

Formation SUFOP « Se protéger des dangers d'Internet »

Ateliers pratiques

Session du 12 décembre 2008

Xavier Montagutelli
Service Commun Informatique
Université de Limoges

Introduction

Les ateliers pratiques de la formation « Se protéger des dangers d'Internet » se dérouleront en environnement Microsoft Windows XP. Pourquoi pas Windows Vista, qui équipe la majorité des ordinateurs vendus actuellement ? Pourquoi pas Mac OS ou Linux ? Nous considérons que le public visé est surtout possesseur de Windows XP, que ce soit au niveau professionnel ou sur son ordinateur personnel, et nous le privilégions donc pour la formation pratique.

De même, pourquoi utilisons-nous tel navigateur Internet ou tel antivirus pendant ces ateliers ? Nous rappelons que l'objet de la formation n'est pas de donner des éléments de sécurité sur un logiciel particulier (voir les formations SUFOP spécifiques pour cela), mais plutôt de donner une vue d'ensemble, avec les éléments clés, à adapter en fonction des logiciels préférés de chacun.

Les ateliers qui suivent sont une série de travaux pratiques, indépendants les uns des autres, à mettre en œuvre sur le PC de la salle de formation.

Si le temps le permet, nous essaierons aussi, à la fin de la journée, de traiter un ou plusieurs cas concrets, à partir de questions ou situations réelles que vous soumettez.

Ateliers

Atelier 1. Adresse IP, serveur de nom	
Objectif	Vérifier (sans les modifier) quelques paramètres réseaux sous Windows XP : à travers l'interface graphique, puis avec une commande MSDOS
Exercice 1.1.	<ol style="list-style-type: none">1. Menu « Démarrer »2. Ouvrir le « Panneau de configuration »3. Ouvrir les « Connexions réseaux » avec un double-clic4. Clic droit sur « Connexion au réseau local » → « Propriétés »5. Dans la liste des éléments, ouvrir les propriétés de « Protocole Internet (TCP/IP) » avec un double-clic6. Vérifier votre adresse IP et votre serveur de nom
Exercice 1.2.	<ol style="list-style-type: none">1. Menu « Démarrer »2. « Exécuter ... »3. Ouvrir : « cmd » (ouvre une fenêtre de commande MS-DOS)4. Taper la commande « ipconfig /all » : elle affiche vos paramètres réseaux

Atelier 2. Mises à jour Windows	
Objectif	Vérifier que les mises à jour Microsoft se font automatiquement
Exercice 2.1.	<ol style="list-style-type: none"> 1. Menu « Démarrer » 2. Ouvrir le « Panneau de configuration » 3. Ouvrir « Mises à jours automatiques » avec un double-clic 4. Vérifier les paramètres

Atelier 3. Mises à jour d'une application	
Objectif	A travers l'exemple du logiciel Acrobat Reader, constatez que les mises à jour des logiciels sont parfois très simples à faire
Exercice 3.1.	<ol style="list-style-type: none"> 1. Lancer le logiciel Acrobat Reader (Menu « Démarrer » → « Tous les programmes » → « Adobe Reader ») 2. Ouvrir le menu d'aide noté « ? » 3. Aller à « Rechercher les mises à jour maintenant ... » 4. Sélectionner les composants à mettre à jour en les ajoutant dans les mises à jour sélectionnées 5. Lancer la mise à jour

Atelier 4. Découverte d'un anti-virus : Norton	
Objectif	A travers l'exemple de l'antivirus Norton, nous allons voir les points suivants : <ol style="list-style-type: none"> 1. validité des signatures 2. désactivation de la protection temps réel 3. fréquence des mises à jour 4. comportement lors du téléchargement d'un virus
Exercice 4.1.	<ol style="list-style-type: none"> 1. Faire un double clic sur le bouclier jaune dans le <i>tray</i>, en bas à droite du bureau 2. Vérifier le numéro des signatures et leur date 3. Fermer en cliquant sur « Quitter »
Exercice 4.2.	<ol style="list-style-type: none"> 1. Faire un clic-droit sur le bouclier de Norton 2. Décocher « Activer Auto-Protect » 3. Constater que l'icône change 4. Ré-activer l'analyse à l'accès !
Exercice 4.3.	<ol style="list-style-type: none"> 1. Faire un double clic sur le bouclier de Norton 2. Aller au menu « Fichier » → « Planifier les mises à jours » 3. Vérifier que la mise à jour se fait tous les jours 4. Cliquer sur le bouton « Planifier », puis « Avancés », et comprendre les différentes options 5. Fermer les fenêtres
Exercice 4.4.	<ol style="list-style-type: none"> 1. Lancer un navigateur Internet 2. Aller à l'URL http://www.eicar.org/ puis suivre le lien « download antimalware test file » (en haut à droite) 3. Téléchargez les différentes versions de eicar 4. Notez que le navigateur émet peut-être un message d'avertissement parce que vous téléchargez un exécutable 5. L'anti-virus devrait émettre un avertissement

Atelier 5. Télécharger un antivirus gratuit	
Objectif	Visiter le site web d'un éditeur d'antivirus (AVast) et télécharger sa version gratuite. Comprendre ses limitations.
Exercice 5.1.	<ol style="list-style-type: none"> 1. Aller sur le site web http://www.avast.com 2. Noter que vous êtes redirigé vers un site en français, l'adresse web change automatiquement 3. Chercher le produit antivirus gratuit (solution : « produits » → « Protection des postes » → « avast ! 4 Edition familiale ») 4. Lire (en diagonale) la page, qui vous donne les fonctionnalités du produit

	<ol style="list-style-type: none"> 5. Quelles sont ses principales fonctions ? 6. A la fin de la page, lisez la page qui suit « avast! Edition Familiale est maintenant gratuite pour les PARTICULIERS et pour une utilisation NON-COMMERCIALE. Vous pouvez trouver plus d'information ici. » 7. Quelles sont les conditions d'utilisation ? Quelle sera la durée de validité du logiciel ?
--	--

Atelier 6. Pare-feu (firewall) de Windows	
Objectif	Vérifier l'activation et le paramétrage du pare-feu de Windows. En compréhension avancée, nous voyons aussi son mécanisme des <i>exceptions</i> .
Exercice 6.1.	<ol style="list-style-type: none"> 1. Menu « Démarrer » 2. Ouvrir le « Panneau de configuration » 3. Ouvrir le « Pare-feu Windows » avec un double-clic 4. Dans l'onglet « Général », vérifier que le pare-feu est activé
Exercice 6.2.	<ol style="list-style-type: none"> 1. Aller à l'onglet « Exceptions » 2. Sélectionner « Assistance à distance » et cliquer sur « Modifier » ; faites « Annuler » dans la fenêtre de modification 3. Sélectionner « Bureau à distance » et cliquer sur « Modifier » ; faites « Annuler » dans la fenêtre de modification 4. Quelles sont les deux types d'exceptions (d'ouverture de portes) que peut faire le pare-feu Windows ?

Atelier 7. Mots de passe pour le web	
Objectif	Vérifier qu'un « super mot de passe » protège les mots de passe enregistrés par Mozilla Firefox.
Exercice 7.1.	<ol style="list-style-type: none"> 1. Lancer Mozilla Firefox 2. Aller au menu « Outils » → « Options... » 3. Aller à la partie « Sécurité » 4. Cocher la case « Utiliser un mot de passe principal ». Si la case n'était pas cochée, Firefox demande le mot de passe principal à utiliser. Pour ne pas bloquer les futurs usagers du PC, merci de ne pas mettre de mot de passe, faites « Annuler » !

Atelier 8. Utiliser un compte limité	
Objectif	Créer un compte aux droits limités sous Windows XP Pro
Exercice 8.1.	<ol style="list-style-type: none"> 1. Menu « Démarrer » 2. Ouvrir le « Panneau de configuration » 3. Ouvrir « Comptes d'utilisateurs » 4. Aller au compte par défaut « formation » 5. Vous avez un menu « Créer un mot de passe » ; par défaut, le premier compte n'a pas de mot de passe. Ne pas le modifier SVP ! 6. Valider <p>Le compte « formation » sera celui de l'administrateur (informaticien du site, parents)</p>
Exercice 8.2.	<ol style="list-style-type: none"> 7. Dans la fenêtre des comptes d'utilisateurs, faites « Créer un nouveau compte » 8. Indiquer le nom du compte : « enfant » 9. Type de compte : « limité » <p>Ce compte peut rester sans mot de passe.</p>
Exercice 8.3.	<ol style="list-style-type: none"> 10. Déconnectez-vous (menu « Démarrer », « Fermer la session ») 11. Vous pouvez constater que Windows demande maintenant le compte à utiliser 12. Connectez-vous en tant que « enfant » 13. Pouvez-vous désactiver l'antivirus ? 14. Fermer la session, et reconnectez-vous en tant que « formation » <p>Note : pour passer plus vite d'un compte à l'autre, vous pouvez utiliser le « changer d'utilisateur » (<i>Fast User Switching</i>) qui ouvre une nouvelle session sans fermer la</p>

précédente.

Atelier 9. Filtrage anti-spam	
Objectif	Comment se débarrasser des Spams : <ol style="list-style-type: none">1. Apprendre à utiliser les filtres du serveur de messagerie de l'université pour classer les messages marqués « {Spam?} » dans une boîte aux lettres dédiée2. A travers le logiciel Thunderbird, utiliser le filtrage d'un client de messagerie « intelligent »
Note	Afin de ne pas faire d'erreur de manipulation, n'utilisez pas votre compte personnel de messagerie universitaire. Nous allons utiliser des comptes dédiés à la formation. L'identifiant est de la forme « sciformN », avec N de 1 à 20. Le numéro à utiliser est le même que celui inscrit sur le boîtier de votre PC. Le mot de passe associé est « passformN » avec N de 1 à 20
Exercice 9.1.	<ol style="list-style-type: none">1. Ouvrir un navigateur Internet2. Aller sur http://webmail.unilim.fr3. Connectez-vous avec l'identifiant <i>sciformN</i> (Cf note ci-dessus)4. Dans l'arborescence à gauche, déplier la partie « Courrier » (en cliquant sur le « + »)5. Aller dans « Filtres »6. Cliquer sur « Nouvelle règle »7. Nom de la règle : « Spam »8. Choisissez un champ : « Sujet »9. Au lieu de « Contient », sélectionner « Commence par »10. Et mettre comme chaîne « {Spam?} »11. Faire ceci : « Placer dans le dossier » « Spam » <p>Avec cette règle de tri, tous les messages dont le sujet commence par {Spam?} se mettront tout seul dans la boîte aux lettres nommée « Spam » sur le serveur de l'université.</p>
Exercice 9.2.	<p>D'abord, nous vérifions que que Thunderbird va traquer les messages indésirables provenant du compte :</p> <ol style="list-style-type: none">1. Lancer le client de messagerie Thunderbird (Menu « Démarrer »...)2. Vous devriez avoir un compte préconfiguré, de type IMAP, qui va vous demander le mot de passe pour se connecter au serveur3. Noter que vous avez un bouton « Indésirable » pour dire à Thunderbird qu'un message est un spam. Thunderbird <i>apprend</i> au fur et à mesure que vous déclarez des messages4. Pour activer la traque des indésirables, aller au menu « Outil » → « Paramètres des comptes »5. Dans le compte, aller dans la partie « Paramètres pour les indésirables »6. Cocher la case « Activer le contrôle adaptatif de courriels indésirables pour ce compte »7. Cocher aussi la case « Déplacer les nouveaux courriels indésirables vers » et sélectionner la boîte « Autre » nommée « Spam » sur le serveur IMAP8. Cliquer sur « OK » <p>Ensuite, nous modifions quelques paramètres sur la gestion des indésirables :</p> <ol style="list-style-type: none">9. Aller au menu « Outil » → « Options »10. Partie « Confidentialité », puis onglet « Indésirables »11. Cocher la case « Quand je marque des messages comme indésirables » → « les déplacer dans le dossier Indésirables »12. Cocher la case « Activer la journalisation du filtre des indésirables » : vous pourrez analyser tout ce que Thunderbird a déplacé automatiquement13. Aller dans l'onglet « Courrier frauduleux » et vérifier que Thunderbird fait aussi une vérification contre le filoutage. <p>Pour tester, notez comme indésirable un message de la boîte aux lettres. Il devrait se déplacer vers la boîte « Spam »</p>


Atelier 10. Web – Se protéger des site dangereux	
Objectif	Etre averti lors de la visite d'un site dangereux, avec Mozilla Firefox version 3.
Exercice 10.1.	<ol style="list-style-type: none"> 1. Lancer Mozilla Firefox 2. Aller au menu « Outils » → « Options... » 3. Aller à la partie « Sécurité » 4. Cocher les cases « Signaler si le site que je visite est suspecté d'être un site d'attaque » et « Signaler si le site que je visite est suspecté d'être une contrefaçon »

Atelier 11. Web – Bloquer les fenêtres surgissantes	
Objectif	Les fenêtres surgissantes (<i>popup</i>) sont une gêne et parfois un danger. Les navigateurs webs permettent maintenant de les bloquer, nous allons voir cette fonction avec Mozilla Firefox version 3.
Exercice 11.1.	<ol style="list-style-type: none"> 1. Lancer Mozilla Firefox 2. Aller au menu « Outils » → « Options... » 3. Aller à la partie « Contenu » 4. Cocher la case « Bloquer les fenêtres popup » 5. Bouton « Exceptions... » : on peut autoriser certains sites à émettre des fenêtres surgissantes 6. Fermer la fenêtre d'options en cliquant sur « OK »

Atelier 12. Web – Se protéger des sites dangereux avec WoT et bloquer les Flash	
Objectif	Installer le module WoT pour se protéger des sites dangereux, sous Firefox Installer le module qui bloque les animations flash
Exercice 12.1.	<ol style="list-style-type: none"> 1. Lancer Mozilla Firefox 2. Aller au menu « Outils » → « Modules complémentaires... » 3. Aller à la partie « Catalogue », et cliquer sur « Parcourir tous les modules complémentaires » 4. Vous êtes redirigé vers le site web de Mozilla ; dans la partie gauche, cliquer sur la partie « Sécurité et vie privée » 5. Dans la partie droite, cliquer sur « Voir tous les modules recommandés » 6. Descendre jusqu'à « Flashblock » et faites « Ajouter à Firefox » 7. Accepter l'installation en cliquant sur « Installer maintenant » 8. Ne pas redémarrer Firefox. Revenir dans la liste des modules recommandés de sécurité 9. Descendre jusqu'à « WOT », puis « Ajouter à Firefox » et accepter l'installation 10. Vous pouvez maintenant redémarrer Firefox 11. Au redémarrage, accepter la licence de WOT 12. Vous pouvez paramétrer WOT en allant au menu « Outils » → « WOT » → « Paramètres » 13. Vous pouvez l'activer ou le désactiver avec la case à cocher « Outils » → « WOT » → « Activé » <p>Pour tester, aller sur un moteur de recherche (Yahoo, Google, ...) et faire une recherche. Essayer aussi le site www.sex.com</p>

Atelier 13. Web – Trace géographique	
Objectif	Constater que la traçabilité géographique, ça marche
Exercice 13.1.	<ol style="list-style-type: none"> 1. Lancer un navigateur web 2. Aller sur le site http://www.geoiptool.com/

Atelier 14.	Web – Effacer ses traces
Objectif	Effacer ses traces de navigation (cookies, cache, historique, ...).
Exercice 14.1.	<ol style="list-style-type: none"> 1. Lancer Mozilla Firefox 2. Aller au menu « Outils » → « Effacer mes traces... » <p>Noter qu' on peut effacer ses traces. Fermer la fenêtre</p> <ol style="list-style-type: none"> 3. Aller au menu « Outils » → « Options... » 4. Dans la partie « Vie privée », noter qu'il y a une case à cocher « Toujours effacer mes informations personnelles à la fermeture de Firefox ».

Atelier 15.	Web – Protection des mineurs
Objectif	<p>Bloquer les sites inappropriés avec K9.</p> <p> La configuration se fait en anglais</p>
Exercice 15.1.	<ol style="list-style-type: none"> 1. Aller sur le site http://www1.k9webprotection.com/ 2. Aller à « Download k9 for free » à droite 3. Vous devez donner vos coordonnées avec une adresse mél. Utiliser comme adresse mél « formationN@unilim.fr » afin d'éviter de futurs messages publicitaires ... 4. Dans le mél, vous recevez une URL pour télécharger K9 plus un code d'activation 5. Télécharger le logiciel, lancer l'installation 6. Pendant l'installation, rentrer le code reçu 7. Ensuite, indiquer le mot de passe pour K9 : mettre « passform » 8. Finir l'installation et rebooter <ol style="list-style-type: none"> 9. Une fois le PC rebooté, aller au menu « Démarrer » → « Blue Coat K9 Web Protection » → « Blue Coat K9 Web Protection Admin » 10. Aller dans la partie « Setup » en indiquant le mot de passe « passform » 11. Noter que K9 classe les sites par catégories, et qu'on peut régler les catégories autorisées ou interdites 12. Essayer ensuite d'aller sur www.sex.com