Olivier Bogaert

SURFONS TRANQUILLE 3.0 !

Préface d'Étienne Wery
Illustrations du Clebs

Racine

www.boutique.rtbf.be
www.racine.be
Inscrivez-vous à nos newsletters et recevez régulièrement
des renseignements sur nos parutions et activités.

Tour et Taxis, Entrepôt royal
86C, avenue du Port, BP 104A • B - 1000 Bruxelles

D. 2015, 6852.29
Dépôt légal : octobre 2015
ISBN 978-2-87386-955-7

Imprimé aux Pays-Bas

PRÉFACE

Hollywood a Robocop ; la Belgique a la Computer crime Unit.

Quant à la Computer Crime Unit, elle a un visage : Olivier Bogaert.

La différence est de taille, et de toute évidence, à l'avantage de la Belgique.

Quand Olivier m'a fait l'honneur de me demander cette préface, j'ai sondé quelques personnes, leur demandant de citer les « figures » de la police, ces visages qu'on n'oublie pas. Deux personnes sont sorties du lot : le commandant De Nève, présentateur de la mythique émission *Contacts*, et Olivier Bogaert.

Á la réflexion, ce n'est pas un hasard. Depuis des années, inlassablement, Olivier ne fait rien d'autre que créer le « contact ». Comme son prédécesseur, il est un homme de médias. Comme son prédécesseur - mais dans une autre matière - il contribue chaque jour à donner au difficile métier de policier, un visage humain, didactique, pédagogique.

Dieu sait pourtant que la tâche est difficile.

Difficile de vendre de la procédure pénale ; c'est une matière complexe et absconse. Difficile de donner l'image d'une possible sécurité quand le monde entier nous rappelle qu'il est dangereux de se promener sur les chemins de l'Internet. Difficile de convaincre que la police est souvent là ; les mauvaises nouvelles se vendent mieux.

Aussi difficile qu'elle soit, la tâche ne rebute pas Olivier qui, pour la troisième fois, met à jour un ouvrage fondamental.

Surfons tranquille!

Rien que le titre de l'ouvrage résonne comme une provocation (ce qui n'est pas la moindre de ses qualités, venant d'un représentant de l'ordre).

Provocation en effet qu'évoquer la tranquillité alors que : « Je vous le demande, Madame, dans quel monde vivons-nous ? » ; et que : « De mon temps, Monsieur, on n'avait pas Internet et on n'était pas plus malheureux » ; et aussi : « Si c'est pour regarder ces horreurs, je suis fier de ne pas avoir de connexion ».

Est-il seulement possible d'imaginer surfer tranquille ?

Olivier nous démontre que moyennant quelques précautions, et une bonne dose de bon sens, on peut en tout cas réduire considérablement les risques.

Cette troisième version met à jour l'ouvrage et l'enrichit de conseils pratiques destinés notamment à protéger les citoyens sur les réseaux sociaux.

Olivier réussit le pari de rendre son ouvrage intéressant pour les parents, et pour les jeunes.

Les premiers y trouveront des réflexions, des conseils et des trucs qui ne leur permettront sans doute pas de rattraper leurs enfants sur le plan de la connaissance des réseaux sociaux, mais à tout le moins de les comprendre et de retrouver leur rôle de guide. Les enfants y puiseront des conseils pratiques, notamment sur le réglage de leurs comptes, et ils pourront ainsi – en toute discrétion – minimiser les risques sans avoir à demander conseil.

Bien entendu, on ne surfera jamais totalement tranquille. De la même manière que l'on ne prend pas le volant sans une légère appréhension quant au possible accident.

L'objectif n'est pas le risque zéro. L'objectif est de tendre vers le risque minimal, vers un équilibre entre la nécessité

de prendre en marche le train de la société de l'information, tout en s'assurant de la sécurité du parcours. Le livre d'Olivier Bogaert s'inscrit parfaitement dans cet objectif.

L'avocat que je suis est comme le médecin qu'on consulte lorsqu'on est malade : le mal est fait, le patient vient chercher un remède.

Combien de fois ai-je regretté l'absence de formation des parents, dépassés par cette technologie trop rapide, et l'absence de conscientisation des enfants, naïfs dès qu'il s'agit d'Internet.

C'est là que réside la solution : la prévention, la formation, l'éducation.

Permettre aux parents de comprendre ce qui se passe dans la tête de leurs enfants ; permettre aux enfants de découvrir le monde virtuel en étant conscients des risques, leur apprendre à détecter la mise en danger.

Dans cette perspective, l'ouvrage d'Olivier Bogaert devrait être disponible dans toutes les classes de nos écoles, trôner dans la bibliothèque de chaque parent. Mes enfants diraient : « Tu ne veux pas aussi qu'il soit remboursé par la sécurité sociale ? » Et pourquoi pas ?

Surfons donc, aussi tranquillement que possible, sur les réseaux sociaux !

Étienne Wery
Avocat
Papa de trois surfeurs pas toujours assez tranquilles

LA SÉCURITÉ

LES TRUCS ET ASTUCES POUR BIEN COMMENCER

1

MOT DE PASSE : MOTUS ET BOUCHE COUSUE

Le choix d'un bon mot de passe

Les mots de passe sont les clés de votre maison virtuelle qui peuvent mener jusqu'à la salle des coffres. Mieux vaut donc réfléchir à deux fois avant de les choisir. Voici quelques mauvais exemples et quelques bons conseils.

D'abord un constat : nous sommes encore trop nombreux à choisir la facilité. Plus d'un quart d'entre nous prennent l'option d'un prénom. On opte pour le sien ou celui des enfants. Certains utilisent leur numéro de téléphone ou une combinaison autour de leur date de naissance. Viennent ensuite les simples suites de caractères : azerty, 1234 ou 12345678. Chez les plus jeunes, ce seront les héros du moment ou la star à la mode. Et puis, il y a les réactifs qui préfèrent « jenaimarre », « jemenfiche » ou encore « nimportequoi », et les romantiques qui se protègent avec un « jetaime ». Ces mots de passe sans imagination ni particularité sont évidemment du pain bénit pour les pirates et facilitent l'intrusion dans les ordinateurs ou dans les systèmes plus complexes. En effet, les pirates informatiques se font aider par des logiciels qui s'appuient sur des dictionnaires. Et grâce à ces outils, il leur est facile de tester toutes les possibilités. Il faut donc leur compliquer la tâche.

Alors, quelques conseils… Si vous devez composer un mot de passe, utilisez des lettres en minuscule et en majuscule. Ajoutez-y un chiffre de votre choix et terminez par un

symbole, celui de l'euro par exemple, ou encore un point d'exclamation. Et veillez également à ce que ce mot de passe comporte un minimum de huit caractères.

Vous pouvez aussi choisir une phrase que vous pourrez mémoriser sans difficulté et dont vous prenez la première lettre de chaque mot. Un exemple ? Un extrait d'une fable de La Fontaine : « Maître Corbeau sur un arbre perché tenait en son bec un fromage. » Ceci nous donnera : MCs1aptesb1f ! Autre exemple ? Ma sœur Christine a déjà 53 ans ! Ce qui nous donnera : MsCad53a ! Enfin, dernier conseil : comme dans la vie réelle, ne donnez pas votre identifiant et votre mot de passe au premier site venu ou au premier inconnu qui vous le demande.

Et si vous souhaitez faire un test afin de vérifier la qualité de votre mot de passe, une adresse :
http://pwdtest.bee-secure.lu/

2

LA VALIDATION EN DEUX ÉTAPES

Un deuxième cadenas sur votre compte

Il ne se passe pas un jour sans que l'on entende le témoignage de quelqu'un dont le profil ou la boîte mail a été piraté.

Souvent, ce piratage a été rendu possible parce que l'utilisateur est tombé dans le piège du *phishing* dont nous parlons dans une des rubriques de ce livre.

Ou alors, parce que le pirate a réussi à trouver la réponse à la question secrète et qu'il a lancé le processus « J'ai oublié mon mot de passe ». La réponse, il a pu la trouver dans les très nombreuses informations que nous diffusons notamment sur les réseaux sociaux.

Depuis plusieurs mois, les grands acteurs du Net nous invitent à augmenter le niveau de sécurité en nous proposant notamment d'adopter la validation en deux étapes.

Dans la vie réelle, c'est un peu comme si vous ajoutiez à la serrure fermant la porte de la maison, une lourde barre qui bloquera l'ouverture même si la serrure est fracturée.

Il existe déjà chez plusieurs opérateurs du Net des solutions très fonctionnelles et qui sont très efficaces.

À titre d'exemple, celle de Google et de son service Gmail pour vous en expliquer le principe.

Si vous disposez d'un compte, vous vous y connectez et, sur la page qui s'affiche, vous cliquez sur votre adresse e-mail en haut à droite. La mention « Compte » apparaît que vous cliquez également.

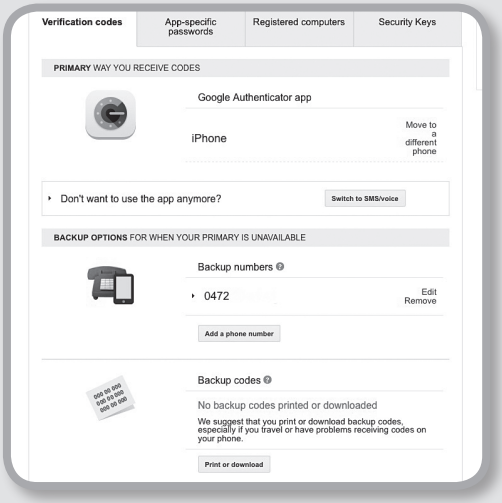
Vous faites alors défiler la liste des réglages possibles et vous vous arrêtez sur «Validation en deux étapes».

Google va soit vous proposer d'utiliser son application Authenticator, soit demander de lui fournir un numéro de GSM sur lequel il pourra vous envoyer un SMS. Quand la solution est activée, à chaque connexion, une fenêtre apparaît après l'introduction de vos identifiant et mot de passe. Et dans le champ qui se présente, vous devez rentrer le code généré par l'application ou celui qui vous a été envoyé par SMS.

Si donc, un pirate a trouvé votre mot de passe, il sera bloqué car il n'aura pas accès au téléphone qui est dans votre sac ou votre poche.

Et pour éviter les soucis en cas de perte de celui-ci, vous pouvez, au moment de la configuration ou même ultérieurement, imprimer ou sauver un document qui contient des codes de secours.

Ce qui vous permettra de toujours garder le contrôle de votre compte.



Chez Yahoo, on envisage d'aller plus loin puisqu'il est question de tout simplement supprimer le mot de passe. Concrètement, cela se ferait via la transmission d'un code simple et éphémère par SMS chaque fois que l'utilisateur souhaitera se connecter à ce service.

3

« LE WI-FI, C'EST GÉNIAL ! »

Bien configurer son réseau sans fil

Une connexion sans fil vers Internet, c'est drôlement pratique : vous pouvez disposer de votre connexion Internet dans les lieux couverts sans devoir vous brancher dans une prise. Le plus souvent, le Wi-Fi est utilisé pour partager la connexion entre les différents ordinateurs de la famille.

Mais il existe de gros risques à utiliser un réseau sans fil mal sécurisé. Le réseau sans fil non sécurisé est ouvert à toute personne se situant dans le voisinage : tout ordinateur pourra s'y connecter et envoyer et recevoir des données pouvant se révéler illégales. Quelle proie facile pour les cybercriminels ! Prenons l'exemple de l'époux qui a découvert la relation extra-conjugale de sa femme. Emportant son ordinateur portable, il se rend en ville et, installé dans sa voiture, recherche un réseau Wi-Fi ouvert et non protégé. Connecté, il peut alors poster des messages insultants, lancer des menaces… Si la victime s'adresse à la police, l'enquête devrait permettre de remonter jusqu'à la connexion à l'origine de ces messages. Évidemment, ce sera le titulaire de l'abonnement, associé à ce réseau sans fil, qui aura à s'expliquer alors qu'il est étranger à toute l'affaire.

Nombreux sont les utilisateurs de Wi-Fi qui pensent que leur connexion est sécurisée mais ils ne savent pas comment. Il règne donc un sentiment de sécurité qui peut se révéler trompeur. Vous devez notamment veiller à utiliser

un protocole de cryptage efficace (idéalement le WPA2, à défaut le WPA). Il permet de rendre vos informations illisibles pendant le trajet les menant d'une machine à une autre ; ainsi personne ne pourra les déchiffrer. De nombreux sites sur Internet vous expliqueront pas à pas comment procéder à une bonne sécurisation de votre réseau. Cherchez « sécuriser » et « wifi » dans votre moteur de recherche favori. Vous aurez l'embarras du choix.

TABLE DES MATIÈRES

Préface d'Étienne Wery 7

LA SÉCURITÉ 11

• **LES TRUCS ET ASTUCES POUR BIEN COMMENCER** 11

Mot de passe : motus et bouche cousue
Le choix d'un bon mot de passe 13
La validation en deux étapes
Un deuxième cadenas sur votre compte 15
« Le Wi-Fi, c'est génial ! »
Bien configurer son réseau sans fil 18
« En vacances avec le Wi-Fi »
Les réseaux Wi-Fi publics 20
Pourquoi un antivirus ?
Infection de votre ordinateur : petit mode d'emploi 22
« Il y a un mouchard dans mon ordinateur »
Les chevaux de Troie 24
Votre ordinateur pris au piège
Connaissez-vous les *botnets* ? 26
Un antivirus ?
Les sites de test 30
Les supports externes
Quelques conseils pour bien les utiliser 32
Le *cloud computing*
Vos données dans les nuages 35
Sur mon smartphone, je vois tout chez moi !
Les objets connectés 37
Les sites web se souviennent de vous
Comment font-ils ? 39

• **VOS DONNÉES PERSONNELLES** 41

Mais comment savent-ils tout ça ?
Les sites web ont un nouvel outil ! 42
Cybercafé : Ne laissez rien traîner derrière vous !
Quelques conseils pour l'utilisation d'un ordinateur public..... 44
La collecte d'informations sur le net
Où vont toutes vos données ?..... 46
Sécurité sur le Net
Des progrès mais… 48
« Les e-mails : à l'abri des regards ? »
La publicité contextuelle à partir du contenu de vos e-mails..... 50
La grande mémoire de Google
Que retient-il de vous ? 52
La grande mémoire de Google
Comment puis-je gérer mes données ? 54
Une nouvelle forme de câblage
Le *graymail* 57
Journées Portes ouvertes
L'intelligence économique 60
« Nous savons que ceci va vous intéresser ! »
Coup de projecteur sur l'ingénierie sociale 62
« Votre compte est bloqué ? Il faut le réactiver en vous connectant à ce site »
Le *phishing* ou « hameçonnage » 64
Attention, vous êtes suivis !
Les virus aiment aussi votre boîte aux lettres 66
« S'il te plait, j'ai besoin de toi ! »
Que faire face aux messages alarmants ?..... 68
Les valises sont bouclées, on peut partir !
Quelques conseils avant les vacances..... 71
« Catastrophe, on m'a volé mon portable ! »
Comment retrouver la trace d'un portable volé ? 73

• **LA JEUNE GÉNÉRATION** 75

Que savez-vous de l'activité de vos enfants sur la Toile ?
Le monde du Net, pourquoi ne pas en parler ? 76
Éduquer les parents ?
Un guide destiné aux adultes 78
Les enfants et les adolescents sur le Net
Quelques conseils 80
Les enfants et les adolescents sur le Net
Et si on se testait ? 82

Le sexe sur le Net : pas que des dangers virtuels
Comment réagir sans dramatiser ? 85
Éduquer un enfant, c'est lui ouvrir un espace de liberté mais aussi le protéger
Les logiciels de contrôle parental 88
Votre image sur le Net
Comment vous préserver des abus ? 90
Facile de se moquer de quelqu'un sur Internet
Calomnie et harcèlement 94
Snapchat
Une application qui favorise les dérives 97
Un clic et c'est payé !
Payer sur le net par Bancontact ou par carte de crédit 99
« Je suis contactable partout ! »
Votre smartphone, la nouvelle cible 102
Sécurité sur smartphone
Des évolutions positives 105
Comment savoir si votre smartphone est infecté ? 107
Sur votre tablette ou smartphone, les droits accordés aux applications 111
Votre smartphone est précieux
Pensez à vous préserver du vol ou de la perte 113
Envie de changer de smartphone ?
Prudence avec vos données 115
Envie de rencontrer l'âme sœur ?
Et pourquoi pas via une application ? 117
Smartphone et voiture
Une source de problème 119
Vous dormez mal ?
Et si c'était votre smartphone ? 121
« La vie privée doit rester un jardin secret »
Éviter de s'exposer sur le Net 123

• **COMMERCE ET PAIEMENTS SUR LE NET** 125

« PayPal, c'est drôlement pratique »
Le paiement par PayPal 126
N'envoyez pas d'argent à un inconnu
Payer avec Western Union 128
« Je me lance sur eBay »
eBay : premiers conseils en cas d'achat et de vente 130
« Mon GSM n'a pas un an et l'écran est en panne »
Les garanties en cas d'achat sur Internet 132

« Je veux acheter sur le Net »
Mais que valent tous ces avis ? 134

• **RÉSEAUX SOCIAUX : PENSEZ AUSSI À VOTRE VIE PRIVÉE !** 137

Il sait tout de vous !
Facebook et vos informations personnelles 138
Vos données personnelles sur Facebook
L'aide au paramétrage 141
Paramétrage de Facebook : bon à savoir ! 143
Graph Search
Le moteur de recherche de Facebook 145
« Qui me suit sur Facebook ? »
La fonction « Abonnement » 147
« Mon passé sur Facebook »
La ligne du temps 149
Facebook et son bouton « J'aime »
oute votre activité sur Internet 151
Facebook me piste ?
Même avec votre smartphone ! 153
« On se fixe rendez-vous par SMS ? »
Facebook les lit ! 155
Un robot comme ami sur Facebook
Prudence avec les demandes ! 158
Ma photo dans une publicité ?
Comment vous protéger de l'utilisation de vos données
sur Facebook ? 160
« Merci pour les infos, on arrive ! »
Les réseaux sociaux, une aubaine pour les cambrioleurs 162
Tu dois réagir. Partages cette info !
Hoax via Facebook 164
La pêche aux infos se diversifie
Le *phishing* sur Facebook 166
C'est pour le boulot, chef !
Les réseaux sociaux au travail 168
Et les réseaux sociaux professionnels ?
LinkedIn, cible des arnaqueurs ! 170
Il n'y a pas que Facebook pour aider les voleurs ! 173
Et si on se passait de Facebook ?
Les réseaux sociaux alternatifs 175

LES ARNAQUES 177

« Mieux vaut prévenir que guérir »
Internet, le miroir aux alouettes ? 178
« Nous vous offrons des ordinateurs ! »
L'imagination des escrocs du Net est débordante 180
« Bienvenue sur notre site ! »
Les faux sites web 183
Vous avez gagné deux places de concert !
Concours par SMS 185
C'est quoi ce message ?
SMS et appels surprises 187
Les escrocs aiment Facebook
Arnaque aux SMS via le réseau social 189
L'Apple Watch à 200 € !
Les fausses bonnes affaires 192
Contrefaçons sur le net ?Un exemple concret 194
« ACHETEZ LE REMÈDE MIRACLE ! » 197
Une carte mémoire pour votre smartphone
Attention à la capacité annoncée ! 199
« J'étais certain d'être connecté à leur site ! »
Le typosquatting 201
Windows 10 est arrivé ! 203
« Super, cet appart ! »
L'arnaque à la location 205
Votre canapé m'intéresse !
Étudiant recherche la bonne affaire 207
Donnez-moi votre adresse mail et je vous paie !
Les escrocs aiment aussi Paypal 209
« J'achète votre vélo et je vous envoie un chèque ! »
Petites annonces : soyez vigilant 212
« Envoyez-moi vos coordonnées et je vous paie »
La communication de données personnelles lors d'une vente sur Internet 214
« À ce prix, cet iPhone est une affaire ! »
En êtes-vous si sûr ? 216
« Mettez à jour vos données sur l'annuaire professionnel du Net »
Le courriel qui vous invite à vous faire connaître 219
Une offre d'emploi prometteuse
Ne devenez pas une « mule » ! 221
Une invitation à une conférence internationale
Votre CV, source d'arnaques ! 224

« Gagnez bien votre vie en devenant délégué commercial de notre société »
Les propositions de ventes pyramidales 226
« Vous avez gagné le gros lot ! Contactez-nous »
Les fausses loteries 228
Tu as vu ce qu'on raconte sur toi ?
Les logiciels voleurs d'infos 230
Et si ce logiciel de sécurité était un virus ?
Les facticiels 232
Vous êtes en infraction !
Le logiciel rançonneur 234
Le logiciel rançonneur
Sur votre smartphone aussi ! 237
Le nouvel iPhone est sorti
Profitez-en pour 1 euro ! 239
1 000 euros d'achats offerts chez IKEA contre quelques informations… Qui pourrait résister ? 241
« Le flirt sur la Toile »
Le chantage à la webcam 243
Une réponse à une question secrète pour retrouver mon mot de passe !
Le vol de mots de passe 245
Les tickets de concert sur le Net 247
« Cherche correspondant en vue de contacts… et plus si affinités »
Les rencontres sur le Net 251
Pourquoi toujours la Côte d'Ivoire ? 254
« Ils trompent les internautes ; autant le savoir »
Comment dénoncer un site malhonnête au niveau international ? 256

LEXIQUE 259

Pour en savoir plus 277