Document exemple : version corrigée, accessible

Sécurité informatique

# Les dangers

Bien suivre les bonnes pratiques de sécurité informatique permet :

* D’éviter de perdre des données : un nouveau type de virus, les « ransomware » tentent de chiffrer et détruire vos fichiers.
* D’éviter de se faire voler des informations personnelles : par exemple, de garder en sécurité ses comptes bancaires, vos informations médicales, et d’autres informations sur vous qui peuvent être utilisées pour vous nuire, même si « vous n’avez rien à cacher ».
* D’éviter de faire courir les mêmes risques avec les personnes avec qui vous échangez des fichiers, qui sont dans vos adresses email de contact, qui sont sur le même réseau… Des techniques fréquemment utilisées par les virus informatiques pour se propager à vos amis.

# Les mails

Lorsque vous recevez un email, n’ouvrez pas de pièce jointe ou de lien si vous n’êtes pas sûr de pouvoir faire confiance à l’expéditeur. Même si vous connaissez l’expéditeur, les virus peuvent envoyer des mails avec une fausse adresse. Faites attention si vous passez la souris sur un lien ou un bouton, vous voyez apparaître l’adresse de destination en bas de la fenêtre, vérifiez que le nom de domaine (ce qu’il y a juste avant le 3eme « / », par exemple **utc.fr/** dans https://ent.**utc.fr/**ma-page-web/machin-truc/) correspond bien au site de l’institution officielle et bien orthographiée que vous souhaitez contacter.

Mail qui vous envoie vers un faux site de banque, pour vous voler vos codes