Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR

CONCOURS INTERNE DE TECHNICIEN DE CLASSE NORMALE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

- SESSION 2019 -

Mercredi 20 mars 2019

Option « Solutions logicielles et systèmes d'information »

Traitement de questions et résolution de cas pratiques, à partir d'un dossier, portant sur l'une des deux options choisies par le candidat le jour de l'épreuve :
- infrastructures et réseaux
- solutions logicielles et systèmes d'information.

Cette épreuve permet d'évaluer le niveau de connaissances du candidat, sa capacité à les ordonner pour proposer des solutions techniques pertinentes et à les argumenter.

Le dossier ne peut excéder 20 pages.

(Durée : 3 heures – Coefficient 2)

L'usage de la calculatrice est strictement interdit

Le dossier documentaire comporte 19 pages.

NOUVEAUTES 2019

1. LES COPIES SERONT RENDUES EN L'ETAT AU SERVICE ORGANISATEUR. A L'ISSUE DE L'EPREUVE, CELUI-CI PROCEDERA A L'ANONYMISATION DE LA COPIE.
2. NE PAS UTILISER DE CORRECTEUR D'ORTHOGRAPHE SUR LES COPIES.
3. ECRIRE EN NOIR OU EN BLEU – PAS D'AUTRE COULEUR.
4. IL EST RAPPELE AUX CANDIDATS QU'AUCUN SIGNE DISTINCTIF NE DOIT APPARAITRE SUR LA COPIE.

SUJET

LES QUESTIONS

Les réponses doivent être rédigées. L'ensemble des questions sera noté sur 10 points.

QUESTION 1:

Quelle est la définition d'un problème selon ITIL et quel est l'objectif du processus de gestion des problèmes (ITIL) ?

QUESTION 2 :

En informatique, quel est l'autre nom de « station de décontamination » et à quoi sert-elle ?

QUESTION 3 :

Comment se nomme l'outil qu'une JVM utilise pour nettoyer la mémoire ?

QUESTION 4 :

Quelle commande système permet de lister les processus dans un environnement Linux ?

QUESTION 5 :

Que signifie l'acronyme SAAS ?

QUESTION 6 :

Citer les différents modèles de clés d'activation des produits Microsoft ?

QUESTION 7 :

Que signifie l'acronyme LAMP et à quoi sert cette suite d'outils ?

QUESTION 8 :

Comment peut aussi être appelé le RAID – 0 ?

QUESTION 9 :

Quelle commande permet de changer le propriétaire d'un fichier UNIX ?

QUESTION 10 :

Combien vaut le nombre binaire 1011 en décimal ?

ETUDE DE CAS

L'étude de cas se subdivise en deux parties distinctes. L'ensemble de ces parties sera noté sur 10 points.

Etude de Cas n°1 (5 points) **:**

Vous êtes Technicien(ne) SIC dans une préfecture. Lors de votre prise de service, vous êtes alerté(e) des 3 problèmes suivants :

-La directrice des ressources humaines ne peut plus imprimer.
-Le poste de travail de la secrétaire de la directrice des ressources humaines présente des signes d'infection virale.
-Le rapport de sauvegarde hebdomadaire du SAN (Storage Area Network) remonte un défaut sur la sauvegarde exécutée la nuit précédente.

Question 1 :
Comment priorisez-vous le traitement de ces incidents ? Justifier vos choix.

Question 2 :
Concernant le poste de la secrétaire, lors de la prise en main à distance, vous vous rendez compte qu'il est infecté par un rançongiciel (ou cryptolocker). Énumérer les actions à entreprendre afin d'enrayer l'incident et permettre à la secrétaire de reprendre son activité.

Etude de Cas n°2 (5 points) **:**

Vous êtes affecté(e) dans une équipe de techniciens de support de proximité au sein de la Direction des Systèmes d'Information et de Communication (DSIC) du Ministère de l'Intérieur. Vous avez la charge, au sein de votre site de rattachement, d'assurer en plus de vos missions d'intervention de soutien informatique, celle d'Assistant Local de Sécurité des Systèmes d'Information (ALSSI).

À ce titre, votre Responsable en Sécurité des Systèmes d'Information (RSSI) vous demande de rédiger un mail d'information décrivant les conduites à tenir en cas de réception de courriels suspects ou frauduleux dans la messagerie professionnelle pour les agents dépendant de votre site.

Rédiger sur votre copie le mail mis en forme à destination de vos collègues. (*Ne pas signer de votre nom le mail afin de respecter l'anonymat de votre copie.*)

Dossier documentaire :

Document 1

Lutter contre le phishing

Suite à la recrudescence des tentatives de piratage sur Internet voici des informations à connaitre sur le phishing.

Qu'est-ce que le phishing ?

Le Phishing est une technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations sensibles, personnelles et/ou confidentielles (coordonnées bancaires, vol d'identité…) vous appartenant. Pour cela, ils reproduisent parfaitement le design d'un e-mail, ou d'un site commercial légitime, d'un fournisseur d'accès à Internet, d'une banque, etc. L'adresse URL du lien compris dans le mail est généralement « masquée » afin de paraître authentique.

Bon à savoir : la forme la plus répandue reste l'envoi d'e-mail dont le contenu invite une victime à cliquer sur un lien afin d'y communiquer ses informations confidentielles. Les faux e-mails sont envoyés en masse et ont pour unique intérêt de piéger les coordonnées bancaires et de connexions d'un maximum de personnes.

Email

Repérer un e-mail Frauduleux ''Phishing'' !

Méfiez-vous des formulaires dans un e-mail ou sur site internet **demandant des informations bancaires.**

En cas de doute, contactez le Service Client de la société pour déterminer s'il est bien l'expéditeur officiel du message.

Adoptez les bons réflexes :

- Ne cliquez sur aucun lien contenu dans un e-mail.
- N'ouvrez pas les pièces jointes.
- Ne répondez pas aux e-mails douteux.
- Classez-le dans vos courriers indésirables.

Que faire si vous recevez un e-mail frauduleux ?

Signalez-le :

- Aux autorités compétentes : vous pouvez signaler un e-mail frauduleux aux autorités compétentes sur la plate-forme Internet **internet-signalement.gouv.fr.** Votre signalement sera traité dans les meilleurs délais par les policiers et gendarmes de la 'Pharos', la '*Plateforme d'harmonisation d'analyse de regroupement et d'orientation des signalements'.*
- A votre organisme : pour dénoncer un e-mail frauduleux auprès de SFR Caraibe, vous pouvez transférer le mail suspect à **serviceclient@sfrcaraibe.fr**

Que faire si vous avez répondu à un e-mail frauduleux ‘’Phishing’’

Vous avez répondu à un e-mail contenant un lien vers un formulaire en ligne vous demandant de renseigner vos données personnelles (adresse e-mail, mot de passe SFR, coordonnées bancaires…etc.), émanant d’une société dont vous êtes client : SFR, organisme bancaire, Trésor Public, EDF, etc… :

1. **Si vous avez communiqué vos coordonnées bancaires :**

Le pirate informatique connait désormais votre numéro de compte et/ou vos numéros de carte de crédit. Dans ce cas, il y a urgence ! Contactez immédiatement votre banque afin de mettre votre carte en opposition. Votre banque sera alors informée du risque d’éventuelles fraudes liées à votre compte bancaire.

Bon à savoir : il est possible de se faire rembourser intégralement les sommes dérobées et ce par votre banque, grâce à un article dans la loi (article L 133-18 du Code monétaire et financier)

2. **Si vous avez donné vos identifiants de connexion :**

L’usurpateur peut faire des commandes et d’autres actions depuis votre espace client, il est donc nécessaire de changer tout de suite votre mot de passe. Lors de la création de vos nouveaux mots de passe, suivez ces conseils afin d’optimiser la sûreté de celui-ci :

- Utilisez des lettres, des chiffres et des symboles ;
- N’utilisez pas de mots simples ;
- Un minimum d’au moins 8 caractères est nécessaire ;
- Choisissez un mot de passe que vous retiendrez facilement ;
- Modifiez votre mot de passe régulièrement ;
- Ne remettez jamais un mot de passe usurpé même plusieurs mois plus tard.

3. **Si vous avez renseigné vos coordonnées postales :**

Les attaques de Phishing ont pour but de dérober principalement vos coordonnées bancaires et vos identifiants. Rares sont les pirates informatiques qui iraient cambrioler ses victimes. Les pirates ne vous connaissent pas personnellement et n’habitent généralement pas dans votre quartier, ville, département voir même parfois pays !

12 gestes simples pour contrer les e-mails frauduleux :

Réseaux sociaux

Repérer un message Frauduleux provenant d'un réseau social ''Phishing'' !

[…] Toutes demandes d'informations personnelles (adresse e-mail, mot de passe SFR, RIB…etc.), doit faire l'objet d'une attention particulière de votre part.

4 règles simples à connaître :

Règle N°1	Règle N°2
Un conseiller SFR Caraibe ne vous demandera **jamais** d'informations personnelles, **sans que vous ayez vous-même engagé la conversation sur Facebook ou sur Messenger.**	Un conseiller SFR Caraibe **n'a pas besoin que vous l'ajoutiez en ami pour discuter avec vous sur Messenger.**
Règle N°3	**Règle N°4**
Un conseiller SFR Caraibe ne vous demandera **jamais des informations sensibles en message public** il vous demandera de passer sur Messenger sur la Page SFR Caraibe (voir exemple ci-dessous)	Jamais un conseiller SFR Caraibe n'utilisera sur Messenger son Patronyme « nom ou prénom » ou Pseudonyme Facebook pour engager une conversation avec vous. Il sera toujours connecté avec le compte SFR Caraibe et signera de son prénom.

RAPPEL

N'envoyez jamais de documents confidentiels comme par exemple vos coordonnées bancaires, numéro de carte/cryptogramme de votre carte bleue par Messenger, ou par toute conversation sur les réseaux sociaux.

Que faire si vous recevez un message frauduleux par Messenger?

Signalez-le :

- Aux autorités compétentes : vous pouvez signaler un comportement frauduleux aux autorités compétentes sur la plate-forme Internet depuis l'adresse internet-signalement.gouv.fr. Votre signalement sera traité dans les meilleurs délais par les policiers et gendarmes de la 'Pharos', la '*Plateforme d'harmonisation d'analyse de regroupement et d'orientation des signalements'.*
- A votre organisme : pour dénoncer un message frauduleux auprès de SFR Caraibe, transférer celui-ci par Messenger en cliquant sur Envoyer depuis la page SFR Caraibe. Réalisé une ne copier écran de ce message et conservez-le.

Que faire si vous avez répondu à un message sur Messenger frauduleux ''Phishing''

Vous avez répondu à un message Messenger en envoyant vos données personnelles (adresse e-mail, mot de passe SFR, coordonnées bancaires…etc.), émanant d'un par les pirates informatiques prenant une identité de conseillers Messenger.

Si vous avez communiqué vos coordonnées bancaires :

Le pirate informatique connait désormais votre numéro de compte et/ou vos numéros de carte de crédit. Dans ce cas, il y a urgence.

Contactez immédiatement votre banque afin de mettre votre carte en opposition. Votre banque sera alors informée du risque d'éventuelles fraudes liées à votre compte bancaire.

Bon à savoir : il est possible de se faire rembourser intégralement les sommes dérobées et ce par votre banque, grâce à un article dans la loi (article L 133-18 du Code monétaire et financier).

Si vous avez donné vos identifiants de connexion :

L'usurpateur peut faire des commandes et d'autres actions depuis votre espace client, il est donc nécessaire de changer tout de suite votre mot de passe. Lors de la création de vos nouveaux mots de passe, suivez ces conseils afin d'optimiser la sûreté de celui-ci :

- Utilisez des lettres, des chiffres et des symboles ;
- N'utilisez pas de mots simples ;
- Un minimum d'au moins 8 caractères est nécessaire ;
- Choisissez un mot de passe que vous retiendrez facilement ;
- Modifiez votre mot de passe régulièrement ;
- Ne remettez jamais un mot de passe usurpé même plusieurs mois plus tard.

3. **Si vous avez renseigné vos coordonnées postales :**

Les attaques de Phishing ont pour but de dérober principalement vos coordonnées bancaires et vos identifiants. Rares sont les pirates informatiques qui iraient cambrioler ses victimes. Les pirates ne vous connaissent pas personnellement et n'habitent généralement pas dans votre quartier, ville, département voir même parfois pays !

En savoir plus pour être prudent sur INTERNET

SMS

Soyez vigilants ! les SMS aussi peuvent être frauduleux…

Des SMS frauduleux circulent actuellement chez plusieurs opérateurs téléphonique. Ces SMS vous invitent à vous rendre sur des sites web ou adresses pour vous demander vos informations personnelles (adresse e-mail, mot de passe SFR, RIB…etc.).
N'envoyez jamais de données, ou documents confidentiels comme par exemple vos coordonnées bancaires, numéro de carte/cryptogramme de votre carte bleue par SMS
Jamais SFR Caraibe ne vous demandera par SMS des informations confidentielles et/ou sensibles.

Que faire si vous avez répondu à un SMS frauduleux ?

Signalez-le :

- Aux autorités compétentes : vous pouvez signaler un comportement frauduleux aux autorités compétentes sur la plate-forme Internet depuis l'adresse internet-signalement.gouv.fr. Votre signalement sera traité dans les meilleurs délais par les policiers et gendarmes de la 'Pharos', la '*Plateforme d'harmonisation d'analyse de regroupement et d'orientation des signalements'.*
- A votre organisme : pour dénoncer un sms frauduleux auprès de SFR Caraibe, transférer la copie écran du SMS par Facebook Messenger. (Réalisez une copie-écran de ce message et conservez-le.)

Si vous avez communiqué vos coordonnées bancaires :

Contactez immédiatement votre banque afin de mettre votre carte en opposition. Votre banque sera alors informée du risque d'éventuelles fraudes liées à votre compte bancaire.

Bon à savoir : il est possible de se faire rembourser intégralement les sommes dérobées et ce par votre banque, grâce à un article dans la loi (article L 133-18 du Code monétaire et financier).

Si vous avez donné vos identifiants de connexion :

L'usurpateur peut faire des commandes et d'autres actions depuis votre espace client, il est donc nécessaire de changer tout de suite votre mot de passe. Lors de la création de vos nouveaux mots de passe, suivez ces conseils afin d'optimiser la sûreté de celui-ci :

- Utilisez des lettres, des chiffres et des symboles ;
- N’utilisez pas de mots simples ;
- Un minimum d’au moins 8 caractères est nécessaire ;
- Choisissez un mot de passe que vous retiendrez facilement ;
- Modifiez votre mot de passe régulièrement ;
- Ne remettez jamais un mot de passe usurpé même plusieurs mois plus tard.

Si vous avez renseigné vos coordonnées postales :

Les attaques de Phishing ont pour but de dérober principalement vos coordonnées bancaires et vos identifiants. Rares sont les pirates informatiques qui iraient cambrioler ses victimes. Les pirates ne vous connaissent pas personnellement et n’habitent généralement pas dans votre quartier, ville, département voir même parfois pays !

Sécurité

SFR vous aide à reconnaître facilement la vraie page d’authentification de votre Espace Client SFR

N.B. : cet affichage apparaîtra uniquement si vous utilisez un système d’exploitation et une version de navigateur Internet compatibles et à jour.

Dans le cas où votre système d’exploitation et votre navigateur Internet ne sont pas compatibles et à jour, il est recommandé de :

- Vérifier que l’adresse du site SFR sur lequel où vous êtes en train de vous identifier commence par https://www.sfrcaraibe.fr ;
- Toujours vérifier la présence du cadenas indiquant un accès sécurisé.

Connaitre les symboles de sécurité

Ces symboles vous informent sur le degré de sécurité d’un site. Ils vous permettent de savoir si un site possède un certificat de sécurité ou non. Par exemple sous Chrome en savoir +.

Comment classer les actions prioritaires ?

De nombreuses méthodes existent pour vous aider, parmi lesquelles :

Le classement A-B-C-D

Comment faire ? Eclatez votre liste de tâches suivant la classification suivante :

- **A / Les tâches incontournables à mener .** Pour certaines, la question ne se pose pas, tellement les enjeux sont importants. Elles doivent être traitées immédiatement.
- **B / Celles qui sont importantes, mais un cran en-dessous des premières .** Les enjeux sont plus modérés en terme de délai et/ou d'impact.
- **C / Classez ici celles qui sont intéressantes à faire ,** mais qui n'ont pas d'impact. C'est du plus.
- **D / Celles à éliminer : ce sont celles qui n'apportent aucune valeur ajoutée.** C'est le cas de quelques tâches administratives.

Passez en revue chaque catégorie, et à l'intérieur de chacune, refaites un classement : A1 - A2 - A2 - B1... de la plus importante, prioritaire, à la moins urgente. Vous obtenez ainsi votre liste priorisée.

Une petite astuce : si vous hésitez pour une tâche, comparez-là avec d'autres déjà classées : "Laquelle des 2 est la plus importante ?". Vous saurez ainsi où la positionner.

La matrice importance / urgence

Cette matrice repose également sur 4 cases combinant 2 axes : **importance et urgence** . Elle permet de ventiler chaque item suivant ces 2 critères pour aboutir à une lecture synthétique des priorités. Bien évidement, **les tâches de la case "important/urgent" requièrent une action au plus vite .**

Vous pouvez aussi prendre en considération d'autres critères, comme **le temps requis pour executer la tâche**, ou tenir compte de la **facilité de traitement** .

Passez en revue vos actions de la journée et classez-les en utilisant l'une de ces méthodes .

N'oubliez pas enfin de **déléguer ce qui peut l'être** . Vouloir tout faire n'a pas de sens si vous n'avez pas le temps de tout traiter dans les délais impartis.

C’est quoi un serveur SMTP ?

By Master isolated images

En voyant l’image associée à l’article, je vous donne un petit indice pour répondre à la question … Qu’est-ce qu’un serveur SMTP ?

Si vous ne connaissez pas le principe de fonctionnement des mails, je vous conseille de lire : Comment ça marche les mails ?

Définition d’un serveur SMTP

Un serveur SMTP est un serveur qui va permettre l’envoi des mails.

- Mais comment c’est fait ?
- A quoi ça sert ?
- Lequel utiliser ?
- Est-ce que j’ai besoin de connaître ça ?

Eh bien, ça en fait des questions auxquelles je vais essayer de répondre simplement.

Voici ce que vous trouverez sur cet article

- La signification de SMTP
- Le fonctionnement du SMTP
- Les différents modes de connexion possibles au SMTP
- Les principaux serveurs SMTP, POP et IMAP des fournisseurs d’accès.

Signification de SMTP

C’est un procotole (langage) pour envoyer des mails.

SMTP = Simple Mail Transfer Protocol = Protocole Simple pour le Transfert des Mails.

Vous le savez peut-être mais, le mail est :

- un des services qui a contribué au succès d’Internet,
- et un des services plus utilisés sur Internet (saviez-vous qu’au début d’Internet presque 80% des échanges étaient des échanges de mails ?).

On parle toujours de serveur SMTP, mais dans les entreprises, il est rare que le serveur qui supporte le service SMTP ne fasse que ça.

Le fonctionnement du SMTP

Même si pour envoyer un mail, vous n'avez pas besoin de savoir comment fonctionne le SMTP : pour votre culture, voici comment cela se passe.

Pour envoyer un mail, vous utilisez un M.U.A. (Mail User Agent), il est en général de 2 types :

- un webmail (lorsque vous vous connectez en ligne)
- un client de messagerie (logiciel installé sur votre ordinateur tel que Outlook, ThunderBird, application de Smartphone, …)

Au moment ou vous envoyez votre mail, votre MUA :

- va convertir votre mail au format texte (même les pièces jointes seront converties en texte)
- va se connecter au serveur SMTP qui est paramétré et envoyer le texte.

Ensuite, le serveur SMTP va envoyer le mail vers le destinataire. Si le message doit passer entre différents serveurs, c'est toujours le protocole SMTP qui sera utilisé pour envoyer le message de serveurs en serveurs, les serveurs utilisent alors des relais SMTP.

Le mail va ainsi voyager de serveurs en serveurs, jusqu'au dépôt sur le serveur de boites postales du destinataire.

Un petit comparatif avec ce qui se passe lorsque vous envoyez un courrier papier devrait faciliter la compréhension de tout ça.

(en gris, toutes opérations effectuées par le serveur SMTP ou le relai SMTP).

Courrier postal	Mail
Je rédige mon courrier (sur une feuille de papier)	Je rédige mon mail (avec l'aide d'un logiciel ou d'un webmail)
Je mets le courrier dans une enveloppe et j'inscris l'adresse du destinataire.	Je saisis l'adresse mail du destinataire.
Je mets mon adresse au dos de l'enveloppe * *(voir plus bas)*	Je n'ai rien à faire, cela est déjà fait par le logiciel.
Je mets le courrier dans la boite aux lettres de la poste.	Je clique sur envoyer
Lors de la relève de la boite postale, la poste récupère tous les courriers	Mon logiciel s'est connecté au serveur SMTP et le serveur SMTP récupère le mail.
Le courrier est trié et en envoyé vers le bureau de poste du destinataire	Le serveur SMTP va envoyer le mail.
Le courrier va passer de centre de tri en centre de tri.	Le mail va passer de serveurs SMTP en serveurs SMTP (on appelle cela des relais SMTP).
Le courrier arrive au bureau de poste du destinataire et le facteur va le déposer dans la boite aux lettres du destinataire.	Il arrive sur le serveur de l'hébergeur de la boite aux lettres du destinataire.
Le destinataire va avec sa clé ouvrir sa boite aux lettres et ouvrir son courrier.	Avec son logiciel de mail ou son webmail, le destinataire va ouvrir sa boite aux lettres (avec son mot de passe) et lire son mail.

** Le fait de mettre mon adresse au dos va permettre de me renvoyer le courrier en cas d'erreur d'adresse de destination.*

Il n'y a pas de contrôle effectué sur l'expéditeur : vous pouvez bien mettre une autre adresse que la votre au dos de la lettre, et faire croire ici que c'est quelqu'un d'autre qui envoie le courrier : c'était comme ça au début du mail, on pouvait mettre l'adresse de quelqu'un d'autre. Cela est toujours possible sur certains serveurs, et c'est pour cela que sur les autres, il faut s'identifier avant d'envoyer le mail.

Modes de connexion au serveur SMTP.

Pour se connecter au serveur, le logiciel utilise des commandes très simple en mode texte.

Il existe différents modes de connexions au serveurs SMTP.

Le 1er mode de connexion utilisait le port 25 et se faisait sans authentification (sans fournir de login et de mot de passe). Cela était très pratique car il était simple d'envoyer des mails. Tout le monde pouvait se connecter à n'importe quel serveur sans aucune autorisation et il était possible d'envoyer des messages avec n'importe quelle adresse (on pouvait donc usurper l'adresse mail de quelqu'un).

Il a fallut remédier à ça, mais il reste encore des serveurs SMTP sans authentification (on parle de « relais ouverts ») : ils font le bonheur des spammeurs. Certains fournisseurs d'accès refusent les messages provenant de ces relais ouverts.

Pour tous les autres serveurs SMTP, plus sérieux, il faut désormais un compte (login) ou adresse mail, ainsi qu'un mot de passe pour se connecter au serveur SMTP. (on se connecte sur les ports 25, 587 avec authentification ou 465 sécurisé, avec envoi de mot de passe en clair ou crypté).

Si vous êtes connecté chez votre fournisseur d'accès, il n'est pas forcément nécessaire de se connecter au serveur SMTP avec un identifiant et mot de passe, car il vous connait: vous êtes déjà connecté sur son réseau, et quelque fois, il n'autorise la sortie que vers on propre serveur SMTP ! (la partie qui suit en gris et italique, est un peu plus technique, vous n'êtes pas obligé de la lire)

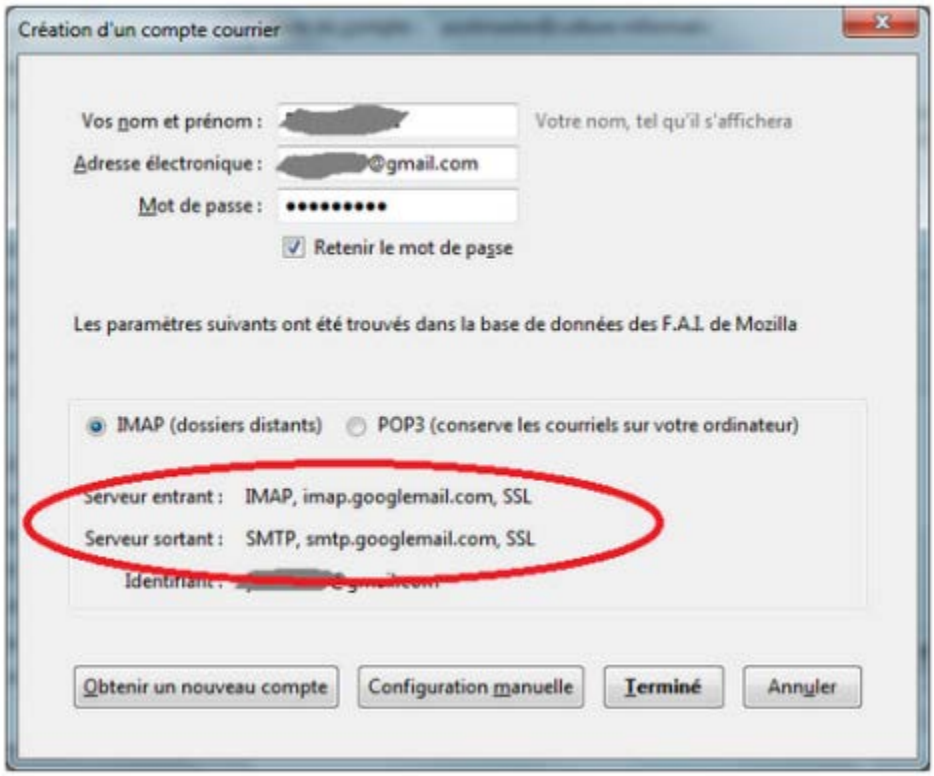
Dans ce cas, il se peut que vous soyez obligé d'utiliser le serveur SMTP de votre fournisseur d'accès plutôt que celui de votre boite aux lettres : Voici un petit exemple pour faciliter la compréhension de ce que je dis :

J'utilise une connexion chez le FAI Free, et je veux envoyer un mail avec mon adresse mail « xxx@orange.fr », et bien dans les paramètres de mon logiciel de messagerie, je vais mettre le serveur sortant : smtp.free.fr et non pas cela d'Orange !

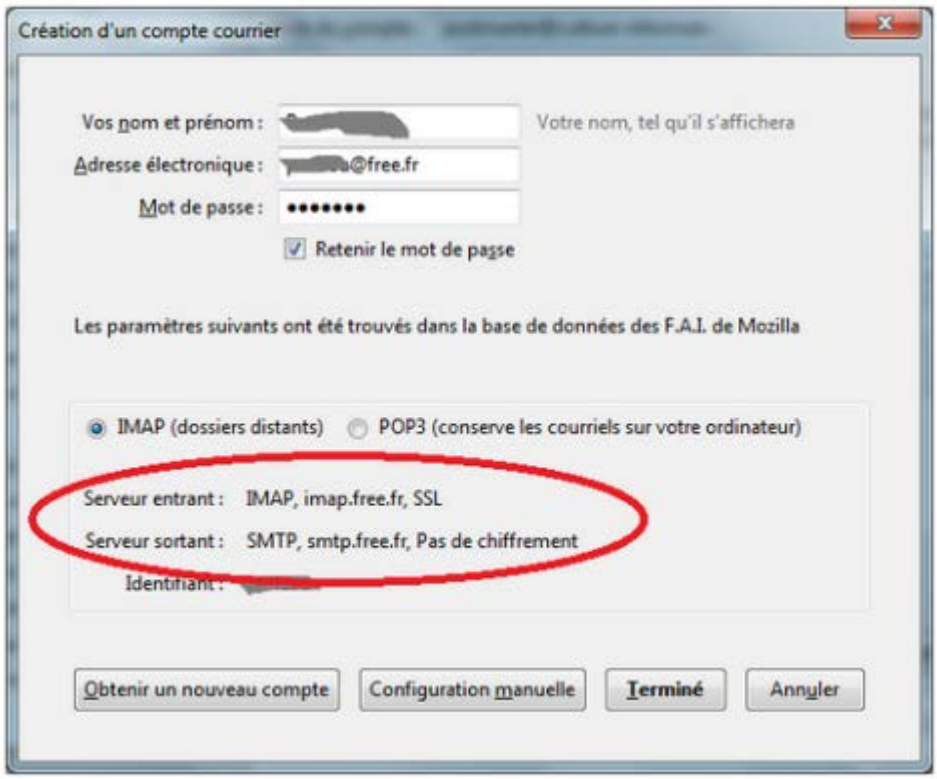
La plupart des logiciels de messagerie (clients lourds tels que Outlook, ThunderBird, Incrédimail, Eudora, …) savent retrouver les serveurs en fonction de votre adresse mail. Dans quelques cas rares ou configurations particulières, vous pouvez avoir besoin de saisir les informations manuellement. (vous trouverez ces informations plus bas).

Voici des exemples des informations que retrouve automatiquement, le logiciel ThunderBird :

1. 1er exemple : avec une adresse chez gmail.com :



2. 2ème exemple, avec une adresse chez free.fr :



Comme vous pouvez le voir, sur la ligne serveur sortant SMTP
Thunderbird ne vous propose pas par défaut le protocole sécurisé (pas de chiffrement).
Si vous voulez un peu sécuriser vos envois de mails,
utilisez le même serveur smtp.free.fr mais avec le port 587 et mot de passe chiffré ! (voir ci-dessous)

Comme je vous le disais au-dessus, la plupart des clients lourds retrouvent les paramètres en fonction de l'adresse, mais si cela ne fonctionne pas ou que les paramètres ne vous conviennent pas.

[...]

Introduction à ITIL

ITIL (IT Information Library, traduisez bibliothèque de l'infrastructure des technologies de l'information) est un cadre de référence (en anglais framework) proposé par l'OGC (Office of Government Commerce) du Royaume-Uni rassemblant, dans un ensemble de guides, les meilleures pratiques en matière de management des services informatiques.La bibliothèque ITIL a été initiée dès le début des années 80 par le gouvernement britannique afin d'améliorer le service rendu par leurs directions informatiques.

L'objectif d'ITIL est de doter les directions des systèmes informatiques (DSI) d'outils et de documents leur permettant d'améliorer la qualité de leurs prestations, c'est-à-dire améliorer la satisfaction de leurs clients, tout en répondant au mieux aux objectifs stratégiques de l'organisation. Pour ce faire, l'approche consiste à considérer le Service informatique comme un ensemble de processus étroitement liés. Pragmatiquement, ITIL répond à la logique visant à faire en sorte que l'informatique soit au service du personnel et des clients et non l'inverse.

La démarche ITIL n'a pas comme seul bénéficiaires les directions informatiques puisqu'elle consiste à sensibiliser ces dernières sur le fait que la qualité et la disponibilité de l'infrastructure technologique a un impact direct sur la qualité globale de l'entreprise.

Le cadre ITIL

ITIL se décompose en neuf domaines, correspondant à neuf livres, permettant de couvrir l'ensemble des problématiques couvertes par les DSI. Les deux premiers (en gras) sont considérés comme le coeur de la méthode ITIL :

- **Service Support**
- **Service Delivery**
- Infrastructure Management
- Applications Management
- Service Management
- Business Perspective
- Business Requirements
- Technology

Service Support

Le domaine « Service Support » s'attache au fonctionnement et au support de l'infrastructure technologique. Il est décomposé selon les 6 processus suivants :

Processus	Objectif
Gestion des configurations	Geacute;rer l'infrastructure technologique en faisant un état des lieux de l'existant afin de mieux le gérer et le faire évoluer.
Gestion des incidents	Mieux détecter les incidents, améliorer le délai de résolution des incidents selon leur criticité sur le fonctionnement de l'entreprise.

Gestion des problèmes	Mieux gérer les problèmes récurrents et mettre en oeuvre des solutions de prévention afin de réduire leur occurence, voire les supprimer.
Gestion des changements	Mettre en oeuvre des démarches de conduite du changement afin d'anticiper les effets de bord.
Gestion des mises en oeuvre	S'assurer de l'adéquation du service avec les besoins métiers.
Gestion de la disponibilité	Assurer un niveau de disponibilité suffisant à un coût raisonnable.

Service Delivery

Le domaine « Service Delivery » .Il est décomposé en 4 processus comme suit :

Processus	Objectif
Gestion des niveaux de service	Maintenir un certain niveau de qualité de service grâce à des contrats de service renégociés périodiquement.
Gestion des capacités	Vérifier l'adéquation des capacités et performances avec les exigences actuelles et à venir.
Gestion de la continuité des services IT	Définir et mettre en oeuvre des délais contractuels pour la reprise après incident.
Gestion financière des services IT	Gérer la rentabilité des moyens mis en oeuvre pour fournir le service.

Bénéfices de la démarche ITIL

Etant donné que la démarche ITIL propose un référentiel des meilleures pratiques, les plus value de sa mise en oeuvre généralement constatées sont les suivants :

- Satisfaction des utilisateurs (personnel et clients),
- Clarification des rôles
- Amélioration de la communication inter-services
- Mise sous contrôle des processus avec des indicateurs pertinents et mesurables, permettant d'identifier les leviers pour réaliser des économies
- Meilleure compétitivité
- Sécurité accrue (disponibilité, fiabilité, intégrité)
- Capitalisation des données de l'entreprise
- Optimisation de l'utilisation des ressources
- Outil de parangonnage (benchmarking) et outil de positionnement vis-à-vis de la concurrence

Le rançongiciel

Qu'est-ce que c'est ?

C'est un programme malveillant, de type WannaCry ou Locky, qui provoque le blocage ou le chiffrement de tous vos fichiers d'ordinateur y compris ceux en partage en réseau.

Comment ça marche ?

Une rançon, en crypto-monnaie (monnaie utilisable sur un réseau informatique décentralisé) de type bitcoin la plupart du temps, vous est demandée en contrepartie du rétablissement de l'accès à l'ordinateur ou de la fourniture d'une clé de déchiffrement.

Cette méthode permet de masquer l'identité de l'attaquant et empêche toute poursuite judiciaire. De plus vous êtes mis sous pression puisqu'un chronomètre affiche le temps restant jusqu'à l'augmentation de la rançon, la destruction de vos données ou de leur diffusion en clair sur les réseaux.

Quel est son mode de propagation ? La diffusion de pièces jointes par courrier électronique reste le mode d'infection de plus courant ainsi que la mise à disposition d'un lien vers un site internet ayant une apparence authentique.

Comment se prémunir ?

Le facteur humain est déterminant puisque l'inattention de l'utilisateur conditionne la réussite de l'attaque. Vous devez être vigilant quant aux risques inhérents à l'ouverture de documents provenant d'émetteurs inconnus et/ou douteux.

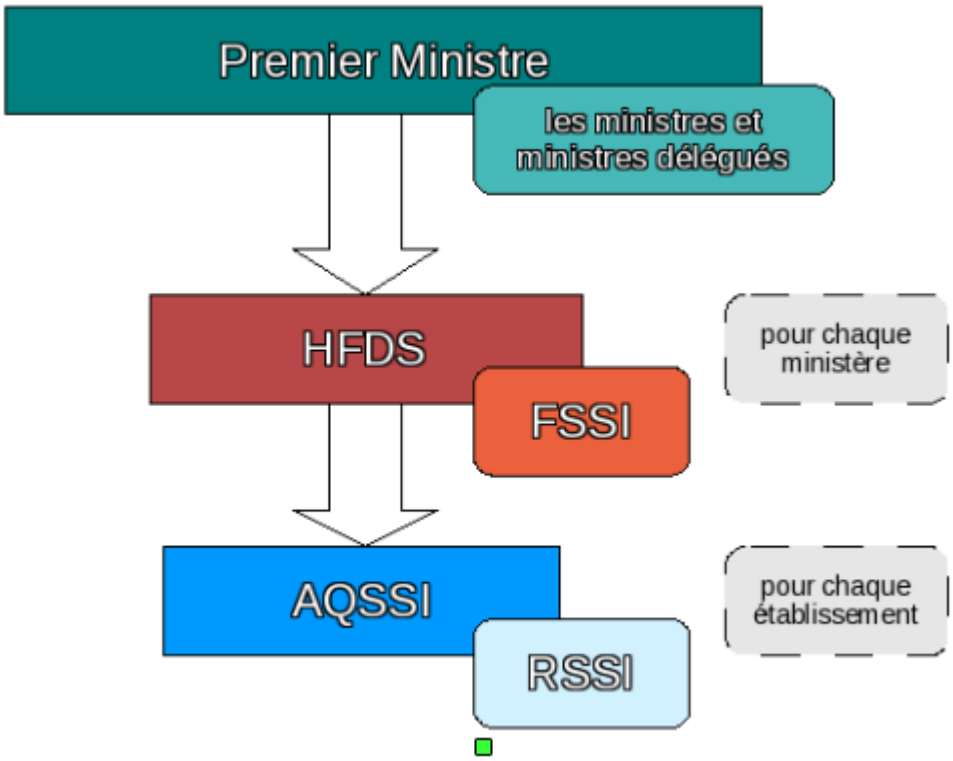
- effectuez des sauvegardes fréquentes, ainsi en cas de chiffrement du disque dur, une restauration des données sera possible,
- évitez l'ouverture de pièces jointes de type SCR ou CAB,
- n'ouvrez pas vos courriels et ne naviguez pas depuis un compte ayant des autorisations « administrateur » mais privilégiez un compte utilisateur,
- utilisez un antivirus et mettez le régulièrement à jour, effectuez vos mises à jour logiciels et système.

Que faire en cas d’incident ?

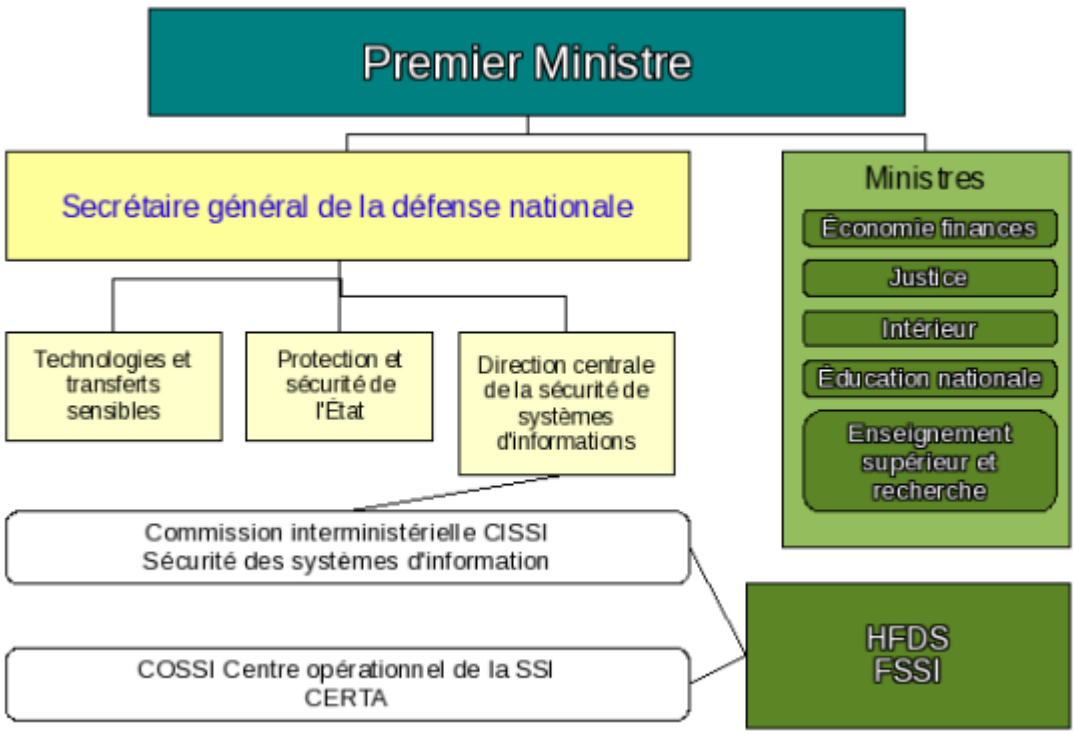
- déconnectez immédiatement votre poste de l’internet (arrêt du wi-fi, cable Ethernet débranché),
- ne payez pas la rançon car cette action ne garantie pas la récupération de vos données et serait un encouragement pour une nouvelle attaque,
- reformatez votre poste et installez un système sain.

Le RSSI dans la chaîne fonctionnelle SSI

La chaîne fonctionnelle selon la recommandation interministérielle n°901



L'organisation interministérielle de la SSI



Les acteurs de la SSI

Les définitions suivantes sont tirées de la recommandation interministérielle n°901 et issues de la présentation de la chaîne fonctionnelle SSI au journées de CRSSI du CNRS 2007 par Isabelle Morel, ancien FSSI MEN/MESR.

HFDS – Haut fonctionnaire de défense et de sécurité

Définition :

« …est le conseiller du ministre pour toute question relative à la défense, la sécurité et la vie de la nation.» *Décret 2007-207 du 19 février 2007*

Son rôle :

- Animer et coordonner la préparation des mesures de défense, de vigilance, de prévention de crise et de situation d'urgence, et contrôler leur exécution
- Veiller à la protection du patrimoine scientifique et technique notamment en liaison avec les fonctionnaires de sécurité de défense (FSD)
- Animer la politique de sécurité des systèmes d'information et contrôler son application

FSD - Fonctionnaire de sécurité de défense

Définition :

Il est le correspondant du HFDS au niveau de chaque établissement d'enseignement supérieur et de chaque organisme de recherche.

Son rôle :

- La protection du patrimoine scientifique et technique
- La préparation et l'exécution des plans de défense et de sécurité
- La protection du secret

FSSI - Fonctionnaire de la sécurité des systèmes d'information

Définition :

« …un fonctionnaire de sécurité des systèmes d'information (FSSI) est désigné par le HFDS et placé sous son autorité…»

Son rôle :

- Porter la réglementation interministérielle relative à la SSI vers les AQSSI
- Participer à l'élaboration des politiques SSI et schémas directeur des grandes entités du ministère et en contrôler l'application
- Veiller à la coordination des flux de communication entre les différents acteurs ainsi qu'à la mutualisation des actions de formation, de sensibilisation et de retours d'expérience.
- Assurer la liaison avec les commissions interministérielles et ministérielles spécialisées en matière de SSI.

AQSSI - Autorités qualifiées pour la SSI

Définition :

« … autorités responsables de la SSI dans les administrations centrales et les services déconcentrés, ainsi que dans les établissements publics … »
« … Leur responsabilité ne peut pas se déléguer … » Dans les faits, il s'agit du chef d'établissement.

Son rôle :

- Définir une politique de sécurité des systèmes d'information adaptée à son organisme et en fixer les objectifs
- Assurer la responsabilité globale du niveau de sécurité requis
- Veiller à la mise en œuvre des dispositions réglementaires
- Procéder aux arbitrages et aux contrôles

RSSI (ASSI dans la circulaire)

Définition :

« … assistent les AQSSI »
« … chargés de la gestion et du suivi des moyens de sécurité des systèmes d'information se trouvant sur le ou les sites où s'exercent leurs responsabilités »

Son rôle :

- Seconder et conseiller les AQSSI. Ils doivent à ce titre avoir une connaissance de l'ensemble des activités des sites où s'exercent leurs responsabilités.
- Assurer le suivi des moyens nécessaires à la mise en oeuvre des consignes et directives définies par l'AQSSI à qui ils rendent compte.