

# LISTE NOIRE DE L'USURPATION D'IDENTITÉ



AVIS DE RECHERCHE

# LISTE NOIRE DE L'USURPATION D'IDENTITÉ

Petit glossaire de  
l'usurpation d'identité

## NOM :

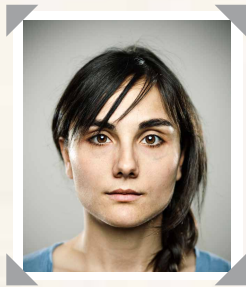
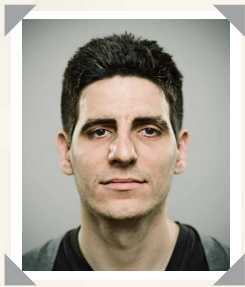
Paulo la Pique / Lulu la Main leste

## MOTIF DE LA RECHERCHE :

Vol

## MODUS OPERANDI :

Vol à la tire



**ALIAS :**  
Fric-Frac

**ALIAS :**  
Lulu la Fauche

**SIGNES  
DISTINCTIFS :**  
Cicatrice au  
front (coup de  
parapluie d'une  
vieille dame)

**SIGNES  
DISTINCTIFS :**  
Tatouage d'un  
sac à main sur  
le poignet droit

Opérant à l'ancienne, cette équipe fauche les portefeuilles et téléphones mobiles dans les poches ou les sacs de leurs victimes, souvent en plein jour. Ils profitent des bousculades dans les foules et affectionnent tout particulièrement les manifestations sportives et les concerts.

Opérant en binôme, Lulu fait diversion : elle fait tomber son sac de courses, appelle à l'aide ou s'arrête brusquement devant vous pendant que Paulo vous bouscule pour vous faire discrètement les poches.

Métros et aéroports font aussi partie de leurs terrains de chasse. Dissimulant leurs mains à l'aide d'un journal ou d'un magazine, ils sont à l'affût de voyageurs distraits ou en pleine conversation téléphonique et subtilisent généralement plusieurs portefeuilles sur un même trajet.

Ils aiment les téléphones mobiles et les PDA car ils sont susceptibles d'héberger une mine d'informations personnelles que leurs propriétaires omettent souvent de protéger par un mot de passe.

Soyez toujours attentif à ce qui vous entoure.  
Pour vous protéger, pensez à prendre  
quelques précautions :

- Gardez votre portefeuille dans votre poche avant, fermez votre sac et gardez-le devant vous (les voleurs pouvant couper la bandoulière).
- Évitez les sacs à dos et les bananes, et protégez votre PDA et/ou téléphone mobile par un mot de passe.
- N'emportez vos cartes bancaires et cartes de crédit avec vous qu'en cas de nécessité.



McAfee

# LISTE NOIRE DE L'USURPATION D'IDENTITÉ

Petit glossaire de  
l'usurpation d'identité

**NOM :**  
**Le Centaure**

**MOTIF DE LA  
RECHERCHE :**  
**Racket**

**MODUS OPERANDI :**  
**Cheval de Troie**



**ALIAS :**  
**Le Jockey**

**SIGNES DISTINCTIFS :**  
**Fer à cheval sur le mollet droit**

Si les centaures de la mythologie étaient de fascinantes et mystérieuses créatures, mi-homme mi-cheval, ils étaient aussi redoutables et sans pitié.

Voici donc un criminel qui mérite bien son surnom. Inoffensif en apparence, il ne fait pourtant pas de quartier et se révèle aussi sournois qu'un autre destrier mythique, le cheval de Troie. Au départ, il se contentait d'introduire des fichiers malveillants dans les pièces jointes des e-mails. A présent, il ajoute ses [charges actives](#) à des photos gratuites, à des PDF et à toutes sortes d'autres fichiers téléchargeables sur Internet.

Une fois dans votre système, il peut se livrer à de multiples combines. Il est capable de contrôler votre ordinateur à distance, de s'emparer de vos informations, fichiers et mots de passe personnels et de télécharger des [enregistreurs de frappe](#) ou d'autres outils du même genre.

C'est un grand champion dans la course à l'usurpation d'identité que mènent pirates, auteurs de [phishing](#), maîtres des [robots](#) et autres enregistreurs de frappe, responsables du vol de plus de 17 milliards d'euros dans le monde entier.

**Assurez-vous d'avoir pris toutes les mesures qui s'imposent pour vous mettre à l'abri de ses manigances. Pour vous protéger, pensez à prendre quelques précautions :**

- Dotez-vous d'un logiciel de sécurité complet et automatiquement mis à jour.
- Appuyez sur la touche ESC et quittez sans tarder un site web qui vous demande d'effectuer une mise à jour d'Adobe Flash ou vous propose un autre téléchargement, même s'il paraît à première vue innocent.
- Rendez-vous sur le site de l'éditeur pour effectuer le téléchargement si vous avez vraiment besoin d'une mise à jour, et n'utilisez pas le téléchargement proposé sur un autre site.



McAfee

# LISTE NOIRE DE L'USURPATION D'IDENTITÉ

Petit glossaire de  
l'usurpation d'identité

**NOM :**

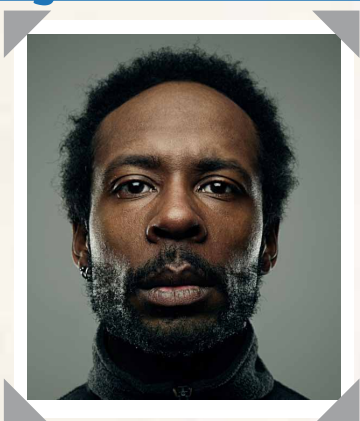
**Charlie Cash dit « la Copie »**

**MOTIF DE LA  
RECHERCHE :**

**Fraude à la carte bancaire  
ou carte de crédit**

**MODUS OPERANDI :**

**Piratage des cartes bancaires**



**ALIAS :**

**Le Vidangeur**

**SIGNES DISTINCTIFS :**

**Tatouage de billets de banque  
sur le pied**

Charlie « la Copie » n'est pas réputé pour sa délicatesse, mais il faut reconnaître qu'il est très doué en électronique. Ce petit ingénieur dispose de tout un arsenal de dispositifs de lecture de cartes et de mini-caméras, capables de lire vos informations bancaires et d'enregistrer votre code PIN.

Si vous avez le malheur d'utiliser l'un des distributeurs de billets qu'il a « améliorés », il recueille, consigne et revend votre numéro de carte et votre code PIN au plus offrant.

Il adore les lieux très fréquentés où il peut s'enrichir très vite avant de disparaître tout aussi rapidement.

Il apprécie tout particulièrement les distributeurs de billets installés dans des sites de concerts, des stades, des stations-service et des superettes. Vider un compte à l'aide des informations personnelles volées est un jeu d'enfant pour lui, mais coûte très cher à ses victimes.

Les dispositifs de lecture illicite de cartes bancaires sont de plus en plus difficiles à détecter. Pour vous protéger, pensez à prendre quelques précautions :

- N'utilisez pas un distributeur de billets si le lecteur de cartes ou le pavé numérique vous semble trop épais ou si vous pouvez faire bouger certains éléments.
- Préférez un distributeur que vous utilisez souvent.
- Couvrez toujours votre main lorsque vous entrez votre code PIN.



McAfee

# LISTE NOIRE DE L'USURPATION D'IDENTITÉ

Petit glossaire de  
l'usurpation d'identité

**NOM :**

**Danny la Poubelle**

**MOTIF DE LA  
RECHERCHE :**

**Usurpation d'identité**

**MODUS OPERANDI :**

**Glanage urbain**



**ALIAS :**

L'Eboueur

**SIGNES DISTINCTIFS :**

Cicatrices sur les bras et les jambes  
(dues à ses nombreuses plongées  
dans les bennes à ordures)

Danny adore raconter qu'il travaille dans le génie sanitaire. De fait, son vrai génie c'est bien de parvenir à faire de l'argent — beaucoup d'argent — avec les ordures des autres...

Son truc, c'est de faire les poubelles et les bennes à ordures pour faire main basse sur des extraits de compte, des demandes de cartes de crédit, des reçus, bref n'importe quel document contenant des informations personnelles.

Ensuite, en toute tranquillité, il déchiffre ou reconstitue les documents déchirés, et en tire tous les renseignements dont il a besoin pour usurper votre identité, mettre à mal votre solvabilité et vous pourrir la vie. S'il veut aller un peu plus loin dans la fraude, une simple recherche lui permettra sans doute de glaner d'autres informations que vous partagez sur Internet.

Et si les trésors ramassés dans les ordures lui permettent de deviner vos mots de passe, c'est direction la banque. La vôtre, naturellement.

Il est difficile de savoir si un « glaneur urbain » a mis la main sur des informations personnelles. Pour vous protéger, pensez à prendre quelques précautions :

- Achetez un bon destructeur de documents et utilisez-le.
- Détruisez tous les documents contenant des informations personnelles (date de naissance, numéro de carte de crédit, factures d'électricité, d'eau ou de téléphone, numéro de permis de conduire, reçus, etc.).



McAfee

# LISTE NOIRE DE L'USURPATION D'IDENTITÉ

Petit glossaire de  
l'usurpation d'identité

**NOM :**

**Foxy la Finaude**

**MOTIF DE LA  
RECHERCHE :**

**Vol de données personnelles**

**MODUS OPERANDI :**

**Reniflage sans fil**



**ALIAS :**

**Le Renard argenté**

**SIGNES DISTINCTIFS :**

**Tatouage d'un renard sur la cheville**

Foxy la Finaude est célèbre pour son efficacité et sa collection d'outils tendance. Son mode opératoire : s'installer dans son cybercafé préféré pour recueillir de croustillantes informations et amasser son butin.

Elle peut se faire passer pour un point d'accès Wi-Fi gratuit et vous laisser accéder Internet via son ordinateur portable pour intercepter vos informations de compte, noms d'utilisateur et autres données personnelles. A l'aide de vos mots de passe, elle peut se connecter à votre compte pendant que vous sirotez tranquillement votre cappuccino à côté d'elle.

En prime, si vous avez activé le partage de fichiers, elle peut parcourir votre ordinateur, copier vos déclarations fiscales et carnets d'adresses ou encore installer des logiciels malveillants qu'elle pourra contrôler à distance, lorsque vous rentrerez à la maison (voir [enregistreur de frappe](#) et [cheval de Troie](#)).

**Soyez extrêmement prudent lorsque vous utilisez des connexions sans fil non sécurisées. Pour vous protéger, pensez à prendre quelques précautions :**

- Ne sélectionnez pas de réseaux aux noms génériques ou peer-to-peer comme « Linksys » ou « WiFi gratuit ».
- Effectuez vos opérations bancaires, achats et autres transactions en ligne sensibles uniquement lorsque vous êtes à la maison ou sur un réseau sécurisé.



**McAfee**

# LISTE NOIRE DE L'USURPATION D'IDENTITÉ

Petit glossaire de  
l'usurpation d'identité

**NOM :**

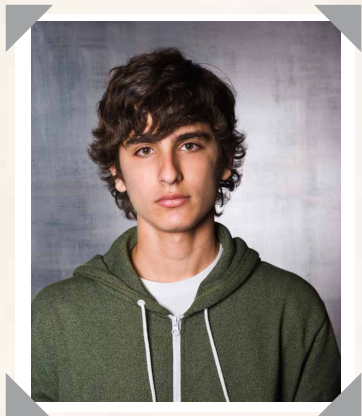
**Bernie le Baladeur**

**MOTIF DE LA  
RECHERCHE :**

**Vol de données personnelles**

**MODUS OPERANDI :**

**War Driving**



**ALIAS :**

**Le Balayeur**

**SIGNES DISTINCTIFS :**

**Tatouages de symboles représentant  
un réseau Wi-Fi ouvert**

Cela vous dit de partager votre connexion Internet privée avec des inconnus ? Pas vraiment, j'imagine. Lui, il adore.

Il sillonne la ville à la recherche de réseaux sans fil ouverts ou non sécurisés. Il lui suffit de passer devant chez vous ou de stationner à proximité, et il se connecte à l'aide de son ordinateur portable, de son smartphone ou de sa Nintendo DS.

Il peut envoyer du spam, surfer à la recherche de contenu illicite ou pornographique, voire explorer le système pour s'emparer d'informations personnelles que vous ne souhaitez pas partager.

Dans la mesure où il peut utiliser votre adresse réseau, il peut effectuer toutes ses opérations sous le couvert de votre identité. Si la police enquête, ce sera à votre porte qu'elle viendra frapper.

Apprenez à sécuriser votre connexion sans fil.  
Pour vous protéger, pensez à prendre  
quelques précautions :

- Modifiez le nom d'utilisateur et le mot de passe par défaut fournis avec le routeur : les pirates informatiques connaissent ces informations de connexion par défaut et les utilisent pour accéder à des réseaux non protégés.
- Désactivez la diffusion de l'identifiant de votre routeur pour empêcher que des tiers voient votre réseau sans fil.
- Activez le chiffrement afin que seuls les utilisateurs disposant du mot de passe correct soient autorisés à y accéder.
- Utilisez un pare-feu pour bloquer les communications émanant de sources non approuvées.



McAfee

# LISTE NOIRE DE L'USURPATION D'IDENTITÉ

Petit glossaire de  
l'usurpation d'identité

**NOM :**

**Aldo dit « Big Phish »**

**MOTIF DE LA  
RECHERCHE :**

**Fraude à la carte bancaire  
ou carte de crédit**

**MODUS OPERANDI :**

**Phishing (hameçonnage)**



**ALIAS :**

**Le Hameçonneur des Lilas,  
le Boss, l'Appâteur**

**SIGNES DISTINCTIFS :**

**Hameçon sur le biceps gauche**

Ce roi du hameçonnage a dérobé plus de 175 millions d'euros à des internautes trop confiants dans le monde entier.

D'abord, il débarque dans votre boîte de réception sous l'apparence d'un innocent représentant en clientèle de votre banque ou société de cartes de crédit. Il prétend avoir besoin de « mettre à jour » votre dossier et, pour ce faire, vous demande franco votre mot de passe ou votre numéro de compte. Il vous invite ensuite à entrer ces données en suivant le lien d'un site web inclus dans son message. Cet e-mail ressemble bien à un message légitime (après tout, Aldo est un vrai pro), mais le site est bidon.

Et puis, d'hameçonné, vous vous retrouvez pigeon... et c'est vous qui financez les goûts de luxe de monsieur.

**Les spécialistes en phishing sont experts en dissimulation et artifices. Pour vous protéger, pensez à prendre quelques précautions :**

- Ignorez ce type de messages ou contactez votre banque pour les signaler.
- Ne cliquez pas sur des liens inconnus dans des e-mails, des messages instantanés ou des pages Facebook car ils peuvent conduire à des sites factices.
- Ouvrez une nouvelle session de navigateur (pas simplement un onglet) et tapez l'URL pour accéder à un site légitime.
- Utilisez le logiciel McAfee SiteAdvisor® qui évalue les risques présentés par les sites renvoyés par vos recherches.



**McAfee**

# LISTE NOIRE DE L'USURPATION D'IDENTITÉ

Petit glossaire de  
l'usurpation d'identité

**NOM :**

**Jacquot Oeil-de-Lynx**

**MOTIF DE LA  
RECHERCHE :**

**Vol de données**

**MODUS OPERANDI :**

**Espionnage par-dessus  
l'épaule**



**ALIAS :**

La Fouine, le Voyeur,  
le Cyberfaucon

Sa vue perçante, ses jumelles ou une caméra cachée permettent à cet escroc de regarder par-dessus l'épaule des gens au moment où ils tapent leur code PIN aux guichets automatiques, remplissent des formulaires ou se connectent à leurs comptes dans des cybercafés.

Il a tellement perfectionné sa technique que vous n'y verrez que du feu.

Après avoir observé et pris note des chiffres, il met ces informations sensibles en vente sur des réseaux cybercriminels. S'il est quelqu'un dont vous ne souhaitez pas sentir le regard sur vous, c'est bien lui.

**Méfiez-vous des yeux baladeurs.  
Pour vous protéger, pensez à prendre  
quelques précautions :**

- Couvrez toujours votre main ou votre écran lorsque vous entrez votre code PIN.
- Choisissez un siège dos au mur lorsque vous voulez vous connecter dans un cybercafé ou tout autre point d'accès public.



McAfee

# LISTE NOIRE DE L'USURPATION D'IDENTITÉ

Petit glossaire de  
l'usurpation d'identité

**NOM :**  
**François la Frappe**

**MOTIF DE LA  
RECHERCHE :**  
**Usurpation d'identité**

**MODUS OPERANDI :**  
**Enregistrement de frappe**



**ALIAS :**  
**Le Pianiste, le Virtuose**

Ce virtuose du clavier est extrêmement talentueux et enjôleur mais méfiez-vous : il peut infecter votre ordinateur et surveiller toutes vos activités en ligne.

Tout en délicatesse, il infiltre un site web légitime pour y installer son logiciel et attend le passage d'innocents internautes. Lorsque vous accédez au site, son [enregistreur de frappe](#) s'installe silencieusement sur votre ordinateur et surveille le moindre de vos mouvements.

Il consigne toutes vos séquences de frappes au clavier et les envoie à son créateur : noms d'utilisateur, mots de passe, numéros de compte bancaire, numéros de carte de crédit et ainsi de suite. Il lui arrive de s'intéresser aux sites web que vous avez consultés et même d'effectuer des captures d'écran lorsque vous cliquez avec votre souris pour s'emparer de vos codes d'accès.

L'invisibilité est le secret de son succès puisque son logiciel est installé à votre insu et qu'il n'existe aucun signe évident de sa présence sur votre système.

Certains outils sont conçus pour bloquer l'accès de logiciels inconnus à votre ordinateur. Pour vous protéger, pensez à prendre quelques précautions :

- Conservez votre navigateur web parfaitement à jour en lui appliquant les derniers patches publiés.
- Dotez-vous d'un logiciel de sécurité complet et automatiquement mis à jour avec un [pare-feu](#) activé.



McAfee

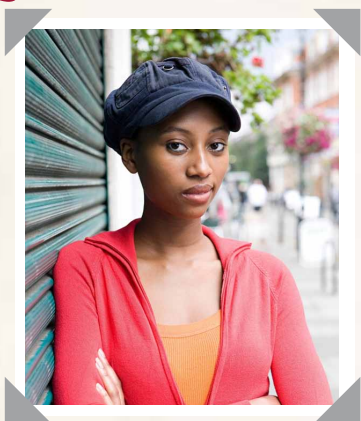
# LISTE NOIRE DE L'USURPATION D'IDENTITÉ

Petit glossaire de  
l'usurpation d'identité

**NOM :**  
**La Postière**

**MOTIF DE LA  
RECHERCHE :**  
**Fraude par courrier**

**MODUS OPERANDI :**  
**Pillage de boîtes aux lettres**



**ALIAS :**  
**La Fouineuse, la Philatéliste**

**SIGNES DISTINCTIFS :**  
**Morsure de chien**

La Postière fouille votre boîte aux lettres non protégée pour y dérober du courrier riche en informations personnelles. Elle affectionne tout particulièrement les demandes et relevés de cartes de crédit, les factures de téléphone, d'eau et d'électricité ainsi que le courrier bancaire et les déclarations fiscales.

Elle exploite toutes ces informations pour ouvrir abusivement des comptes bancaires, comptes de carte de crédit ou abonnements de téléphonie mobile. Elle revient visiter votre boîte aux lettres pour s'emparer des noms d'utilisateur et des mots de passe envoyés par la banque pour chaque nouveau compte. Elle peut même voler ses voisins en s'emparant des relevés dans la boîte aux lettres communautaire pour qu'ils continuent d'ignorer l'existence des comptes.

Cette voleuse souffre de troubles de la personnalité : elle a ouvert plus de 10 000 comptes de cartes de crédit sous différents noms, et accumulé plus de 350 000 euros de factures pour lesquelles elle n'a pas payé un centime. De nombreuses victimes ne se rendent compte de rien pendant plus d'un an... ce qui lui laisse largement le temps d'accumuler les dettes en votre nom.

**Etre proactif est la seule façon de se protéger  
contre les voleurs de courrier postal.  
Pour vous protéger, pensez à prendre  
quelques précautions :**

- Surveillez vos relevés de crédit pour détecter toute activité inhabituelle, par exemple des demandes de notation de crédit et des nouvelles cartes de crédit.
- Demandez à recevoir vos factures en ligne afin d'éviter qu'on vous les envoie par la poste.



McAfee

# LISTE NOIRE DE L'USURPATION D'IDENTITÉ

Petit glossaire de  
l'usurpation d'identité

## Petit glossaire de l'usurpation d'identité

### Attaque de mot de passe

Tentative d'obtention des mots de passe d'un utilisateur à des fins illégales. Les mesures de lutte contre ces attaques sont relativement limitées, mais elles consistent généralement à prescrire une politique en matière de mots de passe stipulant leur longueur minimale, l'emploi de mots non identifiables et l'obligation de les modifier fréquemment.

### Charge active

Domages causés par du code malveillant exécuté par un virus ou un autre [logiciel malveillant](#). La charge active englobe divers types d'activités nuisibles dont le déplacement, l'altération, l'écrasement et la suppression de fichiers.

### Cheval de Troie

Programme malveillant en toute apparence légitime mais conçu pour faciliter l'accès non autorisé au système informatique d'un utilisateur. Les utilisateurs sont amenés par ruse à charger et à exécuter ce logiciel sur leurs systèmes. En général, le cheval de Troie est envoyé par e-mail par un individu, il ne se transmet pas seul. Vous pouvez aussi le télécharger à partir d'un site web ou via un [réseau peer-to-peer](#).

### Cybercriminels

Un cybercriminel est un pirate, craqueur de mots de passe ou autre internaute malveillant qui se sert du Web pour commettre divers délits dont l'usurpation d'identité, le

*suite*

# LISTE NOIRE DE L'USURPATION D'IDENTITÉ

Petit glossaire de  
l'usurpation d'identité

piratage d'ordinateurs, l'envoi illégal de messages de [spam](#), de [phishing](#), de [pharming](#) ou d'autres types de fraude.

## Cybersquattage

Il s'agit de l'enregistrement, du trafic ou de l'utilisation d'un nom de domaine dans l'intention délibérée d'exploiter la clientèle d'une marque commerciale ou d'un nom de marque appartenant à un tiers. Le cybersquatteur propose ensuite de vendre le domaine à la personne ou à la société propriétaire d'une marque commerciale incluse dans le nom, à un prix exagéré. Il arrive également que les cybersquatteurs enregistrent des variantes de marques de grande notoriété, une pratique appelée [typosquattage](#), afin de distribuer leurs [logiciels malveillants](#).

## Enregistreur de frappe

Logiciel malveillant qui enregistre les séquences de touches frappées sur le clavier par l'utilisateur, généralement de manière furtive afin qu'il ne s'aperçoive pas que ses actions sont surveillées et consignées. Les informations enregistrées sont par exemple le texte des messages instantanés et e-mail, les adresses e-mail, les mots de passe, les numéros de compte et de carte de crédit, les adresses personnelles et bien d'autres données confidentielles.

## Espionnage par-dessus l'épaule

Technique d'observation directe dans le but de d'obtenir illicitement des informations saisies par un utilisateur. Simplement en observant par-dessus votre épaule vos frappes sur un clavier,

un criminel peut obtenir votre mot de passe ou votre code PIN lorsque vous vous trouvez à un distributeur de billets ou devant votre ordinateur.

## Exploit

En sécurité informatique, désigne un logiciel qui exploite un bogue ou un problème de fonctionnement dans le but d'induire, dans un autre programme informatique, un comportement imprévu. Il peut par exemple prendre le contrôle d'un ordinateur, modifier les privilèges d'accès ou interdire aux utilisateurs l'accès aux ressources.

## Faux logiciel

Terme parfois utilisé pour désigner un programme conçu pour endommager d'autres programmes ou données ou compromettre la sécurité d'un réseau ou d'un ordinateur.

## Fraude à la carte bancaire (*carding*)

Ce type de fraude commence par le vol d'informations de cartes de crédit, suivi de la vérification de la validité de ces données. Le voleur utilise les informations de la carte sur un site web proposant des transactions en temps réel. Si le traitement de la transaction se déroule correctement, le criminel sait alors que la carte est toujours valable. L'achat porte généralement sur un petit montant, pour éviter de dépasser la limite de la carte et d'attirer l'attention de son propriétaire.

## Fraude par courrier

Fraude qui consiste à obtenir illégalement de l'argent ou d'autres

suite

# LISTE NOIRE DE L'USURPATION D'IDENTITÉ

Petit glossaire de  
l'usurpation d'identité

objets de valeur en utilisant le service postal. Elle peut inclure l'usurpation d'identité par une modification frauduleuse de l'adresse ou par le vol de courrier (pillage de boîtes aux lettres).

## Glanage urbain

Cette pratique consiste à fouiller dans les poubelles de particuliers ou d'entreprises dans l'espoir de trouver des informations à voler ou à exploiter dans le cadre de diverses fraudes.

## Ingénierie sociale

Pratique consistant à manipuler des personnes afin de les pousser à effectuer certaines actions ou à divulguer des informations confidentielles. Basée sur les interactions humaines, elle tente notamment d'obtenir la confiance d'un tiers par des manœuvres trompeuses afin de recueillir des informations, d'accéder à un système informatique ou de se livrer à diverses fraudes.

## Logiciel espion (spyware)

Logiciel installé subrepticement par un pirate sur votre ordinateur pour collecter des informations personnelles à votre insu. Outre surveiller vos activités sur l'ordinateur, il peut également vous diriger vers des sites web factices, modifier vos paramètres ou prendre le contrôle de votre ordinateur de diverses façons.

## Logiciel malveillant (malware)

Terme générique utilisé pour décrire les logiciels conçus dans le but

d'accéder secrètement à un système informatique à l'insu de son propriétaire. Les logiciels malveillants incluent les virus, les vers, les [chevaux de Troie](#), les [logiciels espions](#) et divers autres contenus malveillants actifs.

## Logiciel publicitaire (adware)

Logiciel qui lit, affiche ou télécharge automatiquement des publicités sur un ordinateur. Les publicités affichées sont ciblées en fonction des renseignements obtenus sur les habitudes de navigation de l'internaute. La plupart des logiciels publicitaires sont inoffensifs, mais certains jouent également le rôle de [logiciels espions](#), lesquels recueillent des informations personnelles sur votre disque dur, les sites web que vous consultez ou encore vos frappes au clavier. Certains types de logiciels publicitaires sont en mesure de capturer ou de transmettre des informations personnelles.

## Pare-feu

Matériel ou logiciel conçu pour bloquer les accès non autorisés tout en acceptant les communications autorisées. Il est configuré pour accepter ou refuser les transmissions réseau en fonction d'une série de règles. Sa fonction consiste à protéger les ressources du réseau contre d'autres utilisateurs d'autres réseaux.

## Pharming

Pratique consistant à rediriger le trafic vers un site web factice, généralement au moyen de [logiciels malveillants](#) ou de [logiciels espions](#).

suite

# LISTE NOIRE DE L'USURPATION D'IDENTITÉ

Petit glossaire de  
l'usurpation d'identité

Un pirate crée un site web frauduleux en tout point similaire à un site web légitime afin de capturer les informations confidentielles des internautes.

## Phishing

Parfois appelé « hameçonnage ». Forme d'activité criminelle qui s'appuie sur des techniques d'[ingénierie sociale](#) et perpétrée par l'intermédiaire de la messagerie électronique ou instantanée. Les auteurs d'attaques par phishing tentent d'obtenir par des moyens frauduleux les données personnelles d'autrui, par exemple leurs mots de passe ou leurs informations de carte de crédit. Pour ce faire, ils envoient à leurs cibles des communications aux allures légitimes par voie électronique, se faisant passer pour des sociétés ou des personnes de confiance. En règle générale, les e-mails de phishing demandent aux destinataires de cliquer sur un lien qu'ils contiennent pour vérifier ou mettre à jour des informations de contact ou de carte de crédit. A l'instar du [spam](#), un e-mail de phishing est envoyé en masse, pariant sur le fait que certains des destinataires suivront les consignes et divulgueront des informations personnelles. Les SMS et le téléphone sont également des vecteurs d'attaques par phishing (voir [SMiShing](#) ou [Vishing](#)).

## Pilleurs d'informations

Type de cybercriminel qui revend les données volées, mais ne les utilise pas nécessairement pour commettre des fraudes. Les informations

obtenues par les pilleurs sont vendues aux réseaux criminels qui négocient les informations dans les bas-fonds d'Internet.

## Piratage d'accès

Pratique consistant à accéder de façon non autorisée à un système en exploitant la connexion légitime d'un utilisateur autorisé sans son consentement ou à son insu.

## Piratage des cartes bancaires

Cette technique de fraude consiste à recueillir les informations de compte ou codes PIN des victimes en connectant des dispositifs de piratage aux distributeurs de billets dans lesquels les utilisateurs insèrent leurs cartes magnétiques.

## Pirate de navigateur

Ce type de [logiciel malveillant](#) modifie les paramètres d'un navigateur web. On parle de « piratage » dans la mesure où les modifications sont effectuées sans le consentement de l'utilisateur. Certains actes de piratage peuvent être facilement corrigés, alors que d'autres sont nettement plus difficiles à contrer. Ces programmes détournent le plus souvent la page d'accueil, la page de recherche, les résultats de recherche, les pages de messages d'erreur ou tout autre contenu affiché par le navigateur, les remplaçant par du contenu inattendu ou indésirable. Ils peuvent également rediriger l'internaute vers des sites qu'il n'avait pas l'intention de visiter.

suite

# LISTE NOIRE DE L'USURPATION D'IDENTITÉ

Petit glossaire de  
l'usurpation d'identité

## Porte dérobée (*backdoor*)

Fonctionnalité d'un programme permettant à l'auteur d'une attaque d'avoir accès à un autre ordinateur ou d'en prendre le contrôle à distance, à l'insu de l'utilisateur. Les programmeurs informatiques créent généralement des portes dérobées dans les applications pour pouvoir corriger des erreurs. Si des pirates informatiques ou d'autres individus malveillants apprennent l'existence de ce type de composant, cela peut poser un risque pour la sécurité.

## Ransomware

Littéralement, « logiciel de demande de rançon ». Logiciel malveillant qui chiffre le disque dur de l'ordinateur qu'il infecte. Le pirate entreprend ensuite d'extorquer des fonds au propriétaire de cet ordinateur, en échange de quoi il fournira le logiciel de déchiffrement nécessaire pour permettre d'accéder à nouveau aux données.

## Reniflage de mots de passe

Utilisation d'un outil dans le but d'intercepter des mots de passe transmis sur un réseau ou sur Internet. Un renifleur peut être un composant matériel ou logiciel.

## Réseau de robots — Robot (voir aussi **Zombie**)

Ensemble d'ordinateurs [zombies](#) qui fonctionne de façon indépendante et automatique. Le réseau de robots est aussi appelé botnet, contraction des termes anglais « robot » et « network ». L'ordinateur peut être compromis par un pirate, un virus

informatique ou un [cheval de Troie](#).

Un réseau de robots est composé de dizaines, voire de centaines de milliers d'ordinateurs zombies. Un seul ordinateur d'un réseau de robots peut envoyer automatiquement des milliers de messages de [spam](#) par jour. Les messages de spam les plus courants proviennent d'ordinateurs zombies.

## Réseau peer-to-peer

Parfois abrégé en « P2P ». Système distribué pour le partage de fichiers au sein duquel tout ordinateur du réseau peut « voir » les autres ordinateurs connectés. Les utilisateurs peuvent accéder réciproquement à leurs disques durs pour télécharger des fichiers. Ce type de réseau présente des avantages, mais il alimente les infractions aux droits d'auteur lors de l'échange de fichiers musicaux, de films et d'autres fichiers multimédias partagés. De plus, ses utilisateurs sont particulièrement exposés aux virus, aux [chevaux de Troie](#) et aux [logiciels espions](#) qui se dissimulent dans les fichiers partagés.

## Rootkit

Logiciel conçu pour accéder à un ordinateur tout en dissimulant sa présence au propriétaire ou utilisateur de l'ordinateur. Il s'agit généralement de [logiciels malveillants](#) qui utilisent les ressources de l'ordinateur ou volent des mots de passe à l'insu du propriétaire de l'ordinateur.

## SMiShing

Utilisation de techniques d'ingénierie sociale similaires au [phishing](#) mais

suite

# LISTE NOIRE DE L'USURPATION D'IDENTITÉ

Petit glossaire de  
l'usurpation d'identité

via SMS. Il s'agit d'une contraction des termes « SMS » et « phishing ». Un SMS, ou texto, est un message texte envoyé à partir d'un téléphone mobile. La technique du SMiShing utilise ces messages pour vous inciter à divulguer des informations personnelles. Le SMS peut être lié à un site web ou à un numéro de téléphone qui établit une connexion à un système de messagerie vocale automatisé.

## Spam

Messages électroniques envoyés en masse, non sollicités ou indésirables. Le spam peut être envoyé par l'intermédiaire de la messagerie électronique, de la messagerie instantanée, de moteurs de recherche, de blogs, de réseaux sociaux et de SMS. Le spam inclut les publicités légitimes ou trompeuses, de même que les messages de [phishing](#) conçus pour amener les destinataires peu méfiants à communiquer leurs informations personnelles et financières. Un e-mail n'est pas considéré comme du spam si l'utilisateur a explicitement donné son consentement pour qu'il lui soit envoyé.

## Spim

Spam ciblant la messagerie instantanée. Les messages peuvent être de simples publicités non sollicitées ou des messages de [phishing](#) frauduleux.

## Téléchargements involontaires

Certains programmes sont conçus pour se télécharger automatiquement

sur l'ordinateur de l'internaute sans son consentement et parfois à son insu. Ils y installent ensuite des [logiciels malveillants](#) ou des programmes potentiellement indésirables sans autre interaction préalable que l'ouverture d'un e-mail ou l'accès à un site.

## Typosquattage ou piratage d'URL

Forme de cybersquattage qui mise sur des erreurs des internautes, telles des fautes de frappe, lors de la saisie d'une adresse de site web dans un navigateur. Si l'utilisateur entre accidentellement l'adresse incorrecte, il peut être dirigé vers un autre site web appartenant à un cybersquatteur.

## Usurpation criminelle d'identité

Délit par lequel un criminel utilise l'identité d'une autre personne pour s'identifier auprès des forces de l'ordre, par exemple au moment de son arrestation. Il arrive que les malfaiteurs présentent des pièces d'identité obtenues auprès de l'administration à l'aide d'informations d'identification volées, ou simplement de faux papiers.

## Usurpation d'identité d'enfant

On assiste à une augmentation remarquable du nombre d'usurpations d'identités d'enfants, même en bas âge. Pour un criminel, il s'agit d'une identité particulièrement intéressante car vierge de tout passif. Le méfait n'est généralement découvert qu'après de nombreuses années, lorsque la victime effectue ses premières transactions financières.

suite

# LISTE NOIRE DE L'USURPATION D'IDENTITÉ

Petit glossaire de  
l'usurpation d'identité

Les risques sont nombreux, tels qu'un mauvais profil de solvabilité ou des obligations fiscales.

## **Vishing (voir aussi Phishing)**

Pratique criminelle consistant à se faire passer pour une source légitime afin d'obtenir des informations par téléphone ([phishing](#) par téléphone/messagerie vocale). Elle est facilitée par la technologie VoIP (voix sur IP) car elle peut usurper l'ID de l'appelant pour avoir accès à des informations personnelles et financières.

## **War Driving**

Technique consistant à déambuler en voiture à la recherche de réseaux sans fil non sécurisés, pour y subtiliser des informations personnelles à l'aide d'un ordinateur portable ou d'un PDA. Si la connexion sans fil de votre domicile n'est pas sécurisée, les voleurs peuvent accéder aux données présentes sur tous les ordinateurs connectés à votre routeur sans fil, et voir toutes les informations que vous entrez sur les sites bancaires et les formulaires de paiement par carte de crédit.

## **Zombie**

Ordinateur compromis par un virus ou un [cheval de Troie](#) qui le place sous le contrôle distant d'un pirate connecté à Internet. Le pirate l'utilise pour envoyer du [spam](#) ou rendre l'ordinateur inutilisable par son propriétaire. L'utilisateur ne se rend généralement pas compte que

son ordinateur a été compromis. La plupart du temps, l'ordinateur zombie est intégré à un [réseau de robots](#) qui contrôle à distance un grand nombre d'ordinateurs comme lui afin de se livrer à diverses activités malveillantes.



# LISTE NOIRE DE L'USURPATION D'IDENTITÉ



Limitation de responsabilité : les renseignements contenus dans le présent document ne sont fournis qu'à titre informatif, au bénéfice des clients de McAfee. Les informations présentées ici peuvent faire l'objet de modifications sans préavis et sont fournies sans garantie ni représentation quant à leur exactitude ou à leur adéquation à une situation ou à des circonstances spécifiques. McAfee et le logo McAfee sont des marques déposées ou des marques commerciales de McAfee, Inc. ou de ses filiales aux Etats-Unis et dans d'autres pays. Les autres marques et noms peuvent être la propriété d'autres sociétés.

©2011 McAfee, Inc. McAfee, le logo McAfee et McAfee Labs sont des marques commerciales déposées ou des marques commerciales de McAfee, Inc. et/ou de ses sociétés affiliées aux Etats-Unis et/ou dans d'autres pays. Les autres marques et noms peuvent être la propriété d'autres sociétés.