

*Etre capable de maîtriser l'environnement des nouvelles technologies et d'orienter ses choix parmi les très nombreuses solutions techniques proposées.*

---

**ITEM 1 : Introduction au net**

**ITEM 2 : Comprendre la technologie inter / intranet**

**ITEM 3 : Connaître les protocoles**

**ITEM 4 : Connaître les outils disponibles : langages et éditeurs**

**ITEM 5 : Connaître les points essentiels du passage à l'Intranet**

**ITEM 6 : Acquérir les notions d'administration et de maintenance**

**ITEM 7 : Commencer en ASP**

**ITEM 8 : S'initier aux serveurs linux et windows 2000**

---

Public ou prérequis **Intranet / Extranet**

*Tout utilisateur expérimenté du Web souhaitant mieux appréhender l'implantation d'un Intranet au sein d'un système existant*

Définitions, points communs, différences  
Les avantages et les inconvénients

**Les services**

La messagerie, les sites d'informations  
Les annuaires, les moteurs de recherche, les forums de discussion

Activités principales **Les protocoles**

TCP/IP, URL, DNS, imap, ldap, nntp

*Ce stage est basé sur des exemples et des cas concrets intégrant les fonctions et opérations proposées :*

*- installation et mise en service de messagerie  
- utilisations des logiciels présentés  
- initiation à l'ASP.*

**Les langages et les standards de publication**

HTML, DHTML, XML, XHTML

Les images  
Javascript, Java

**Les éditeurs**

Frontpage, Dreamweaver  
Office 2000  
L'utilisation de Flash  
L'intégration de la téléphonie, de la vidéo et du son : l'état de l'art.

**Les points essentiels de l'évolution d'un SI vers Intranet**

**L'administration et la maintenance**

**Commencer en ASP**

Introduction aux formulaires, zones de textes simples, multilignes  
Cases à cocher, cases d'options, menus déroulants

D  
E  
L  
P  
H  
E  
S

Acquérir les connaissances nécessaires à la création et à la gestion d'un site INTRANET.

ITEM 1 : Connaître le PHP et les langages serveur

ITEM 2 et 3 : Savoir administrer et gérer un intranet

ITEM 4 : Connaître le XML

ITEM 5 : Se familiariser avec les aspects réseaux

Public ou prérequis **Les bases de PHP** (sécurité des fichiers, gestion des connexions, gestion des cookies, utilisation des fichiers à distance)

*Développeur sites web.*

*Connaissance souhaitée de la programmation objet, du langage HTML .*

*La syntaxe de base du langage :*

- les constantes, les structures de contrôle, les expressions
- les fonctions, les classes et les objets
- les opérateurs, les références
- les types, les variables

**Gérer les fonctions, exemples :**

Activités principales

- Apache
- tableaux, calendrier, objets, caractères
- dates et heures
- gestion des erreurs
- FTP, HTTP, Email
- Java, MySQL

*Le stage est basé sur un cas pratique d'administration de réseau Intranet.*

**SPIP, système de publication PHP/MySQL**

Etude du langage de balises SPIP

Interfaçage templates avec PHP

Phpmysqladmin : Administration de la base MySQL

Exemples d'applications (Boucles, formulaires)

Administration et gestion de l'application intranet

Syntaxe XML de base et mise en oeuvre avec XSL.

Exemples d'applications

**Administration du serveur WEB APACHE.**

Fichier htaccess et htpasswd pour sécuriser les répertoires du serveur.

Configuration d'un firewall.

D  
E  
L  
P  
H  
E  
S

**Ce programme est personnalisable et adaptable en fonction de vos besoins.**

Tél. 04 94 16 90 70 [www.delphes-france.net](http://www.delphes-france.net) Fax. 04 94 16 90 77

Num module

4

Rechercher et analyser les informations issues d'INTERNET et gérer la sécurité

ITEM 1 : Internet : quelques notions de base

ITEM 2 : Connaître les outils de recherche

ITEM 3 : Savoir rechercher sur Internet

ITEM 4 : Savoir traiter l'information

ITEM 5 : Connaître la sécurité

Public ou prérequis

*Destiné à des utilisateurs confirmés d'internet*

Activités principales

*Au cours de ce stage, vous perfectionnerez votre connaissance du réseau Internet et des services qu'il propose grâce à des recherches plus poussées. De plus, vous apprendrez à mieux maîtriser les techniques de sécurité.*

**Les outils avancés**

Les navigateurs, les répertoires, les moteurs de recherche  
Les méta-moteurs, les agents intelligents  
Gérer son courrier électronique de façon automatisée

**Recherche simple et recherche avancée** (utilisation d'opérateurs logiques et de voisinages)

Recherche avec les répertoires et avec les méta-moteurs (metacrawler)  
Recherche avec les agents intelligents (Copernic 2000, Digout4u, Mata Hari, Bulleyes, Umap WEB)  
Aspiration de sites (MemoWeb)  
Recherche sur LEGIFRANCE

**La sécurité**

Le reformatage (utilisation de macro-commandes WORD)  
L'analyse  
L'espionnage industriel et militaire  
L'intégrité du commerce  
La mise hors service des serveurs  
Le système de fichiers en réseau  
Le "CRACKAGE" de mot de passe  
Le "SNIFFING" des mots de passe et des paquets  
Les chevaux de Troie, les vers  
Le TCP-SYN FLOODING  
Les Firewalls : Qu'est-ce qu'un Firewall ? Qu'est-ce qu'un Firewall ne peut pas faire ?  
La protection des mots de passe et la création de mots de passe sûrs  
Les mots de passe "SHADOW"  
Le cryptage asymétrique ou à clé publique, le cryptage symétrique  
Les outils de vérification de la sécurité  
La restriction d'IP, l'éducation de la prise de conscience

D  
E  
L  
P  
H  
E  
S

Découvrir les potentialités et les modalités d'utilisation du réseau INTERNET. Connaître les différentes fonctionnalités d'INTERNET et savoir les utiliser.

ITEM 1 : Connaître le réseau Internet

ITEM 2 : Savoir envoyer et réceptionner le courrier électronique

ITEM 4 : Savoir utiliser le World Wide Web

ITEM 5 : Savoir télécharger

ITEM 6 : Connaître les différences entre intranet et internet

ITEM 7 : Gérer la sécurité

### Public ou prérequis

Historique et perspective

### *Etre utilisateur d'un poste informatique*

Moyens de connexion au réseau, les fournisseurs de connexions

#### **Savoir envoyer et réceptionner le courrier électronique**

Principes de fonctionnement

Identification des serveurs sur le réseau

### Activités principales

Les logiciels de gestion du courrier, Envoi et réception du courrier, Risques des envois électroniques

*Au cours de ce stage, les participants apprendront à chercher sur le Web, créer une boîte aux lettres électronique, télécharger des fichiers ou des programmes. Familiarisés avec la "toile", ils sauront à l'issue de ce stage l'utiliser de la manière la mieux adaptée à leurs besoins et usages professionnels.*

#### **Savoir utiliser le World Wide Web**

Principes de fonctionnement

Classification

Participation à un forum

Ecrire et recevoir des articles

#### **Savoir télécharger**

Organisation

Principe de l'hypertexte

Navigation entre les serveurs

Méthodes de recherche des informations

Importation du texte et des images

#### **Savoir gérer Internet dans l'organisation (entreprise ou service public)**

Connaître les domaines d'emploi d'Internet et d'Intranet

Téléchargement de documents

#### **Savoir travailler à distance**

Moyens de connexion au réseau

Identification des serveurs sur le réseau

Les logiciels de gestion du courrier

Envoi et réception du courrier

D

E

L

P

H

E

S

**Ce programme est personnalisable et adaptable en fonction de vos besoins.**

Tél. 04 94 16 90 70 [www.delphes-france.net](http://www.delphes-france.net) Fax. 04 94 16 90 77

*Maîtriser l'environnement des nouvelles technologies et d'orienter ses choix parmi les très nombreuses solutions techniques proposées.*

**ITEM 1 : Intranet et client serveur**

**ITEM 2 : Les services**

**ITEM 3 : Les protocoles**

**ITEM 4 : Les langages et les standards de publication**

**ITEM 5 : Les points essentiels de l'évolution vers Intranet**

**ITEM 6 : Les bases de PHP**

**ITEM 7 : Administration du serveur WEB APACHE.**

**ITEM 7 : La sécurité**

Public ou prérequis

**Intranet et client serveur**

Définitions, points communs, différences  
Les avantages et les inconvénients

**Les services**

La messagerie, les sites d'informations  
Les annuaires, les moteurs de recherche, les forums de discussion

**Les protocoles**

TCP/IP, URL, DNS, imap, ldap, nntp

**Les langages et les standards de publication**

**Les éditeurs**

**Les points essentiels de l'évolution d'un SI vers Intranet**

**Les bases de PHP** (sécurité des fichiers, gestion des connexions, gestion des cookies, utilisation des fichiers à distance)

*La syntaxe de base du langage :*

**Gérer les fonctions, exemples :**

- Apache
- tableaux, calendrier, objets, caractères
- dates et heures
- gestion des erreurs
- FTP, HTTP, Email
- Java, MySQL

**SPIP, système de publication PHP/MySQL**

Etude du langage de balises SPIP

Interfaçage templates avec PHP

Phpmyadmin : Administration de la base MySQL

Exemples d'applications (Boucles, formulaires)

Administration et gestion de l'application intranet

Syntaxe XML de base et mise en oeuvre avec XSL.

Exemples d'applications

**Administration du serveur WEB APACHE.**

Fichier htaccess et htpasswd pour sécuriser les répertoires du serveur.

Configuration d'un firewall.

**La sécurité**

**Les attaques sur les réseaux**

**La sécurité des systèmes d'exploitation**

**La politique de sécurité : conception et mise en oeuvre**

**La protection périmétrique par Firewall**

**La protection des données**

*Tout technicien  
expérimenté souhaitant  
mieux appréhender  
l'implantation d'un  
Intranet au sein d'un  
système existant*

Activités principales

*Ce stage est basé sur  
des exemples et des cas  
concrets intégrant les  
fonctions et opérations  
proposées :  
- installation et mise en  
service de messagerie  
- utilisations des  
logiciels présentés*

D  
E  
L  
P  
H  
E  
S

Etre à même de protéger et sécuriser vos informations sur des réseaux TCP-IP et les postes accédant à internet en paramétrant les systèmes d'exploitation, en sachant choisir et paramétrer un firewall et implémenter un VPN.

- ITEM 1 : Identifier les types d'attaques sur les réseaux
- ITEM 2 : Savoir sécuriser les systèmes d'exploitation
- ITEM 3 : Définir la politique de sécurité : conception et mise en oeuvre
- ITEM 4 : Savoir isoler et protéger les réseaux TCP/IP
- ITEM 5 : Implémenter une protection périmétrique par Firewall (TP)
- ITEM 6 : Savoir protéger les données de votre organisation
- ITEM 7 : Déployer un VPN (TP)
- ITEM 8 : Paramétrer l'authentification des utilisateurs
- ITEM 9 : Savoir évaluer et faire l'audit de la sécurité

Public ou prérequis Les virus : typologie des attaques par le réseau.

*Avoir des connaissances de base sur TCP/IP et maîtriser un système d'exploitation.*

Activités principales

*A l'issue de ce stage, vous serez à même de mettre en oeuvre le système de sécurité le mieux adapté à votre réseau.*

Les firewalls dédiés / non dédiés ; où implémenter le ou les firewalls ?  
 Comment se protéger des serveurs, des clients, de l'Internet.  
 La mise en place de solutions DMZ (zones démilitarisées).  
 Comment calculer le nombre de DMZ nécessaires.  
 Les principales solutions du marché et leurs caractéristiques  
 Comment sélectionner le firewall le mieux adapté à vos contraintes.  
 Les firewalls : quelle exploitation au quotidien ?  
 Quelle ressource nécessaire pour administrer et exploiter les firewalls ?  
 Comment détecter les symptômes d'une intrusion.  
 Les outils d'analyse de logs et de remontée d'alertes indispensables.  
 Fuite ou vol d'information, violation d'intégrité, authentification des messages.  
 Les algorithmes à clé symétrique / asymétrique.  
 Comment crypter vos données.  
 Choisir les outils appropriés, les logiciels d'analyse de sécurité.  
 Les logiciels de scan avancés.  
 Les détections temps réel.  
 La sécurisation des communications Web.  
 Comment offrir un service sécurisé aux clients privilégiés.  
 Dans quels cas le firewall est indispensable devant ses serveurs ?  
 Les solutions DMZ sécurisées ; combien de DMZ ?  
 Comment réaliser les mises à jour à distance et sécurisées.  
 L'authentification renforcée, les vérifications d'intégrité.  
 La création de VPN (Virtual Private Network) avec la solution firewall-réseau public-firewall.  
 Comment déployer des accès distants à travers l'Internet.  
 Préserver la confidentialité des mots de passe.  
 Authentifier les accès entrants et sortants.  
 La sécurité des réseaux sans fil ?  
 Architecturer ses réseaux sans fil  
 Comment réaliser l'audit de la sécurité de votre réseau.

D  
E  
L  
P  
H  
E  
S

Comment protéger et sécuriser vos informations sur des réseaux TCP-IP : illustré de nombreux exemples pratiques et d'études de cas concrets, ce séminaire dresse l'état de l'art en la matière et répond à toutes les préoccupations actuelles dans le domaine de la sécurité TCP-IP.

- ITEM 1 : Identifier les types d'attaques sur les réseaux
- ITEM 2 : Savoir sécuriser les systèmes d'exploitation
- ITEM 3 : Définir la politique de sécurité : conception et mise en oeuvre
- ITEM 4 : Savoir isoler et protéger les réseaux TCP/IP
- ITEM 5 : Connaître la protection périmétrique par Firewall
- ITEM 6 : Savoir protéger les données de l'entreprise
- ITEM 7 : Déployer un VPN
- ITEM 8 : Paramétrer l'authentification des utilisateurs
- ITEM 9 : Savoir évaluer et faire l'audit de la sécurité
- ITEM 10 : Savoir sécuriser les services en ligne

#### Public ou prérequis Les attaques sur les réseaux

*Avoir des connaissances de base sur TCP/IP et maîtriser un système d'exploitation.*

Les origines des attaques et leur propagation  
Evaluation du risque et applications à risque (DNS, HTTP, SMTP,...)

#### **La sécurité des systèmes d'exploitation**

La sécurité des différents systèmes : ITSEC, TCSEC, Unix,...  
Les niveaux de sécurité D1, C1, C2, B1, B2, B3, A de l'Orange Book  
L'exception Windows NT, les avis du CERT  
Les authentifications Kerberos et LanMan

#### Activités principales

#### **La politique de sécurité : conception et mise en oeuvre**

Les objectifs d'une politique de sécurité globale, le rôle des hommes dans la sécurité  
Externalisation de la sécurité ; concilier bon sens, technique et coût  
Isolation et protection des réseaux TCP/IP  
Les virus : typologie des attaques par le réseau, es serveurs anti-virus  
Le plan d'adressage sécurisé, les serveurs proxy, le reverse proxy,...  
Firewall ou proxy : concurrence ou complémentarité ?

#### **La protection périmétrique par Firewall**

Usages et pratiques du Firewall : le firewall le mieux adapté aux contraintes  
Ressources nécessaires à l'administration et l'exploitation des firewalls  
La détection des intrusions, les outils de remontée d'alertes et d'analyse de logs  
Les solutions à haute disponibilité (Raware, legato, Stonesoft)  
Le filtrage multi-zones et les données

#### **La protection des données de l'entreprise**

Fuite et vol d'information, violation d'intégrité, authentification des messages  
Cryptage et clés de chiffrement

D  
E  
L  
P  
H  
E  
S