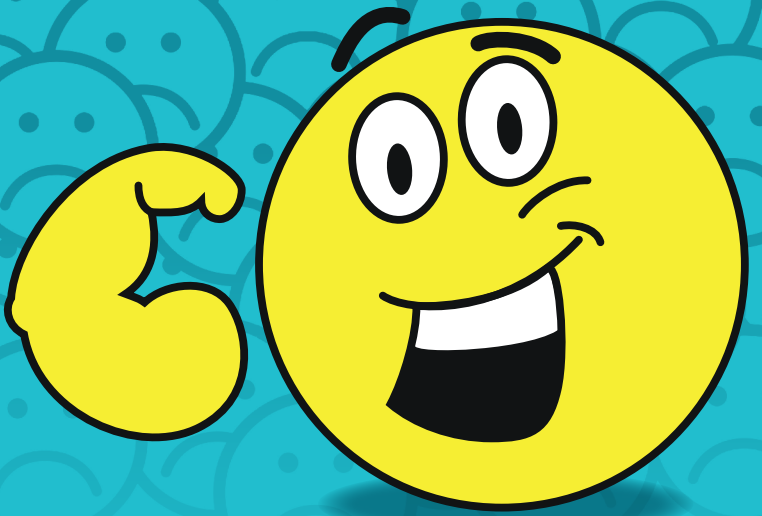


Olivier Bogaert

INTERNET

Évitez les arnaques et le harcèlement

Racine

Olivier Bogaert

INTERNET

Évitez les arnaques et le harcèlement

Racine

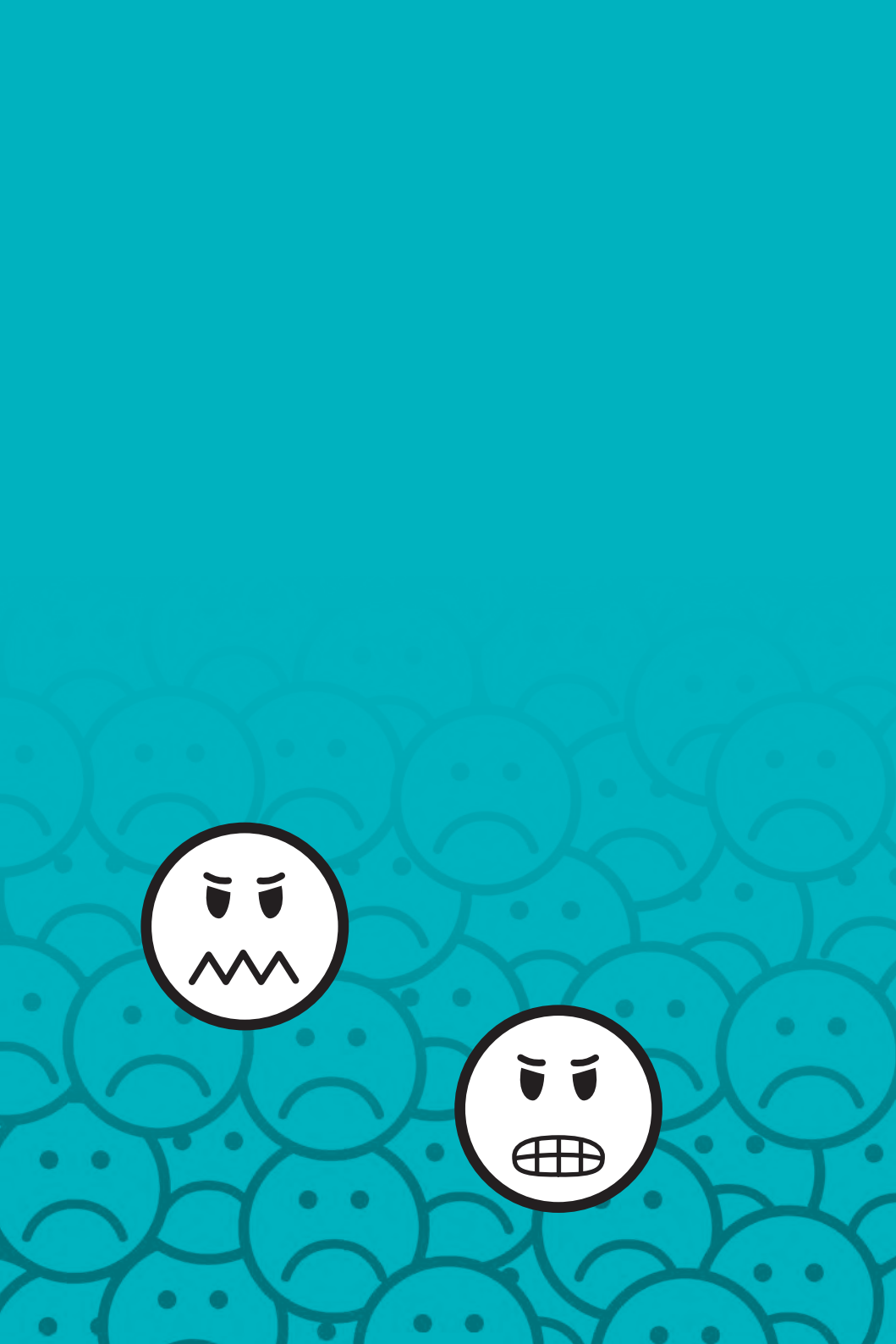
SOMMAIRE

INTRODUCTION

Certains escrocs sont de véritables artistes : ce sont les rois de la manipulation et de l'ingéniosité. Ils font preuve d'une imagination débordante pour inventer des récits émouvants et divers stratagèmes afin d'appâter et de tromper leurs futures victimes.

Internet leur offre la possibilité d'atteindre un grand nombre de victimes potentielles, à court terme et à faible coût. Ils jouent sur le fait que, parmi ce grand nombre, il se trouvera toujours quelques personnes plus crédules ou moins averties que les autres, qui tomberont dans le panneau. Très souvent, ils vont jouer avec la naïveté des victimes, leur goût du profit et leurs actions irréfléchies encouragées par la nature du monde virtuel. En outre, le caractère plus anonyme et virtuel des contacts sur Internet leur permet d'être plus difficilement identifiables et localisables. Ils se croient à l'abri de toute poursuite, surtout lorsqu'ils opèrent à partir de l'étranger.

O. Bogaert



PREMIÈRE PARTIE

LES ARNAQUES LES PLUS COURANTES

1

LES ARNAQUES VIA LA VENTE ET LE PAIEMENT EN LIGNE

Les billets pour des événements, cible des arnaqueurs

Jouant avec la passion des spectateurs et encouragés par la distance qui les sépare de leurs acheteurs potentiels, de nombreux sites peu scrupuleux profitent de l'aubaine pour tromper les amateurs.

Ces sites, moyennant paiement, parviennent à se faire référencer de manière prioritaire par les moteurs de recherche. Ils apparaissent en tête des résultats quand vous vous documentez au sujet de l'événement qui vous intéresse.

- N'achetez vos billets que par le biais du site officiel de l'artiste ou de l'organisateur. Si vous avez un doute, visitez le site de la salle dans laquelle se déroulera le concert.
- Lisez soigneusement les conditions de vente et soyez attentif à ce que le vendeur vous offre suffisamment de garanties.
- Vérifiez les informations de contact du revendeur de billets. Si vous ne trouvez pas ces informations ou si elles sont incomplètes, méfiez-vous.

Réserver ses vacances

Nous sommes nombreux à chercher la bonne affaire dans la région ou dans le pays de nos rêves. Les arnaqueurs en profitent. Au printemps, lorsque nous commençons à faire des recherches, 10 % des spams en circulation ont pour thème nos futures vacances.

Parmi ces e-mails frauduleux, ce sont les fausses confirmations de vol qui sont les plus répandues.

Ces messages sont accompagnés d'une pièce jointe ou comportent un lien vers une page web contrefaite qui permet l'installation d'un logiciel malveillant sur l'ordinateur du destinataire.

Parfois, vous recevez une fausse lettre d'information présentant de bonnes affaires si vous réservez un séjour de luxe. Les croisières, les offres d'assurance de voyage et les prêts vacances sont également utilisés pour vous séduire alors que vous êtes en pleine préparation de cette escapade estivale. Et, bien sûr, pour en profiter, obligation de fournir des données personnelles précises... Méfiance !

- Renseignez-vous au sujet du site que vous utilisez avant de réserver un vol ou un hôtel.
- Consultez les opinions des autres utilisateurs sur les sites de vente de billets/de réservation. Lisez leurs commentaires et leurs avis au sujet des services.
- Essayez d'entrer en contact avec un représentant de l'entreprise afin d'obtenir un maximum d'informations sur le lieu de vacances.
- Ne cliquez pas sur les liens contenus dans les e-mails, surtout si vous n'avez pas demandé de renseignements sur des offres de voyage ou réalisé de réservation, et n'ouvrez jamais les fichiers joints à ce type de message.

Les arnaques via les cartes Apple

Si ce mode de paiement vous est proposé alors que vous souhaitez acheter quelque chose sur un site de petites annonces, gardez à l'esprit que vous êtes très probablement la cible d'une escroquerie.

La technique qui consiste à vous contacter par téléphone est souvent utilisée. Votre interlocuteur se présente comme un membre d'une administration publique, de votre banque ou encore comme un opérateur. Au cours de l'entretien, il explique que pour simplifier le paiement qui vous est demandé, il est possible de l'effectuer en utilisant une carte prépayée. Jouant sur votre inquiétude, il vous propose de réaliser ce paiement en achetant une carte cadeau App Store, iTunes ou Apple Store. Une fois la carte achetée, il vous demande d'effectuer le paiement requis en lui communiquant le code indiqué au dos de la carte.

- Ne communiquez jamais le numéro situé au dos de la carte à une personne que vous ne connaissez pas. Une fois que l'escroc aura pris connaissance de ce numéro, la somme associée à la carte sera très probablement dépensée avant que vous n'ayez eu le temps de contacter Apple ou les autorités.
- Les cartes cadeaux App Store ou iTunes ne peuvent être utilisées que lorsqu'elles sont associées à leurs services. Si vous achetez une carte cadeau, elle ne pourra être utilisée que sur l'App Store, sur iTunes ou dans un magasin Apple.

 # Apple nous met régulièrement en garde parce que l'entreprise a constaté que des arnaqueurs utilisaient ses modes de paiement pour nous piéger.

Un chèque qui contient trop d'argent… ?

C'est devenu une habitude pour beaucoup d'entre nous : on revend le cadeau reçu dans un magasin de seconde main ou sur Internet…
Si vous êtes contacté par une personne se disant à l'étranger, restez vigilant.

« L'arnaqueur va vous expliquer qu'il n'habite pas en Belgique ni en France et vous demander si vous acceptez un paiement par chèque. Vous acceptez et vous lui communiquez vos coordonnées. Trois jours plus tard, vous recevez un chèque par la poste. Surprise ! Le chèque est d'un montant plus élevé que le prix demandé pour l'objet. L'acheteur vous explique que c'est un chèque qu'il a lui-même reçu pour paiement lors d'une vente et que, s'agissant d'un chèque au porteur, il veut l'utiliser pour vous payer. Il vous demande juste de lui renvoyer la différence via une carte de crédit prépayée que vous obtiendrez, par exemple à la poste en lui envoyant le colis. Vous déposez le chèque à la banque et constatez que le montant est crédité sur votre compte. »

Mais vous n'avez pas remarqué la mention « sauf bonne fin ». Cela signifie que votre banque vous « avance » le montant du chèque dans l'attente de son paiement par la banque émettrice. Comme vous avez reçu l'argent, vous envoyez l'objet et la carte prépayée. Deux ou trois jours plus tard, en consultant votre solde, vous constatez que le montant a été retiré. Votre banque vous explique qu'il s'agissait en réalité d'un chèque volé et qu'il y avait opposition sur son montant.

« Vous vendez un canapé et vous êtes contacté par quelqu'un qui se dit très intéressé. Il est étudiant, en colocation, et vous demande de le lui réserver, précisant qu'il va s'organiser pour que ses parents viennent le chercher. Pour achever de vous convaincre de sa bonne foi, il vous propose le paiement des deux tiers du montant et vous demande votre numéro de compte. Vous êtes en confiance. Effectivement, deux jours plus tard, votre compte bancaire est crédité d'une somme bien supérieure à celle que vous aviez indiquée. L'étudiant vous contacte alors et vous explique que la comptable de l'entreprise, dans laquelle il est en stage, lui a rendu le service d'effectuer le versement mais qu'elle a commis une erreur. Il vous demande de bien vouloir renvoyer la somme via un numéro de compte qu'il vous communique. Il insiste : « Vite, s'il vous plaît, sinon, elle va avoir des ennuis. » Compréhensif, vous faites ce versement. Sauf que quelques jours plus tard, le reste de la somme disparaît également. »

Votre banque vous informe que le montant versé initialement provient d'un chèque anglais frappé d'opposition, car volé.

Si, après avoir placé une annonce ou encore parce que vous êtes commerçant, vous êtes contacté par une personne se disant à l'étranger, n'hésitez pas à contacter votre banquier pour qu'il vous conseille.

Une enquête française nous apprend que 57 % des personnes interrogées ont déjà revendu ou sont prêtes à revendre un cadeau reçu à Noël et que cette proportion est de 73 % dans la catégorie des 25-34 ans.

Comment bien utiliser PayPal ?

Nous sommes nombreux à utiliser les services de PayPal et les escrocs profitent du déficit d'informations de certains utilisateurs pour les tromper.

Son principe de fonctionnement est très simple. Lors de la création de votre compte, vous fournissez vos coordonnées et vous choisissez une adresse e-mail qui deviendra votre identifiant unique. Le service est gratuit si vous l'utilisez pour payer un achat.

Il est payant, via le prélèvement d'un petit pourcentage, si vous êtes le vendeur. Dans ce cas, soit PayPal vous fait parvenir une facture que vous payez via votre compte bancaire, soit la société prélève cette commission sur la carte de crédit dont vous avez communiqué les coordonnées lors de votre inscription.

> « Vous avez décidé de vendre des objets dont vous n'avez plus l'usage et vous utilisez un site d'enchères. L'enchère terminée, votre acheteur vous contacte et vous demande s'il peut régler le montant final via PayPal. Pas de souci.
> Mais c'est là que l'imagination des escrocs peut vous jouer des tours. Petite illustration d'une situation. Jean a vendu son objet 100 € et voit son compte crédité de 1000 €. Son acheteur le contacte en s'excusant : il a fait une erreur de manipulation et il lui demande le remboursement des 900 € qu'il a versés par erreur, sur un compte dont il donne les coordonnées. Confiant et pensant lui rendre service, Jean s'exécute et verse les 900 €. »

Mais… Il aurait dû vérifier qu'il s'agissait bien d'une procédure PayPal, ce qui n'est pas le cas. Dans le cas d'une vente via ce service, le remboursement se fait par un simple renvoi de la somme vers le compte PayPal de l'acheteur. Dans notre histoire, l'acheteur n'était pas le titulaire du compte PayPal mais bien un escroc qui en utilisait les coordonnées sans doute obtenues par phishing. Jean est doublement victime : à la somme qu'il a envoyée, s'ajoute celle que lui réclame désormais le légitime titulaire du compte qui a été utilisé.

« AUTRE EXEMPLE : vous revendez un objet sur un site de petites annonces et une personne intéressée vous demande si vous êtes d'accord de recevoir un paiement via PayPal. Vous acceptez et vous recevez alors un e-mail de PayPal qui vous confirme que le paiement a bien été effectué et que vous pouvez envoyer l'objet. Sauf que cet e-mail est un faux qui reprend avec exactitude la forme et le contenu de ceux de PayPal. Vous n'êtes donc pas surpris, vous préparez votre colis et vous l'envoyez. Mais en consultant votre compte PayPal, vous ne trouvez pas la somme annoncée. »

Pour vous prémunir contre cette technique, vous devez

- Vérifier l'adresse de l'expéditeur. Si cette adresse ne contient pas la mention « @paypal.be » ou « @paypal.fr », il s'agit très certainement d'un e-mail frauduleux.
- Vous connecter à votre compte PayPal. Si votre compte n'a pas été crédité par celui qui se dit intéressé par l'objet que vous proposez, ne donnez évidemment aucune suite.

Quelques autres conseils pour vous éviter les mauvaises surprises

- Préférez toujours les sites de votre pays. En cas de problème avec votre acheteur, vous disposerez de davantage de ressources d'un point de vue juridique.
- Restez attentif aux frais à couvrir. Il n'est pas normal que vous, le vendeur, deviez envoyer de l'argent.
- Si un e-mail vous paraît suspect, testez l'adresse sur votre moteur de recherche. Des sites spécialisés dans la prévention des arnaques, comme Signal Arnaques, mettent en évidence les adresses qui ont déjà servi à abuser d'autres vendeurs.
- Et puis, finalement, rien ne vaut un rendez-vous avec l'acheteur dans un lieu public. C'est la solution la plus facile : vous lui remettez l'objet et il vous paye.
- Et s'il ne vit pas dans votre région, le bon vieux virement bancaire, l'envoi par la poste contre remboursement ou un autre service avec un numéro de suivi.

Évitez de réaliser des achats en ligne ou de consulter des comptes bancaires lorsque vous utilisez des hotspots wifi tels que ceux des aéroports, des cafés, des centres commerciaux ou des hôtels.

TABLE DES MATIÈRES

DEUXIÈME PARTIE

LES ARNAQUES QUI TOUCHENT LES JEUNES 103

TROISIÈME PARTIE

LES SITES QUI PEUVENT VOUS AIDER 125

QUATRIÈME PARTIE

LE LEXIQUE 132

INTERNET

Évitez les arnaques et le harcèlement

- Pourquoi des offres personnalisées s'affichent-elles sur votre profil ?
- Comment a-t-on découvert votre numéro de téléphone ?
- Comment éviter la sextortion ?
- Et si vous deveniez une mule sans le savoir ?
- Vous recevez un mail d'un ami qui demande de l'aide ?
- Vous voulez éviter les logiciels malveillants sur Play Store ?
- Votre adresse mail est piratée, mais comment ont-ils trouvé le mot de passe ?

Olivier Bogaert dresse l'inventaire complet et actualisé de ces arnaques dont nous sommes la cible potentielle. Il nous livre une foule d'infos claires et précises pour nous en protéger et sécuriser notre environnement numérique. Que ce soit sur ordinateur, smartphone ou tablette.
L'auteur aborde également le cyberharcèlement, le revenge porn…
L'ouvrage se découpe en 4 parties :

1. les arnaques les plus courantes (achats en ligne, réservations de vacances, faux sites internet, arnaques QRcode, via Facebook, offres d'emploi… et bien d'autres.)
2. les arnaques qui touchent les jeunes (TikTok, Snapchat, WhatsApp, harcèlement sur les réseaux sociaux…)
3. les sites qui peuvent vous aider
4. le lexique

INFORMATIONS VALABLES POUR LA BELGIQUE ET LA FRANCE

Olivier Bogaert
Commissaire à la Police judiciaire fédérale belge, Olivier Bogaert travaille au sein de l'unité en charge de la cybercriminalité. Véritable expert, il est très actif dans les médias et sur les réseaux sociaux afin de nous sensibiliser à la cybersécurité.

Racine
www.racine.be

9 782390 251354