Quelques gestes simples pour mieux se prémunir de la menace

IDENTIFICATION

1 - Vos mots de passe doivent être :
- Notés nulle part
  (sauf coffre-fort numérique type Keepass)
- Renouvelés régulièrement
- Strictement personnels (non partagés)
- Suffisamment longs
  (12 caractères minimum)
- Suffisament complexes
  (Lettres, chiffres, caractères spéc.)

2 - Si possible, préférez la double-authentification (A2F)

3 - Ne transmettez jamais vos identifiants !

COMMUNICATIONS

1 - e-mails = Vecteur d'attaque n°1
Soyez donc vigilants !
Connaissez-vous l'émetteur ? Êtes-vous sûr de son identité ?
Attendiez-vous ce message ? Le message est-il cohérent ?

2 - Posture de prudence : un mail est dangereux jusqu'à preuve du contraire (et pas l'inverse)

3 - En cas de doute : Supprimer un mail est moins grave que de subir une attaque informatique !

4 - On peux vous attaquer/manipuler par téléphone, fax ou sur les réseaux sociaux, attention aux informations que vous donner : Êtes-vous bien sûr(e) de qui est à l'autre bout ?

1 - Votre système informatique est un "organisme vivant" qui doit être entretenu.

2 - Les mises à jour mensuelles (Windows) permettent de combler des failles et sécurisent vos ordinateurs. Il est important de les appliquer régulièrement.

3 - Vos programmes tiers (médicaux...) **doivent être régulièrement mis à jour** (pour les mêmes raisons).

HYGIENE NUMERIQUE

1 - Vos postes informatiques doivent être protégés par des solutions de sécurité à jour antivirus, parefeu...)

2 - Vos données numériques doivent être sauvegardées régulièrement sur un support externe sécurisé.

3 - Attention, les clés USB extérieures peuvent mettre en danger vos ordinateurs.

4 - Déclarez tout incident de sécurité survenu (CERT Santé)

PROTECTION NUMERIQUE

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
ars Agence Régionale de Santé Normandie
L'Assurance Maladie
nes normand'e.santé
AGENCE DU NUMERIQUE EN SANTÉ
MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ
SÉGUR NUMÉRIQUE