


**Sécurité informatique**

**Protection des données personnelles**

**Sensibilisation**



- **Protéger son matériel**
- **Protéger ses données**
- **Protéger sa vie privée**

The background features a light gray field with faint, semi-transparent text and binary code. The text includes "NAME ADRES", "OLIN", and "IN". Binary strings like "011010101101010110101101" and "01101001010010101101001" are scattered throughout. The central text is bold and black.


**RISQUE :**  
**MENACE + VULNERABILITE**  
**SOLUTIONS**

# ***Menaces & Vulnérabilités***

Matériel

**Matériel** = ordinateur, disques, médias, câbles

Matériel obsolète / Mauvais état  → inutilisable

Pas sécurisé  → Vol – dommages – destruction

# *Menaces & Vulnérabilités*

Logiciel

Logiciel Système & applications

Logiciels pas adaptés, défectueux

Mises à jour non effectuées

protection (firewall, anti-virus)

- Plantage
- trous de sécurité
- Virus

# Menaces & Vulnérabilités

Humain

Vous : l'utilisateur

- Négligence 🙄
- Ignorance 😐
- Erreur 😬

Les autres :

- environnement 👁️👁️
- réseau 😈

# ***Pour se protéger***

## Préservez votre matériel

- Entretenez le
- Protégez le
  - humidité
  - chaleur
  - électromagnétisme
  - transport
  - Stockage (médiats)
- Manipulez avec précaution :
  - disques durs
  - lecteurs DVD
  - câbles

# *Pour se protéger*

## Logiciels

- Faites les mises à jour
  - Système
  - Applications
- Maintenance logiciel
  - réparer les autorisations
  - Utilitaires (CleanMyMac, Onyx)
- Protégez votre mac :
  - Firewall
  - anti virus...(pas nécessaire)
  - Réglages navigateur internet
  - Réglages mail
- Sauvegardez vos données
  - Time Machine
  - Clonez votre disque : carbon copy cloner



# ***Pour se protéger***

## Utilisateur

- Protégez vous
  - Connaissez vos logiciels/Matériels
  - N'installez pas n'importe quoi (pour essayer !)
  - Ne tentez pas des opérations que vous ne maîtrisez pas
  - Maintenez le matériel et les logiciels
  - Adoptez une bonne stratégie de sauvegarde (archivage)
- Protégez vous des autres
  - Utilisez des mots de passe
  - déplacements (filtre écran)
  - Activez le firewall
  - Utilisez les réglages de sécurité
  - Soyez prudents sur le web
  - Soyez vigilants et malins avec le courrier électronique
  - Utilisez le compte invité
  - vendeur : remettez une configuration neutre



# PAUSE



# *Les mots de passe*

- Protégez votre session – mise en veille
- MDP Facile à retenir (xpJy@n+&%Uf528##gloups!)
- Phrase de passe
- Une phrase par service
- l'écrire pour s'en rappeler
- Stockage des MDP (Onepassword)
- test : <http://howsecureismypassword.net>

# ***Les mots de passe***

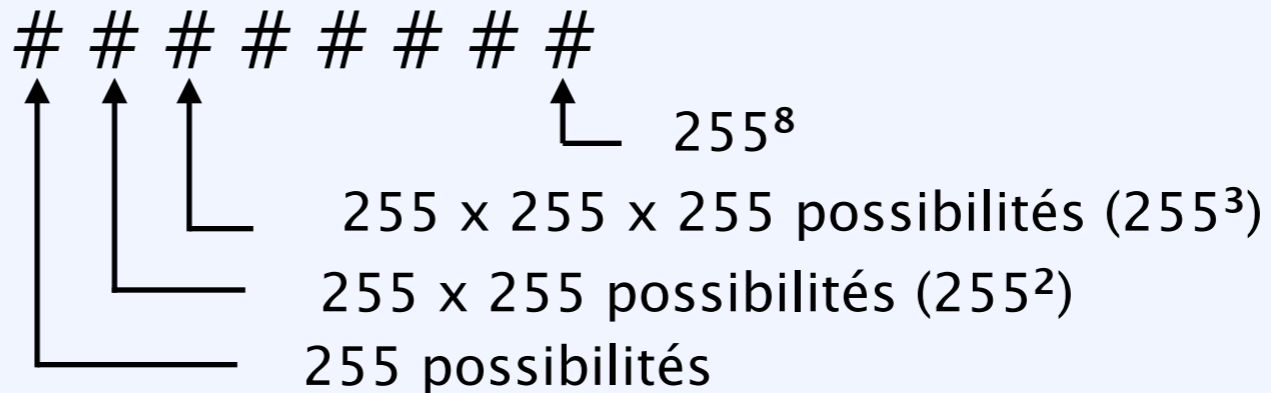
## Risques sur les mots de passe

- Attaque par dictionnaire
- attaque par force brute

# *les mots de passe*

Force d'un mot de passe  
capacité à résister à une énumération des MDP possibles

Décryptage  
par énumération



Il est plus facile d'allonger un mot de passe  
que de chercher à le rendre plus complexe

Complexité = oubli

# *Utiliser internet*

## Attaques sur le réseau

### **Le sniffing :**

technique permettant de récupérer toutes les informations transitant sur un réseau (on utilise pour cela un logiciel sniffer). Elle est généralement utilisée pour récupérer les mots de passe des applications qui ne chiffrent pas leurs communications, et pour identifier les machines qui communiquent sur le réseau.

### **La mystification (en Anglais spoofing) :**

technique consistant à prendre l'identité d'une autre personne ou d'une autre machine. Elle est généralement utilisée pour récupérer des informations sensibles, que l'on ne pourrait pas avoir autrement.

### **Le déni de service (deny of service en Anglais) :**

technique visant à générer des arrêts de service, et ainsi d'empêcher le bon fonctionnement d'un système.

# *Utiliser internet*

Naviguer sur le Web

Cookies

Caches

validation URL

logique

prudence sur les forums

Achats : site sécurisé (https - )

téléchargement : légal sinon Hadopi ...

# *Utiliser internet*

## Comprendre une URL

### Uniform Resource Locator

protocole://sous domaine.domaine.tld

nom de domaine = masque sur un adresse IP

adresse IP : 255.255.255.255

192.168.0.1



# *Utiliser internet*

## Comprendre une URL

http://compteclient.orange.fr

↑  
protocole

http : **H**yper **T**ext **T**ransfert **P**rotocol

https: **H**yper **T**ext **T**ransfert **P**rotocol **S**ecure

ftp : **F**ile **T**ransfert **P**rotocol

# *Utiliser internet*

décrypter une URL

http://compteclient.orange.fr



Sous domaine

# *Utiliser internet*

## Comprendre une URL

http://compteclient.orange.fr

↑  
domaine

# *Utiliser internet*

## Comprendre une URL

http://compteclient.orange.fr



tld : domaine 1er niveau

.fr

.eu

.net

.org

.com

.gouv

# *Utiliser internet*

Comprendre une URL

<http://orange.compte.fr>

<http://facebook.secure.com>

<http://compte.orange.fr>

# Utiliser internet

## Le courrier électronique

adresse électronique

nom d'utilisateur @ nom de domaine

*titulaire du compte*



*entreprise ou organisation  
ou fournisseur d'accès*

*arobase*

tours.micro.club @ numericable.fr

nom utilisateur : tours.micro.club

mot de passe : #####

# *Utiliser internet*

## Techniques d'attaque par messagerie

**SPAM** : Le spam, ce sont des emails publicitaires indésirables

- activez les filtres antispam, le filtrage du courrier indésirable
- n'achetez pas ce qui vous est proposé
- n'essayez pas de vous désinscrire
- si l'adresse du mail ne vous dit rien, n'ouvrez pas le message

**HOAX** : canular, souvent une chaîne de solidarité. Peux vous inciter à faire des manipulations dangereuses sur votre ordinateur.

**SCAM** : un dignitaire d'un pays d'Afrique vous demande de servir d'intermédiaire pour une transaction financière importante, en vous promettant un bon pourcentage. Pour amorcer la transaction, il vous faut donner de l'argent. C'est bien entendu une arnaque.

**L'Hameçonnage** (filoutage – fishing) :vous recevez un message imitant le format des message. d'un fournisseur, d'une banque, d'une société. Le but est de vous soutirer vos coordonnées, n° de carte... ou de l'argent.

# *Utiliser internet*

## La messagerie électronique

- Vérifiez l'adresse de l'expéditeur, il n'existe pas à priori d'expéditeur de confiance
- Méfiez vous des pièces jointes
- Ne répondez pas à une demande d'informations confidentielles
- Aucune banque/organisme ne vous demandera n° carte ou de compte par mail
- Attention aux chaines de solidarité, ce sont des canulars ou des escroqueries
- [www.hoaxbuster.com](http://www.hoaxbuster.com)
- Vérifiez les liens dans les messages, l'ortographe et le vocabulaire
- paramétrez correctement votre logiciel de courrier électronique (préférences)



# Utiliser internet

## Arnaques : les scam

De: "f2.sankoh@laposte.net" <f2.sankoh@laposte.net>  
Date: Ven 8 août 2003 15:16:57 Europe/Paris  
À: "f2.sankoh" <f2.sankoh@laposte.net>  
Objet: M. Felix Sankoh

M Felix Sankoh  
Abidjan, Cote D'Ivoire.  
Rui 21 de cocody  
Email:fksank@yahoo.fr

Cher Ami(e),

Je viens par la présente solliciter de votre haute bienveillance, une assistance de grande importance.

Je me nomme Monsieur Felix Sankoh je suis le fils de feu Dr.Divine Sankoh ex Directeur des Mines de la république de Sierra-Leone.

Mon père était assassiné par des rebelles de Sam Bockary lors d'une visite sur un site d'exploitation d'or et de diamant situé à 230 KM de FREETOWN, la capitale de notre pays.

Après le décès de notre père, la vie est devenue très difficile pour nous comme on était constamment menacé par les rebelles. Compte tenu de cette situation difficile, ma mère s'est arrangée avec un des meilleurs amis de mon défunt père pour nous faire quitter le pays.

Ma mère a donc pris sur elle tous les biens de mon père qui étaient dans son coffre fort qui sont deux caisses métallique et tous ses documents importants qu'elle a emmené avec moi en Côte d'Ivoire .

Nous sommes présentement en Côte d'Ivoire avec des biens y compris la somme de 14.5 millions des dollar Américains. Comme nous ne connaissons personne en Côte d'Ivoire, ma mère a décidé de déposer les deux caisses métallique dans une compagnie privée de sécurité de la place afin de les sauvegarder et protéger cette importante somme d'argent que nous ne pouvons garder sur nous à l'hôtel.

Compte tenu du climat politique instable en Cote D'Ivoire et que notre famille est très connue dans la sous région, ma mère a décidé de chercher un partenaire afin d'investir cette somme hors du continent dans des domaines rentables, c'est donc la raison pour laquelle nous venons vers vous pour solliciter votre assistance et nous aider à investir dans votre pays.

La meilleure méthode pour conclure cette transaction vue la tension politique en cote D'Ivoire, sera d'expédier les fonds en dans votre pays .

Dès l'arrivée de ces fonds en dans votre pays, vous allez les récupérer et les sauvegarder et engager les démarches pour nous aider à venir s'établir dans votre pays.

Nous avons prévu pour vous les 15 % du montant total de mes biens.

Répondez-moi le plus tôt possible.

Veillez m'excuser pour les fautes d'autographe car ma langue maternelle est l'ANGLAIS.

Que Dieu vous Bénisse !

Felix Sankoh.

# Utiliser internet

## Arnaques : l'hameçonnage (fishing)

Renouvellement <mailtoe@net.fr>

À : m.barbet@wanadoo.fr

"Orange.fr" : Facture impayée



**Refus Bancaire lors de facturation**

**Réf. mail : 0049042797312A8-1A02**

Votre montant a été refusée par votre banque.

Nous vous invitons à remplir le fichier de facturation

Afin de régulariser, vous devez impérativement cliquer sur le lien ci-dessous :

[cliquez ici pour résoudre ce problème](#)

En l'absence de confirmation de votre part dans un délai de 48 heures,

Nous procéderons à suspendre définitivement votre abonnement.

**Pourquoi ce courrier électronique vous a-t-il été envoyé ?**

L'envoi de ce courrier électronique s'applique lorsque votre

Renouvellement est arrivé à terme .

Pour plus d'aide, accéder la page Questions et réponses.

**Luc Vignon.**  
Directeur Relation-Clients

# Utiliser internet

## Arnaques : l'hameçonnage (fishing)

★ **BNP Paribas <assistance@bnp.paribas.fr>**

À : LAVAGNINI française <francoise.lavagnini@club-internet.fr>

Votre conseiller : Votre reçu No 1960043116



**BNP PARIBAS.net** | La banque et l'assurance d'un monde qui change

Bonjour,

Vous avez actuellement **2 messages non lus\***, sur espace sécurisé de [BNPPARIBAS.NET](#).

Emetteur	Objet	Message reçu le	Valable jusqu'au
BNPPARIBAS.NET	<u>Une demande d'activité inhabituelle sur votre carte</u>	05/06/2014	05/07/2014
BNPPARIBAS.NET	<u>Votre carte arrive à suspendu</u>	05/06/2014	05/07/2014

Pour vous connecter à votre Messagerie, il suffit de [Connecter à vos comptes](#)

**Accéder aux messages**

\* Les messages non lus seront automatiquement supprimés à leur date de fin de validité.

**Merci de votre confiance.**  
**BNP Paribas**



Votre Conseiller en agence est joignable sur sa ligne directe (appel non surtaxé). Si vous ne disposez pas de ce numéro de téléphone direct, envoyez-lui un message par votre messagerie sécurisée, il vous le donnera en retour. Vous pouvez aussi contacter le Centre de Relations Clients au 0 820 820 001 (0,12 € TTC/min)

# ***10 règles simples***

- Utilisez des mots de passe (efficaces)
- Changez de mot de passe 2 fois par an
- N'utilisez pas le même mot de passe partout
- Verrouillez votre ordinateur (mobile)
- Utilisez les outils de sécurité (firewall)
- Faites les mises à jour système et applications
- faites des sauvegardes
- Soyez vigilants et malins avec internet
- Evitez les réseaux sociaux (ou soyez discrets)