GOUVERNEMENT DE LA NOUVELLE-CALÉDONIE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

vice-rectorat de la Nouvelle-Calédonie
direction générale des enseignements

Formation RNT et Nouveaux RNE

Point sur la sécurité

24 juillet 2018

- Point sur la sécurité
  - Les règles sur les mots de passe
  - Les règles sur les mises à jour
  - Les règles sur les antivirus
  - Les règles sur les locaux

Formation RNT et Nouveaux RNE

Point sur la sécurité
- Les règles sur les mots de passe

Pour protéger vos informations, il est nécessaire de choisir et d'utiliser des mots de passe robustes, c'est-à-dire difficiles à retrouver à l'aide d'outils automatisés et à deviner par une tierce personne.

Voici quelques recommandations :

- Utilisez un **mot de passe unique pour chaque service**. En particulier, l'utilisation d'un même mot de passe entre sa messagerie professionnelle et sa messagerie personnelle est impérativement à proscrire ;
- Choisissez un **mot de passe qui n'a pas de lien avec vous** (mot de passe composé d'un nom de société, d'une date de naissance, etc.) ;
- **Ne demandez jamais à un tiers de générer pour vous un mot de passe** ;
- **Modifiez systématiquement et au plus tôt les mots de passe par défaut** lorsque les systèmes en contiennent ;
- **Renouvelez vos mots de passe** avec une fréquence raisonnable. **Tous les 90 jours** est un bon compromis **pour les systèmes contenant des données sensibles** ;
- **Ne stockez pas les mots de passe dans un fichier** sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur Internet), **encore moins sur un papier** facilement accessible ;
- **Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle** ;
- **Configurez** les logiciels, y compris **votre navigateur web**, pour qu'**ils ne se « souviennent » pas** des mots de passe choisis.

La robustesse d'un mot de passe dépend en général d'abord de sa complexité, mais également de divers autres paramètres, expliqués en détail dans le document Recommandations de sécurité relatives aux mots de passe.

Si vous souhaitez une règle simple : choisissez des mots de passe d'au moins 12 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux).

Deux méthodes pour choisir vos mots de passe :

- La méthode phonétique : « J'ai acheté huit cd pour cent euros cet après-midi » deviendra ght8CD%E7am ;
- La méthode des premières lettres : la citation « un tien vaut mieux que deux tu l'auras » donnera 1tvmQ2tl'A.

Chaque jour, des vulnérabilités sont mises en évidence dans de très nombreux logiciels largement utilisés.

En règle générale, quelques heures seulement sont suffisantes pour que des codes malveillants exploitant ces vulnérabilités commencent à circuler sur Internet.

Il est donc très important d'utiliser en priorité des **technologies pérennes** dont la **maintenance est assurée**, d'**éviter les technologies trop innovantes** ou **non maîtrisées** en interne et de respecter les recommandations suivantes.

Connaître les modalités de mises à jour de l'ensemble des composants logiciels utilisés.

Commencez par les composants de base

- **système d'exploitation**
- **suite bureautique**
- **navigateur web**
- outils nécessaires à la navigation – tels que la **machine virtuelle Java** ou le **lecteur Flash**
- **visionneuses de document**

Puis compléter l'inventaire avec l'ensemble des autres composants logiciels.

Formation RNT et Nouveaux RNE

vice-rectorat
de la Nouvelle-Calédonie
direction générale des enseignements

Il est **indispensable** d'avoir sur **chaque PC** un bon **antivirus mis à jour** le plus régulièrement possible. Tous les antivirus ne sont pas équivalents. Ils sont plus ou moins performants et certains peuvent laisser passer des virus ou ne pas savoir correctement les éradiquer lorsqu'une machine est infectée.

Le ministère de l'éducation à fait l'acquisition de **Trend Micro Office scan**.

- Le serveur installé sur le WSUS
- Le client installé sur chaque ordinateur du réseau Administratif et Pédagogique

Quelque règles à suivre pour éviter une contamination :

- **Ne jamais raccorder une machine sur le réseau sans un antivirus mis à jour**.
- Toujours **scanner** une **clé USB** avant d'ouvrir un document stocké dessus
- **Vérifier** qu'il **se met bien à jour**
- Ne **jamais** le **désactiver**
- Si le message ne vous semble pas "normal" (texte incohérent semblant provenir d'une personne que vous connaissez, titre alléchant, ...) et s'il contient un fichier joint, n'ouvrez surtout pas ce fichier, ne cliquez pas dessus ! C'est la méthode "traditionnelle" de transmission des virus.
- De même, **n'acceptez jamais**, lorsque vous naviguez sur le web ou lorsque vous discutez via IRC, MSN, ... ("Chat"), **le téléchargement d'un fichier que vous n'avez pas sollicité explicitement**.
- Sachez aussi qu'aucun éditeur de système d'exploitation (Microsoft, Apple, ...) n'envoie de mises à jour ou de correctifs par courrier électronique. Si vous recevez un tel message, semblant provenir de Microsoft, par exemple, c'est très certainement un faux et le fichier en annexe contient à coup sûr un virus !

La salle serveur :
- doit toujours être fermée à clé.
- doit avoir un système de climatisation à redémarrage automatique (24°C)
- doit avoir des barreaux au fenêtres si au rez de chaussé
- doit avoir un circuit ondulé

Les locaux techniques :
- doivent aussi être fermés à clé
- ne doivent pas contenir autres choses qu'une baie informatique
- doivent être climatisés si possible

Les baies informatiques :
- doivent aussi être fermées à clé
- doivent être ondulées

Formation RNT et Nouveaux RNE

vice-rectorat
de la Nouvelle-Calédonie
direction générale des enseignements

Des questions ?