

Rappels sur la sécurité



Menaces & Vulnérabilités

Matériel & logiciels:

- Entretien
- mises à jour

Vous : l'utilisateur

- Négligence 
- Ignorance 
- Erreur 

Les autres :

- environnement 
- réseau 

Pour se protéger

- **Faites les mises à jour**
 - Système
 - Applications
- **Maintenance logiciel**
 - Utilitaires (CleanMyMac, Onyx)
- **Protégez votre mac :**
 - Firewall
 - Réglages navigateur internet et mail
- **Sauvegardez vos données**
 - Time Machine
 - Clonez votre disque : carbon copy cloner

Pour se protéger

● **Protégez vous**

- Connaissez vos logiciels/Matériels
- N'installez pas n'importe quoi (pour essayer !)
- Ne tentez pas des opérations que vous ne maîtrisez pas
- Adoptez une bonne stratégie de sauvegarde

● **Protégez vous des autres**

- Utilisez des mots de passe
- Soyez prudents sur le web
- Soyez vigilants et malins avec le courrier électronique
- Utilisez le compte invité
- vendeur : remettez une configuration neutre

Malware - Adware

Les malwares (contraction de « malicious » et « software »)

Ce sont des logiciels malveillants.

Leur but est d'accéder à l'appareil d'un utilisateur à son insu.

Ces types de logiciels incluent les logiciels espions, les logiciels publicitaires, les virus, les chevaux de Troie, les vers informatiques, les rootkits, les logiciels de rançon et les détourneurs de navigateur.

Il est facile de s'en prémunir en ne téléchargeant que depuis des sources réputés sûres (sites d'éditeurs fiables .)... 😊

Sinon on peut s'en débarrasser avec un logiciel gratuit comme **Malwarebytes**



Utiliser internet

Comprendre une URL

Uniform **R**essource **L**ocator

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

Comprendre 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://www.orange/clients.fr

page « orange » sur le site "clients.fr"

http://www.clients/orange.fr

Page « clients » sur le site "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

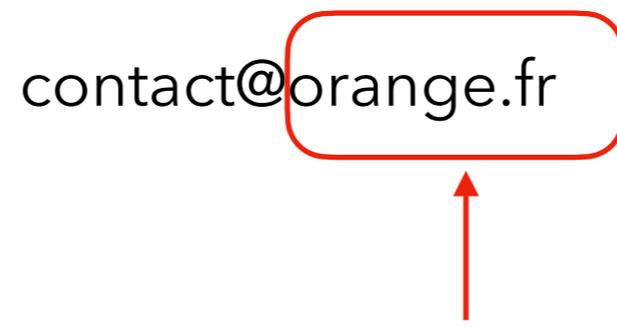
nom utilisateur : tours.micro.club

mot de passe : #####

Utiliser internet

Le courrier électronique

contact@orange.fr



L'expéditeur à un compte chez « orange »

contact@orange.compte.fr



L'expéditeur a un compte chez « compte »

Utiliser internet

Techniques d'attaque par messagerie



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, ne répondez pas.

HOAX: canular, souvent une chaîne de solidarité.

SCAM: l'expéditeur 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.

L'Hameçonnage (filoutage - phishing) : vous recevez un message imitant le format des messages d'un fournisseur, d'une banque, d'une société.

Le but est de vous soutirer vos coordonnées, n° de carte... ou de l'argent.

Le chantage à la webcam Ce nouveau concept consiste à piéger une personne sur le web et à lui demander de l'argent en la menaçant de divulguer des photos ou vidéos peu flatteuses voire compromettantes.

Utiliser internet

Arnaques : le chantage à la webcam

L'arnaque à la webcam débute généralement à l'occasion d'un simple chat sur un réseau social, sur Skype ou un site de rencontre. De nombreux « brouteurs » opèrent depuis la côte d'Ivoire ...

Les attaques de faux hackers :

ils se font passer pour des hackers ayant piraté votre compte et votre webcam et prétendent avoir des vidéos compromettantes. C'est faux. Le messages est standardisé et il vous réclament une rançon en Bitcoins.

Leur but est de faire peur pour obtenir une rançon.

Ces messages frauduleux ne sont pas ciblés et sont diffusés en masse, peu importe que les destinataires soient allés ou non sur un site pornographique.

Parfois le message prétend utiliser un compte et/ou un mot de passe qu'utilise effectivement le destinataire. Les escrocs l'ont récupéré dans des bases de données qui ont fuité sur Internet

Arnaques : le chantage à la webcam

Vous ne me connaissez pas et vous vous demandez probablement pourquoi vous recevez ce mail, non?

Je suis un hacker qui a piraté vos appareils il y a quelques mois.

Je vous ai envoyé un e-mail depuis VOTRE compte piraté.

J'ai mis en place un virus sur le site pour adulte (porno) et devinez quoi, vous avez visité ce site pour vous amuser (vous savez ce que je veux dire).

Pendant que vous regardiez des vidéos, votre navigateur internet a commencé à fonctionner comme un RDP (contrôle à distance) ayant un keylogger, ce qui m'a donné l'accès à votre écran et votre webcam.

Après cela, mon logiciel a obtenu tous vos contacts et fichiers.

Vous avez entré vos mots de passes sur les sites que vous avez visités, et je les ai interceptés.

Bien sûr, vous pouvez les modifier, ou alors vous les avez déjà changés.

Mais ça n'a pas d'importance, mon virus l'a mis à jour à chaque fois.

Qu'ai-je fait ?

J'ai créé une vidéo en double écran. La 1ère partie montre la vidéo que vous regardiez (vous avez de bons goûts ahahah...), et la deuxième partie montre votre webcam.

N'essayez pas de trouver et de détruire mon virus ! (Toutes vos données sont déjà téléchargés vers un serveur distant)

– N'essayez pas d'entrer en contact avec moi

– Les antivirus ou services de sécurité;

Formater votre disque ou détruire l'ordinateur ne vous aidera pas non plus, puisque vos données se trouvent déjà sur un serveur distant.

Je vous garantis que je ne vous dérangerai plus après votre paiement, car vous n'êtes pas ma seule victime. C'est le code d'honneur des hackers.

Ne m'en voulez pas, chacun son travail.

Vous voulez savoir ce que vous pouvez faire ?

Eh bien, à mon avis, 520 EURO est un juste prix pour notre petit secret. Vous effectuerez le paiement par Bitcoin (si vous ne connaissez pas, recherchez "comment acheter des Bitcoins" sur Google).

L'adresse de mon portefeuille Bitcoin:

Utiliser internet

Arnaques : le chantage à la webcam



1Jh4QXj2ZAcq2mJ1hjXy6Zkhft2NYmtfck
bitcoin

(respecter les majuscules et minuscules, vous pouvez utiliser **Bitpay.com** pour le paiement par code QR)

Important:

Vous avez 48 heures pour effectuer le paiement. (J'ai un traqueur dans ce mail, et en ce moment je sais que vous avez lu ce message).

Si je n'obtiens pas les Bitcoins, j'enverrai certainement l'enregistrement vidéo à tous vos contacts, y compris vos parents, vos collègues, et ainsi de suite. Cela dit, si je reçois le paiement, je détruirai la vidéo immédiatement.

Si vous avez besoin de preuves, répondez par "oui!" et j'enverrai l'enregistrement vidéo à 6 de vos contacts. C'est une offre non négociable, cela étant dit, ne me faites pas perdre mon temps et le vôtre en répondant à ce message.

Arnaques : le chantage



DIRECTION CENTRALE DE LA POLICE JUDICIAIRE
BRIGADE DE PROTECTION DES MINEURS

CONVOCAZIONE EN JUSTICE

Pour les nécessités d'une enquête judiciaire
(Article 390-1 du Code de procédure pénale)

À votre attention,
À la demande de Madame, **Catherine DE BOLLE** commissaire générale de la police fédérale, élue au poste de directrice d'Europol " Brigade de protection des mineurs (BPM) " nous vous adressons cette convocation.

La **COPJ** ou **convocation** par officier de police judiciaire est prévue par l'article 390-1 du Code de Procédure Pénale. Elle vaut citation devant le Tribunal et est décidée par le Procureur de la République.

En application des dispositions de l'article 372 du code pénal énonce : " Tout attentat à la pudeur commis sans violences ni menaces sur la personne ou à l'aide de la personne d'un enfant de l'un ou de l'autre sexe, âgé de moins de seize ans accomplis, sera puni de la réclusion.
L'article 227-23 du Code pénal dispose : « Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 Euros d'amende.

Nous engageons à votre rencontre, des poursuites judiciaires peu après une saisie informatique de la Cyber-infiltration pour :

- Pédopornographie
- Pédophilie
- Exhibitionnisme
- Cyber pornographie
- Trafic sexuel

Pour votre information, la loi de mars 2007 aggrave les peines lorsque les propositions, les agressions sexuelles ou les viols ont pu être commis en recourant à internet.

Vous avez commis l'infraction après avoir été ciblé sur internet (site d'annonce), visualisation de vidéo à caractère pédopornographique, des photos/vidéos dénudées de mineur ont été enregistrées par notre cyber gendarme et constituent les preuves de vos infractions.

Cette convocation présente un caractère obligatoire. Conformément à l'article 78 du code pénal, l'officier de police judiciaire peut contraindre à comparaître par la force publique, avec l'autorisation préalable du procureur de la République, les personnes qui n'ont pas répondu à une convocation à comparaître ou dont on peut craindre qu'elles ne répondent pas à une telle convocation.

Dans un souci de confidentialité nous vous adressons cet e-mail, vous êtes prié de vous faire entendre par mail en écrivant vos justifications pour qu'elles soient mises en examen et vérifiées afin d'évaluer les sanctions ; cela dans un délai strict de 72 heures. Passé ce délai, nous nous verrons dans l'obligation de transmettre notre rapport à **Mme Myriam Quéméner**, procureur adjoint au tribunal de grande instance de Créteil et spécialiste de cybercriminalité pour établir un mandat d'arrêt à votre rencontre, nous vous adresserons dans ce cas une lettre recommandée avec accusé de réception (arrestation immédiate) par la gendarmerie la plus proche de votre «Lieu de résidence » et vous serez fiché au registre national des délinquants sexuels. Dans ce cas, votre dossier sera également transmis aux associations de lutte contre la pédophilie et aux medias pour publication de personne fiché au **RNDS**.

*En cas de non-respect de la procédure et du délai, la lettre de **convocation** vous sera envoyée par courrier postal.
Cordialement,

Mme Catherine De Bolle, commissaire générale de la police fédérale, élue au poste de directrice d'Europol" la brigade de protection des mineurs (BPM)"

DIRECTION CENTRALE DE LA POLICE JUDICIAIRE
BRIGADE DE PROTECTION DES MINEURS
Adresse : RUE ROYALE 202 À ,1000 Bruxelles, Belgique
24H/24H

DETACHEMENT DU DEPARTEMENT DE LA PREFECTURE DE POLICE DE PARIS (BPM)
36 RUE DU BASTION, 75017 PARIS



Arnaques : le chantage



CONVOCAATION EN JUSTICE

Pour les nécessités d'une enquête judiciaire (Article 390 du Code de procédure pénale)

À votre attention,

À la demande de Madame, **Catherine DE BOLLE** commissaire générale de la police fédérale, élue au poste de Directrice d'Europol " Brigade de protection des mineurs (BPM) " nous vous adressons cette convocation. La **COPJ** ou **convocation** par officier de police judiciaire est prévue par l'article 390-1 du Code de Procédure Pénale. Elle vaut citation devant le Tribunal et est décidée par le Procureur de la République.

En application des dispositions de l'article 372 du code pénal énonce : " Tout attentat à la pudeur commis sans violences ni menaces sur la personne ou à l'aide de la personne d'un enfant de l'un ou de l'autre sexe, âgé de moins de 16 ans accomplis, sera puni de la réclusion. L'article 227-23 du Code pénal dispose : « Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 Euros d'amende. Nous engageons à votre rencontre, des poursuites judiciaires peu après une saisie informatique de la Cyber-infiltration pour :

- **Pédopornographie**
- **Pédophilie**
- **Exhibitionnisme**
- **Cyber pornographie**
- **Trafic sexuel**

Pour votre information, la loi **390-1 du Code de procédure pénale** de mars 2007 aggrave les peines lorsque les propositions, les agressions sexuelles ou les viols ont pu être commis en recourant à internet.

Vous avez commis l'infraction après avoir été ciblé sur internet (site d'annonce), visualisation **de vidéo à caractère pédopornographique, des photos/vidéos dénudées de mineur ont été enregistrées par notre cyber-gendarme et constituent les preuves de vos infractions.**

Dans un souci de confidentialité nous vous adressons cet e-mail, vous êtes prié de vous faire entendre par mail en écrivant vos justifications pour qu'elles soient mises en examen et vérifiées afin d'évaluer les sanctions ; cela dans un délai strict de 72 heures. Passé ce délai, nous nous verrons dans l'obligation de transmettre notre rapport à **Mme Maryvonne CAILLIBOTTE**, Procureur de la République de Versailles pour établir un mandat d'arrêt à votre rencontre et nous procéderons à votre arrestation immédiate par la gendarmerie la plus proche de votre Lieu de résidence et vous serez fiché au registre national des délinquants sexuels. Dans ce cas, votre dossier sera également transmis aux associations de lutte contre la pédophilie et aux médias pour publication de personne fiché au **RNDS**.

Cordialement,

Mr. Christian RODRIGUEZ,
Directeur général de la Gendarmerie Nationale

DIRECTION CENTRALE DE LA GENDARMERIE
BRIGADE DE PROTECTION DES MINEURS
Adresse : 4 rue Claude-Bernard 92130 Issy-les-Moulineaux

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

Réagir aux arnaques
Sites officiels

◆ CNIL

<https://www.cnil.fr/fr/reagir-en-cas-de-chantage-la-webcam>

◆ Ministère de l'intérieur

<https://www.cybermalveillance.gouv.fr/>

<https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action>

◆ Gendarmerie

signal-spam.fr/

Adresse mail compromise ? : haveibeenpwned.com

Utiliser internet

Signal-spam

la gendarmerie a mis en place un système de signalement automatique.

Vous pouvez vous créer un compte sur le site ministériel "signal-spam.fr"

Il existe un plug-in officiel de signalement automatique pour les logiciels mail

Il est disponible sur "signal-spam.fr", c'est un plug-in signé numériquement,

une fois installé, apparait une petite icone qui vous permet de signaler directement

et simplement le mail auprès de l'organisme interministeriel...

Merci Gilles

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
- Vérifiez les liens dans les messages, l'ortographe et le vocabulaire
- paramétrez correctement votre logiciel de courrier électronique (préférences)

Professeur Mo2Pass

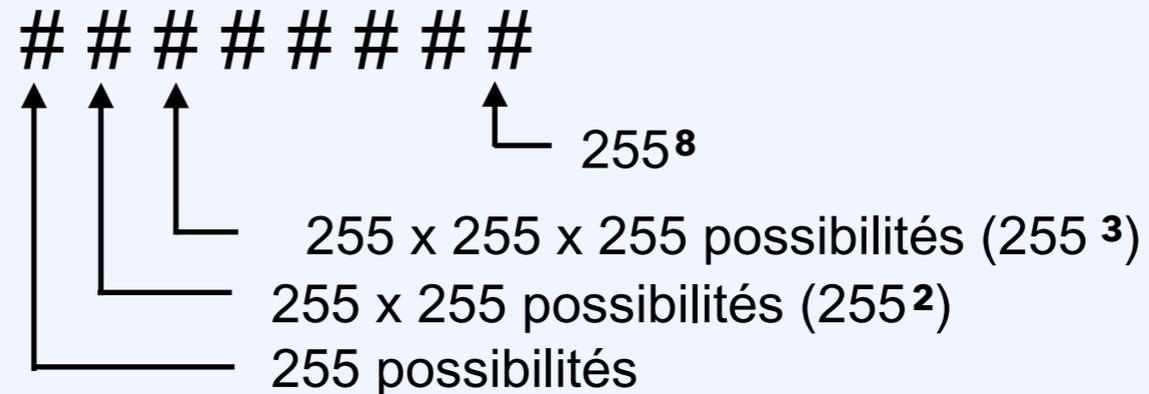
Vous êtes paniqués ?



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

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 (Carnet - Logiciel)
- test : <http://howsecureismypassword.net>

Double authentification

Authentification à deux facteurs

Apple

Google

Linkedin

Tik Tok

Twitter

Facebook

Deux sûretés valent mieux qu'une,
Et le trop en cela ne fut jamais perdu.

La Fontaine : Le loup, la chèvre et le chevreau

les mots de passe

Pour gérer ses mots de passes

Notez les de façon organisée:

- * dans un carnet
- * sur des feuilles
- * dans un logiciel
- * ou vous voulez

Mais

**Débrouillez vous pour vous en rappeler ou pour les
retrouver facilement !**

les mots de passe

Pour gérer ses mots de passes

Quand vous changez un mot de passe

- * Notez le pour vous en rappeler
- * Effacez l'ancien mot de passe pour éviter les erreurs
- * Si besoin, notez la date à laquelle vous l'avez changé

les mots de passe

Ces documents sont des copies au format pdf des exposés du mardi. Vous pouvez les enregistrer sur votre ordinateur en sélectionnant l'option de menu **Fichier** Enregistrer sous... de votre navigateur.

Date	Sujet	fichiers
05/02/2019	Les batteries	3,2 Mo 
09/01/2019	Sauvegarde et Synchronisation des appareils sous ios	2,6 Mo 
07/11/2018	Appareil Photo numerique- iphone	2,5 Mo 
02/10/2018	Sécurité et protection de vos données	1,6 Mo 
12/06/2018	Navigateurs internet	450 ko 
13/03/2018	WeTransfert	1,1 Mo 
13/03/2018	Team Viewer	1,6 Mo 
09/01/2018	Sauvegardes et sécurité	6 Mo 
14/11/2017	Apercu	1,4 Mo 
09/05/2017	iPhone - iPad	4,7 Mo 
14/03/2017	Stratégies de sauvegarde-Malwares	603 ko 
14/03/2017	Modèle liste mots de passe (archive zip)	626 ko 
13/12/2016	Le courrier électronique	6,3 Mo 
07/06/2016	Téléphonie et GPS	204 ko 

les mots de passe

Mots de passe importants

APPLE id pour accéder à iTunes, iCloud, Appstore, Face-time.	APPLE id	votre adresse mail
	Mot de passe	votre mot de passe
Administrateur de votre Ordinateur C'est le nom/mot de passe pour ouvrir votre session administrateur, faire les mises à jour, installer des logiciels.	Utilisateur	
	Mot de passe	
Compte Mail 1 (Orange, free, SFR, Bouygues ...)	adresse email	votre adresse mail
	nom utilisateur	votre nom utilisateur (identifiant)
	mot de passe	le mot de passe associé à cette adresse mail
Compte Mail 2 (Orange, free, SFR, Bouygues ...)	adresse email	votre adresse mail
	nom utilisateur	votre nom utilisateur (identifiant)
	mot de passe	le mot de passe associé à cette adresse mail
Compte Gmail (Chez Google)	adresse Gmail	votre adresse Gmail
	mot de passe	le mot de passe associé à votre adresse gmail
Pour utiliser votre Box en WiFi Le nom et le code sont en général inscrits sur l'étiquette de la Box ou dans votre documentation	Nom de votre box	
	code (WPA ou WEP)	
Site TMC	Utilisateur	tmc
	Mot de passe	1982-2019
Bornes WiFi du local TMC	Nom de la borne	TMC ou TMC NUMERICABLE
	Mot de passe	tmc37tmc37
	Utilisateur	
	Mot de passe	

les mots de passe



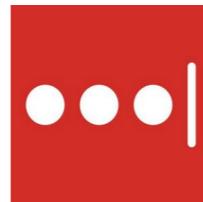
Keychain :
gestionnaire de MDP d'Os X



KeepassX:
Opensource – Multiplateforme



Dashlane:
MDP et portefeuille électronique
Synchro mobiles payante



Lastpass:
logiciel en ligne



1 Password
pratique et complet mais payant (abonnement)

Logiciels gratuits (merci Bruno !)
Secrets – StrongBox – Kaspersky password manager

les mots de passe

Gestion par logiciel :
OnePassword : onpassword.com



Un seul mot de passe pour accéder à tous ses comptes

Versions MacOSX et iOS

Base de données sur iCloud pour partage entre idevices

les mots de passe

The image shows the 1Password application interface. On the left is a sidebar with navigation options: Tous les éléments (123), Favoris (8), Catégories (Identifiants: 67, Notes sécurisées, Cartes de crédit, Identités: 1, Mots de passe: 1, Passeports: 1, Adhésions: 1, Comptes e-mail: 9, Licences du logiciel: 40, Routeurs sans fil: 1, Serveurs: 2), Dossiers (Administrations: 6, Banques: 4), and Audit de sécurité (Watchtower, Mots de passe faibles: 33, Mots de passe en double: 39, 3 ans et +: 36, 1-3 ans: 18, 6-12 mois: 10), and Corbeille (1).

The main area displays a search bar "Chercher dans 1Password" and a list of 67 items. The list is filtered by the letter 'M' and includes entries like MAIF, Maif, mike-b@orange.fr, Nespresso, Nikon Store, Openjabnab, ORANGE, OVH (selected), Paru vendu, PayCar, Paypal, photoservice.com, and Pixmania.

The right pane shows the details for the selected OVH entry. It includes the OVH logo, a star icon, and a share icon. The fields are: nom d'utilisateur (XXXXX-XXX), mot de passe (masked with dots, with a "copier" button), force (indicated by a yellow bar), and site Internet (www.ovh.com). A context menu is open over the password field with options: copier, révéler, and gros caractères. Below the fields are buttons for "Afficher les détails du formulaire Internet" and "Montrer les mots de passe utilisés précédemment". At the bottom, it shows "dernière modifi..." (12 sept. 2018 à 12:19) and "créé" (1 déc. 2015 à 10:48). There is a "+" button at the bottom left and an "Édition" button at the bottom right.

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 sur internet
- Soyez prudents sur les réseaux sociaux