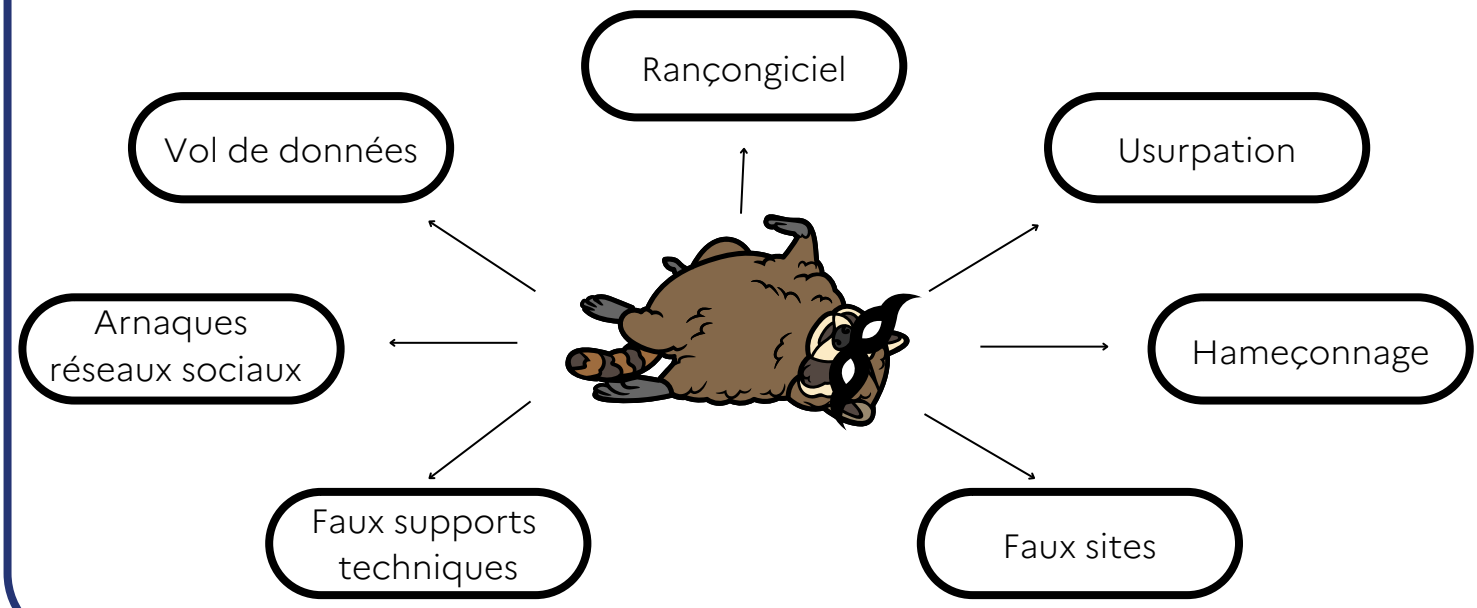
LA CYBERSÉCURITÉ

FICHE RÉSUMÉ

LES MENACES



LES BONNES PRATIQUES POUR UTILISER LE WEB EN TOUTE SÉCURITÉ

Utiliser des mots de passes robustes

- Longueur : 10 caractères minimum, 12 caractères c'est encore mieux !
- Majuscules, minuscules, chiffres et caractères spéciaux
- Pas d'informations personnelles (nom, prénom, date de naissance, noms des enfants ....
- **NE JAMAIS COMMUNIQUER VOS MOTS DE PASSES**
- Un mot de passe différent pour chaque service autant que possible
- Utiliser un gestionnaire de mot de passe

Financé par GOUVERNEMENT Liberté Égalité Fraternité
FRANCE RELANCE
Financé par l'Union européenne NextGenerationEU
St Médard d'Excideuil
CONSEILLER NUMÉRIQUE France services

Utiliser un Antivirus et un pare-feu.

Réaliser les mises à jours sur votre ordinateur et autres appareils dès que possible

ETRE ATTENTIF AUX TENTATIVES DE HAMEÇONNAGE

Voici les principaux signaux d'alertes

- Demande de mise à jour ou de confirmation de données personnelles – identifiants, mots de passe, coordonnées bancaires… – par un prétendu organisme public ou commercial de confiance, sous peine de sanction.
- Défaut de paiement ou problème de facturation : un faux mail vous informe qu'un bien ne peut être expédié en raison d'un problème de facturation ou que vous devez régler un impayé.
- Demande d'informations inattendue pour un remboursement, une annulation de commande, une livraison, etc.
- Demande d'informations contre l'envoi d'un cadeau ou pour participer à un jeu-concours avec un gain attrayant, ou encore pour récupérer le gain d'une loterie.
- Demande de règlement pour éviter la fermeture d'un accès, la perte d'un nom de domaine ou une prétendue mise en conformité RGPD.
  Appel aux dons frauduleux.
- Appel à l'aide : le cybercriminel se fait passer pour un proche, expliquant qu'il se trouve dans une situation désastreuse qui requiert votre aide financière.
- Les chaînes d'emails type porte-bonheur, pyramide financière, appel à solidarité ou alerte virale, peuvent dissimuler une tentative de phishing.

Télécharger uniquement sur des sites officiels

Sauvegarder régulièrement les données importantes pour ne pas les perdre en cas d'attaque

NE PAS SAUVEGARDER vos coordonnées bancaire sur votre navigateur.
Aucun service de l'Etat ou entreprise ne vous demanderont vos coordonnées bancaires par mail ou sms

ÊTRE VIGILANT SUR LES RÉSEAUX SOCIAUX

Vos compte de réseaux sociaux peuvent contenir des informations personnelles sensibles.

Protéger votre compte avec un mot de passe robuste.

Attention aux faux profils ou faux compte, ne discuter qu'avec des personnes que vous connaissez.

Vérifiez vos paramètres de confidentialité.

Notes :

Financé par GOUVERNEMENT Liberté Égalité Fraternité
FRANCE RELANCE
Financé par l'Union européenne NextGenerationEU
St Médard d'Excideuil
CONSEILLER NUMÉRIQUE France services