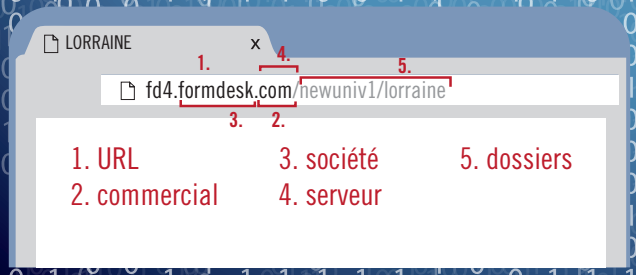
EXERCER UNE CULTURE DE SÉCURITÉ

Le bon sens peut suffire pour vous éviter des désagréments :

- Faites attention aux mails et leurs pièces jointes pouvant contenir des virus
- N'activez pas de macros dont le virus pourrait modifier ou remplacer le macro d'origine,
- Pensez à modérer, à l'aide d'un mot de passe, l'accès à votre poste ainsi qu'à tous vos appareils connectés,
- Verrouillez votre session de travail dès que vous quittez votre poste pour de longues minutes,
- Lors d'achats en ligne, assurez-vous que le site marchand vous propose une URL en httpS (le « S » signifiant Sécurisé)

Attention aux phishing !

Apprenez à lire les URLS avant de cliquer dessus :



RANÇON-NING, PHISHING, HACKING...

le numérique fait aujourd'hui partie intégrante de notre quotidien mais la sécurité est très rarement pris en compte dans nos usages. Aujourd'hui un appareil connecté non protégé peut subir très facilement des intrusions, des contaminations, des dégradations,...

En cas du moindre doute ou d'incident constaté, vous devez immédiatement alerter votre informaticien de proximité qui fera le relais vers les correspondants et les responsables sécurité.

Pour cela contactez l'adresse :
rssi@univ-lorraine.fr

UNIVERSITÉ DE LORRAINE

CYBER SECURITÉ

LES BONNES PRATIQUES INFORMATIQUES

OCTOBRE 2016

LES MOTS DE PASSE :

LA CLÉ D'ACCÈS À VOS DONNÉES PERSONNELLES

De nos jours, les mots de passe sont omniprésents dans notre quotidien. Il est donc nécessaire de protéger vos informations personnelles de façon judicieuse :

- Dans la mesure du possible, utilisez un mot de passe unique par service utilisé,
- Evitez de rassembler tous les services utilisés dans un seul et même endroit,
- Dès le moindre doute, modifiez votre mot de passe sur : **sesame.univ-lorraine.fr**

Il est parfois difficile de mémoriser plusieurs mots de passe complexes. C'est pourquoi des logiciels, disponibles gratuitement sur internet, permettent de les centraliser et de les crypter en lieu sûr.

ATTENTION !

Ne jamais communiquer vos mots de passe :
ces derniers sont strictement personnels. Même les services informatiques ne peuvent vous les demander.

LA MISE À JOUR RÉGULIÈRE DE VOS APPAREILS CONNECTÉS

Qu'il s'agisse d'applications, de logiciels ou bien de systèmes d'exploitation, des vulnérabilités existent. C'est pourquoi des mises à jour de sécurité sont régulièrement proposées par les éditeurs afin de les corriger et d'éviter toute cyber-attaque. Il est donc essentiel d'avoir des appareils connectés à jour en appliquant de façons régulières les mises à jour proposées. De cette façon, l'accès à vos appareils sera beaucoup plus difficile pour les pirates. Pour cela il est important de :

- Mettre à jour vos applications (Flash Player, une suite bureautique,…) et anti-virus, mais uniquement sur les sites officiels des éditeurs,
- Penser à vérifier l'origine des mises à jour, ne pas télécharger de produits douteux,
- Ne pas oublier que vos appareils professionnel sont gérés par l'équipe informatique et que vos appareils personnels le sont par vous-même

En cas de doute, n'hésitez pas à demander conseil et assistance à votre équipe informatique.

PENSEZ AUX SAUVEGARDES !

Il est vivement conseillé d'effectuer régulièrement des sauvegardes afin que vos données soient en sécurité. Il sera alors plus simple pour vous de les récupérer en cas de dysfonctionnement ou d'une attaque. Pour cela vous pouvez :

- Effectuer des sauvegardes sur les supports externes (les DVD par exemple)
- Utiliser l'espace de stockage commun de l'établissement ou bien sur bul.univ-lorraine.fr

Il est préférable de privilégier les services de stockage de l'université plutôt que les services externes (Google drive, Dropbox, Icloud,…) afin de pouvoir bénéficier d'une assistance technique en cas de problème.