishing* en anglais) !

BUT

Voler des informations personnelles ou professionnelles (identité, adresses, comptes, mots de passe, données bancaires…) pour en faire un usage frauduleux.

TECHNIQUE

Leurre envoyé *via* un faux message, SMS ou appel téléphonique d'administrations, de banques, d'opérateurs, de réseaux sociaux, de sites d'e-commerce…

LES RANÇONGICIELS

EXTORSION D'ARGENT

Vous ne pouvez plus accéder à vos fichiers et on vous demande une rançon ? Vous êtes victime d'une attaque par rançongiciel (*ransomware*, en anglais) !

BUT

Réclamer le paiement d'une rançon pour rendre l'accès aux fichiers verrouillés.

TECHNIQUE

Blocage de l'accès à des données par envoi d'un message contenant des liens ou pièces jointes malveillantes ou par intrusion sur le système.

L'ARNAQUE AU FAUX SUPPORT TECHNIQUE

ESCROQUERIE FINANCIÈRE

Votre ordinateur est bloqué et on vous demande de rappeler un support technique ? Vous êtes victime d'une arnaque au faux support !

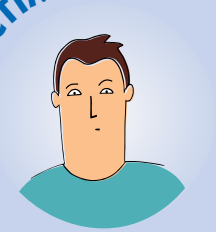
BUT

Inciter la victime à payer un pseudo-dépannage informatique et/ou la faire souscrire à des abonnements payants

TECHNIQUE

Faire croire à un problème technique grave impliquant un risque de perte de données ou d'usage de l'équipement (par écran bloqué, téléphone, SMS, courriel etc.).

VICTIME



COMMENT RÉAGIR ?

- Ne communiquez jamais d'information sensible suite à un message ou à un appel téléphonique
- Au moindre doute, contactez le service informatique par téléphone au 1999 ou par mail à hotline@ahbfc.fr (sans transférer le mail douteux le cas échéant)
- Changez vos mots de passe divulgués/compromis
- Faites opposition immédiatement (en cas d'arnaque bancaire)

- Arrêtez votre poste informatique
- Alertez le service informatique :
  au 1999 du lundi au vendredi de 8h30 à 17h00 (16h00 le vendredi), sauf jours fériés,
  ou par mail à hotline@ahbfc.fr
  (copie à rssi@ahbfc.fr) en dehors de ces créneaux
- Ne payez pas la rançon
- Ne rebranchez pas le poste tant que le service informatique n'est pas intervenu

- Ne répondez pas
- Conservez toutes les preuves
- Arrêtez votre poste informatique
- Alertez le service informatique :
  au 1999 du lundi au vendredi de 8h30 à 17h00 (16h00 le vendredi), sauf jours fériés,
  ou par mail à hotline@ahbfc.fr
  (copie à rssi@ahbfc.fr) en dehors de ces créneaux
- Ne rebranchez pas le poste tant que le service informatique n'est pas intervenu

Mai 2022 - Infographie adaptée par l'AHBFC à partir du site **www.cybermalveillance.gouv.fr**