GUIDE DES MESURES DE SÉCURISATION DES USAGES MONÉTIQUES

مصرف المغرب
CRÉDIT DU MAROC
Toute une banque pour vous

SOMMAIRE

PAIEMENTS SUR INTERNET

CE QU'IL FAUT SAVOIR AVANT D'EFFECTUER VOS ACHATS SUR INTERNET, ET COMMENT RECONNAÎTRE UN SITE D'ACHAT EN LIGNE SÉCURISÉ.

LES INFORMATIONS NORMALEMENT DEMANDÉES

Lorsque vous effectuez un paiement sur Internet, le site marchand (ou celui de la banque du commerçant) peut légitimement vous demander :

- **Le n° de votre carte bancaire :** 16 chiffres répartis en 4 blocs de 4 chiffres, présents en relief sur la face avant de votre carte,
- **La date de validité :** en relief sur la face avant de votre carte, après la mention « EXPIRE FIN »,
- **Le cryptogramme :** 3 derniers chiffres imprimés au dos de votre carte à droite de la zone de signature,
- **Le nom et éventuellement le prénom :** en relief sur la face avant de votre carte.

Le code secret à 4 chiffres (PIN), utilisé pour les retraits sur GAB ou pour les paiement TPE, est **absolument inutile pour un paiement sur Internet**. Ne le communiquer **jamais** sur un site Internet. Il n'est généralement demandé que sur des sites frauduleux.

Certains sites enregistrent vos informations Carte Bancaire lors de votre premier paiement. Aux paiements suivants, votre n° de carte devra apparaître partiellement masqué. Le cryptogramme ne doit jamais être enregistré. Il faut éviter les paiements sur les sites qui le font.

Enfin, assurez-vous que les échanges sont bien sécurisés avec le site, sur lequel vous donnez vos identifiants confidentiels. L'adresse doit comporter un « s » après http (https://adresse du site accompagné d'un petit cadenas sur votre navigateur).

Dans la mesure du possible, conservez une copie du justificatif de paiement (indiquant le numéro de commande, les coordonnées du marchand et le montant de la transaction). Il pourrait vous être utile en cas de réclamation ou de litige.

L'AUTHENTIFICATION FORTE COMPLÉMENTAIRE

Pour lutter contre l'utilisation des numéros de cartes volées (en phishing par exemple), certains sites commerçants demandent à la banque du client de vérifier que la personne qui effectue le paiement est bien le propriétaire de la carte.

Dans ce cas, lors de l'opération de paiement sur le site marchand (ou sur le site de la banque du commerçant), un code secret complémentaire peut vous être demandé. Il peut vous être envoyé par sms, par mail ou par téléphone. Le code sms étant le plus souvent utilisé.

Le dispositif adopté par le Crédit du Maroc est le dispositif 3D Secure, mis en place pour les cartes Visa et Mastercard. Les noms de marque sont « Verified by Visa » et « Mastercard Secure Code ».

ATTENTION

Tous vos paiements par carte sur Internet ne sont pas concernés par ce système, car certains sites marchands, y compris de grands acteurs, n'ont pas ce dispositif de protection pour le client.

CE QU'IL NE FAUT PAS FAIRE

Communiquer les informations de votre carte bancaire ou code de sécurité complémentaire, si vous n'êtes pas l'initiateur d'un achat en ligne ou d'une opération sur votre banque en ligne.

Cela peut être une tentative de phishing ou autre fraude, pour vous voler ces informations, et les utiliser à votre insu.

N'ENTREZ PAS DANS N'IMPORTE QUELLE E-BOUTIQUE !

Avant d'effectuer un achat sur un site marchand, assurez-vous de sa notoriété. Des sociétés spécialisées collectent les avis des internautes qui ont choisis ces sites marchands et les notent sur plusieurs critères.

Un logo et parfois une note sont présents sur le site marchand :

FIA-NET.com LA GARANTIE SÉRÉNITÉ DE L'ACHAT kelkoo LeGuide.com

Cliquez sur ce logo pour en savoir plus sur la notoriété du site marchand.

Si vous n'avez jamais entendu parler de cette boutique en ligne, posez-vous quelques questions ou effectuez quelques contrôles :

- Les informations sur l'entreprise sont-elles claires et complètes ?
- Puis-je les contacter par téléphone ? Par e-mail ?
- Quelles sont les garanties de livraison et de retour ?
- Consultez les conditions générales de vente.
- Essayez de trouver des avis d'internautes via un moteur de recherche.
- Ma vie privée est-elle protégée ? (Mes données personnelles sont-elles protégées ? Puis-je y accéder ou demander leur suppression ?)

QUAND SERAI-JE DÉBITÉ POUR MON ACHAT ?

Il n'existe aucune règle en la matière. En revanche, les Conditions Générales de Vente sur le site marchand doivent décrire précisément les modalités applicables sur le site :

- carte bancaire débitée dès la commande
- carte bancaire débitée à l'expédition
- Débits partiels en cas de livraison partielle.

Il est également possible de n'être débité qu'après réception et vérification des produits achetés.

Ce sont des solutions de paiements complémentaires proposées sur certains sites marchands et qui sont utilisables avec toutes les cartes bancaires

VOTRE PAIEMENT EST REFUSÉ

Après avoir bien vérifié les informations fournies (N° de Carte, date de validité, nom et cryptogramme), votre paiement est refusé.

Les causes possibles :

- Votre carte est périmée.
- Vous avez atteint le plafond hebdomadaire ou mensuel de paiement (Vous pouvez consulter ce plafond et votre encours sur le site de la banque en ligne du Crédit du Maroc)
- Vous n'avez pas saisi le bon code sécurité reçu par SMS
- Votre carte a été mise en opposition par le Crédit Du Maroc.

LE PHISHING

LE TERME

Issu de l'anglais **« password harvesting fishing »**, signifiant « pêche aux mots de passe ». Traduction française officielle « Filoutage ».

LA TECHNIQUE

Consiste à abuser de la crédulité de l'internaute.

Celui-ci reçoit un courriel reprenant la charte graphique d'une société ou d'une administration connue (banque, opérateur téléphonique, PayPal, Impôts, CNSS…).

L'objectif est d'attirer l'internaute vers un site Internet en utilisant toutes sortes de raisons auxquelles il est particulièrement sensible (sécurité, utilisation frauduleuse, remboursement…).

En cliquant sur le lien proposé dans le courriel, l'internaute se trouve connecté sur un site à la même signalétique. Il y est invité à fournir des informations confidentielles (codes d'accès, n° de carte bancaire…) sans se rendre compte de la fraude.

Les pirates récupèrent ainsi facilement ces codes afin d'effectuer des opérations à leur propre profit.

LES BONS RÉFLEXES

Méfiez-vous des demandes (trop) urgentes d'informations personnelles, faites par courriel, appels téléphoniques, messages vocaux ou SMS.

Méfiez-vous des courriels et des sites Internet contenant des fautes d'orthographe grossières, des fautes de grammaire, des tournures de phrase inhabituelles, des caractères issus d'alphabets étrangers…

Ne vous fiez pas à l'adresse de l'émetteur d'un message (De :), il est facile d'y mettre ce que l'on veut.

Ne vous fiez pas aux informations personnelles contenues dans le courriel. Elles ne cherchent qu'à le crédibiliser Évitez de suivre les liens dans les courriels. Préférez, quand c'est possible, une saisie de l'adresse du site dans votre navigateur ou utilisez un « favori ».

Utilisez les fonctions anti-phishing des navigateurs et des anti-virus récents. Vérifiez régulièrement les opérations effectuées sur vos comptes et votre carte bancaire.

QUE FAIRE SI...

Si vous avez le moindre doute, si vous avez cliqué sur le lien et surtout si vous avez fourni des informations confidentielles, contactez rapidement votre agence.

Si vous en avez la possibilité, transférez le mail reçu à l'adresse qui vous sera donnée par votre conseiller, puis détruisez-le.

Si vous avez communiqué vos identifiants et mots de passe d'accès à la banque en ligne, contactez votre agence et modifiez immédiatement votre mot de passe.

Si vous avez communiqué vos informations de cartes bancaires (numéro de carte, code pin, date d'expiration, cryptogramme ou code à 3 chiffres), faites opposition sur votre carte bancaire le plus rapidement possible.

BON À SAVOIR

Le Crédit du Maroc n'utilise jamais la messagerie électronique pour demander à ses clients des informations confidentielles.

Certains courriels d'hameçonnage, au visuel d'organisations non-bancaires (opérateurs téléphoniques,…), ont pour unique finalité de vous dérober vos secrets bancaires (particulièrement ceux des cartes bancaires).

AUTRES FORMES

Le phishing par téléphone (Vishing) : le pirate vous appelle ou fait en sorte que vous l'appeliez.

Pour cela, il utilise toutes sortes de raisons auxquelles vous serez particulièrement sensible (sécurité, utilisation frauduleuse, remboursement…).

Il va tenter d'obtenir vos informations confidentielles, en utilisant un argumentaire particulièrement efficace ou via un serveur vocal.

Le phishing par SMS (Smishing) : L'accroche se fait par SMS, vous incitant à vous connecter sur un site Internet, appeler un n° de téléphone, ou envoyer un SMS.

LE SPAM

LE TERME

Le « Spam » est un courriel non sollicité (voir indésirable), envoyé en grande quantité, le plus souvent à des fins publicitaires.

Traduction française officielle « pourriel ».

LA TECHNIQUE

Le pourriel est un courriel support :

- Le plus souvent d'une publicité cherchant à vous faire acheter un produit ou un service. Les plus courants visent les produits pharmaceutiques et les produits de luxe, parfois contrefaits.
- D'un canular (hoax en anglais) : fausses informations dont les finalités sont diverses.
- D'une escroquerie.
- D'un logiciel malveillant qui va être installé sur votre ordinateur en ouvrant la pièce jointe, en visualisant les images contenues dans le courriel ou en vous connectant sur un site mis en avant dans le mail.
- D'une campagne de phishing.

La plupart des « spams » sont émis depuis des réseaux d'ordinateurs infectés (« botnet de zombies » voir logiciels malveillants). Cette technique permet de ne pas pouvoir facilement remonter à la source de la malveillance.

Le carnet d'adresses du poste infecté est parfois utilisé pour crédibiliser les pourriels.

LES BONS RÉFLEXES

Si vous utilisez des logiciels de messagerie sur votre ordinateur (Outlook, Thunderbird…) équipez-vous d'un logiciel anti-spam, très souvent inclus dans les logiciels anti-virus.

Si vous utilisez le site de courriels de votre opérateur Internet («webmail»), assurez-vous que l'option anti-spam est activée.

Lorsque cela est possible, désactiver l'affichage systématique des images contenues dans les courriels.

QUE FAIRE SI...

Vous recevez un courriel vous proposant des produits à un prix extrêmement attractif : Résistez à la tentation et détruisez le courriel.

- Pour les produits pharmaceutiques, ils peuvent se révéler dangereux pour la santé.
- Pour les produits de luxe vendus parfois 20 fois moins cher que le produit original, il s'agit généralement de contrefaçons .

Vous recevez un courriel vous informant d'une nouvelle catastrophique ou révoltante. Vérifiez avant tout s'il s'agit d'un canular sur les sites spécialisés comme www.hoaxbuster.com

BON À SAVOIR

De nombreux pirates commercialisent sur Internet, pour une poignée d'argents, des listes importantes d'adresses, récupérées par divers moyens illégaux (intrusions sur des sites commerciaux, logiciels malveillants…). Les tarifs évoluent en fonction de la qualification des adresses, à savoir si elles existent bien, sont actives et ciblent une catégorie socioprofessionnelle particulière. Enfin, certaines listes sont créées sur la base de listes ne contenant que nom et prénom. Les combinaisons nom.prénom, prénom.nom etc. sont essayées chez la plupart des grands opérateurs marocains (Orange, Maroc Telecom…). Il y a un fort déchet, mais au fil du temps et des avis de non-remise, ces listes se fiabilisent et prennent de la valeur.

Un lien dans le courriel vous propose de ne plus recevoir de courriel de cet émetteur. S'il provient d'un site légitime et que vous ne souhaitez plus recevoir d'information de sa part, vous pouvez cliquer sur le lien pour vous désinscrire.

S'il ne provient pas d'un site légitime :

- Ignorez le message et ne cliquez pas sur le lien !
- En effet, par cette action, vous allez confirmer à l'émetteur que votre adresse est correcte. Celle-ci sera vendue beaucoup plus cher sur Internet car elle est qualifiée.
- Pour les mêmes raisons, interdisez l'envoi d'accusé de réception pour ces courriels.

AUTRES FORMES

Toutes ces malveillances peuvent également être véhiculées par SMS.

LES MALWARES

LE TERME

« Malware » est issu de l'anglais « malicious software », c'est-à-dire « logiciel malicieux ».

Le terme « virus » est souvent employé abusivement, car les virus ont été historiquement les premiers logiciels malveillants. Un logiciel « anti-virus » cible tout « logiciel malveillant ».

LA TECHNIQUE

C'est un logiciel qui a été installé à votre insu sur votre ordinateur.

Les moyens d'infection sont nombreux :

- Connexion à Internet avec un ordinateur ayant des failles de sécurité exploitables,
- Exécution d'un programme infecté,
- Ouverture d'une pièce jointe ou d'un document infecté,
- Navigation sur des sites douteux,
- Clic sur des bannières publicitaires infectées,
- Connexion de périphériques infectés (clef usb, disque dur amovible...).

Son fonctionnement est totalement invisible, il dépend du logiciel malveillant et parfois du site Internet sur lequel l'internaute désire se connecter.

Les objectifs des escrocs qui les exploitent sont divers :

- Vendre un produit et enregistrer votre navigation sur Internet pour mieux cibler vos habitudes
- Voler vos informations confidentielles pour les réutiliser à leur profit (Carte Bancaire, codes d'accès Facebook…)
- Voler vos documents (photos, documents d'entreprise…)
- Faire du chantage : bloquer votre ordinateur et demander une somme d'argent (virement, achat forcé…) pour le débloquer
- Utiliser votre ordinateur pour déclencher des attaques : paralysie d'un serveur spécialement ciblé (déni de service) ou générateur de courriels massifs

Votre ordinateur infecté est appelé « zombie », intégré à un réseau (« botnet » ou réseau de robots) de plusieurs milliers d'autres ordinateurs infectés.

Les logiciels malveillants se mettent à jour automatiquement en contactant par Internet leur centre de contrôle. La version téléchargée leur apporte de nouvelles fonctionnalités et une nouvelle signature, les rendant indétectables pour quelque temps.

LES BONS RÉFLEXES

Équipez-vous d'un anti-virus et d'un pare-feu (firewall). Il en existe de nombreux sur le marché, parfois gratuits ou déjà installés sur votre ordinateur (firewall Microsoft Windows par exemple).

Maintenez à jour l'antivirus et l'anti-spyware, et effectuez un scan régulièrement. Au moins une fois par semaine.

Effectuez régulièrement les mises à jour de votre système pour corriger les failles de sécurité.

Vérifiez régulièrement les opérations effectuées sur vos comptes et votre carte bancaire.

Attention aux mails d'origine inconnue avec une pièce jointe.

Attention aux sites douteux, sites à caractère pornographique, sites de téléchargement illégal …

QUE FAIRE SI...

Si vous détectez des opérations frauduleuses sur vos comptes ou vos cartes bancaires :

- Contactez rapidement votre agence par courriel ou par téléphone. Un conseiller vous contactera en retour pour vous guider.
- Le cas échéant, votre conseiller fera le nécessaire pour renouveler votre carte bancaire.

Vérifiez que votre anti-virus et votre anti-spyware sont opérationnels et à jour. Si un logiciel malveillant (virus, backdoor, logiciel espion…) est détecté, faites-le éradiquer par votre anti-virus ou votre anti-spyware, puis seulement après, modifiez les codes secrets d'accès à tous les services Internet protégés par ce type de contrôle d'accès.

Si aucun malware n'a été détecté, ou si vous voulez effectuer un deuxième contrôle, vous pouvez exécuter un 'scan en ligne' depuis Internet, en utilisant les solutions offertes par les grands éditeurs d'anti-virus.

BON À SAVOIR

On me dit que j'envoie des virus.

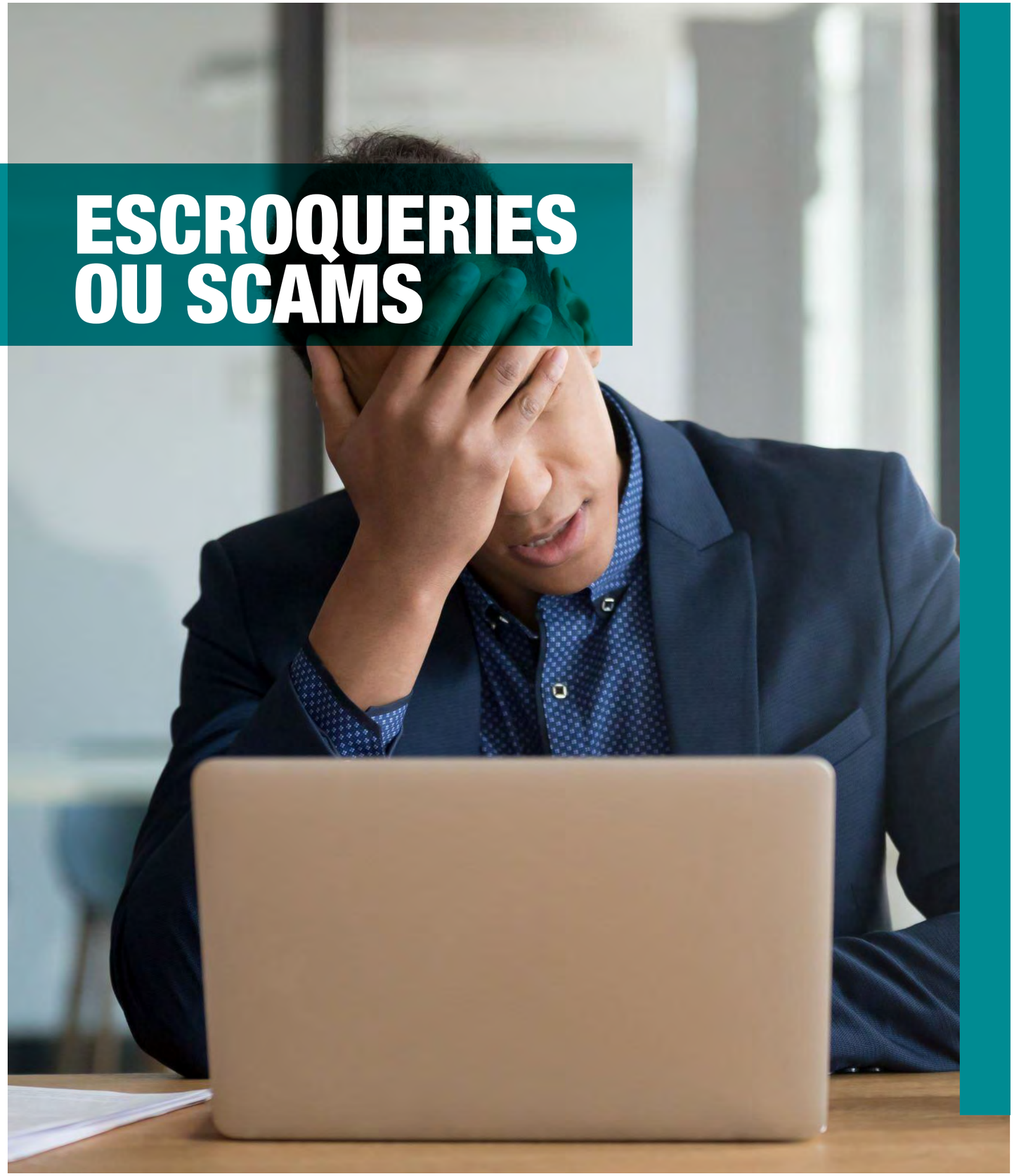
- Vous êtes infecté par un logiciel malveillant qui exploite votre carnet d'adresse pour générer des courriels en masse ou pour se propager et infecter d'autres ordinateurs.
- Vérifiez que votre anti-virus et votre anti-spyware sont opérationnels et à jour.
- Effectuez un scan sur votre ordinateur.
- Si un logiciel malveillant est détecté, faites-le éradiquer par votre anti-virus ou votre anti-spyware.

AUTRES FORMES

Selon leur mode opératoire, les logiciels malveillants peuvent également être nommés :

- **« Spyware »** ou **« espiogiciel »** ou **« logiciel espion »** : les logiciels malveillants chargés de dérober par espionnage (Spy signifie espion) tous les échanges entre l'ordinateur de l'internaute et les sites sur lesquels il navigue.
- **« Keylogger »** ou **« Enregistreur de frappe »** : spyware qui enregistre toutes les frappes au clavier.
- **« Form-grabber »** : spyware qui enregistre les informations que vous saisissez dans les formulaires.
- **« Cheval de Troie »** ou **« troyen »** ou **« trojan »** ou **« trojan horse »** : autres noms génériques pour désigner les logiciels malveillants qui s'installent à votre insu sur votre ordinateur.
- **« Ver »** : logiciel malveillant qui se reproduit sur d'autres ordinateurs en utilisant les réseaux informatiques (Internet).
- **« Backdoor »** : traduction de passage secret. Ce sont des accès privilégiés cachés, installés par les concepteurs de logiciels ou par des malwares, qui permettent d'accéder à un ordinateur, à l'insu de son propriétaire.

ESCROQUERIES OU SCAMS



LE TERME

Le terme « scam » en anglais signifie escroquerie ou ruse.

En français, on utilise aussi le terme « arnaque ».

On parle parfois de scam africain, car c'est une source importante de ce type de malversation (Côte d'Ivoire et Bénin pour les courriels en français).

On parle également de scam 419 en référence à la loi n° 419 du Nigeria, réprimant ce type de pratique. Le Nigeria est réputé pour être à la source de nombreux scam en anglais.

LA TECHNIQUE

Vous recevez un courriel indésirable (voir pourriel) qui va chercher à abuser de votre crédulité ou de votre compassion pour vous soutirer de l'argent.

- **Crédulité :** un courriel vous informe que vous avez gagné une somme importante à une loterie. On vous demande de prendre contact avec un huissier ou un avocat (bidon). Celui-ci vous informe que pour effectuer le transfert, il y a quelques frais (somme très modique au regard de la somme espérée) et vous demande de vous en acquitter en mandat international (Western Union par exemple). Vous ne recevrez jamais la somme promise. Vous serez même peut-être relancé pour d'autres « frais ».
- **Compassion :** un courriel vous informe qu'une personne est dans la détresse et a besoin de votre aide ou qu'elle détient une grosse somme d'argent, mais ne peut la faire sortir du pays qu'avec votre aide ou qu'elle est mourante…. Vous allez encore devoir envoyer des sommes modiques à l'étranger par Western Union…
- **Gain ou cadeau :** une page web s'affiche pour vous informer que vous avez gagné un cadeau, vous proposer de répondre à un sondage et vous offrir un cadeau en remerciement, … Le cadeau sera gratuit, mais on vous demandera des frais de livraison. Vous ne recevrez jamais les cadeaux. On vous demande aussi vos codes de carte bancaire pour payer les frais de livraison. Certains l'utilisent pour effectuer un paiement frauduleux ou voler vos codes CB. Vos coordonnées postales et adresse email peuvent également être utilisées.

LES BONS RÉFLEXES

Méfiez-vous des gains trop faciles, ils cachent généralement une escroquerie. C'est le cas de nombreuses arnaques qui vous demandent de payer des frais à l'avance. C'est aussi le cas de certains sondages qui vous offrent un cadeau en remerciement, ou de pages web qui vous proposent des produits à prix extrêmement bas.

Un avocat ou un huissier a le plus souvent une adresse de courriel au nom de son cabinet.

Méfiez-vous des adresses obtenues sans contrôles chez les grands opérateurs mondiaux : gmail, hotmail, yahoo…

Méfiez-vous tout particulièrement des mails avec des numéros de téléphone étranger.

Si un de vos amis vous réclame de l'aide en grande urgence, essayez de vérifier qu'il s'agit bien de lui en croisant plusieurs informations.

Ne donnez jamais vos codes de cartes bancaires pour payer les frais de livraison d'un cadeau, ou de produits à prix 'cassés', sans vous assurer de la pertinence et de la notoriété du site web ou de la société à l'origine de l'offre.

QUE FAIRE SI...

Déposer une plainte en expliquant que vous avez été victime d'une arnaque sur Internet et que vous avez envoyé des fonds à telle personne.

BON À SAVOIR

Lorsqu'il organise une loterie, le Crédit du Maorc ne demande jamais le paiement de frais pour obtenir le gain.

AUTRES FORMES

D'autres formes d'arnaque cherchent à vous faire dépenser de l'argent en vous incitant à contacter des numéros surtaxés dont ils récupèrent une partie du profit :

- Appel manqué : votre mobile sonne et le correspondant raccroche de suite. Le numéro affiché est 0899… Vous allez chercher à contacter ce correspondant mystère en le rappelant… C'est un numéro surtaxé à l'appel et à la durée. Un message vocal très bien fait va chercher à vous faire rester le plus longtemps possible en ligne…
- SMS surtaxés : vous recevez un SMS vous incitant à répondre. Quelques exemples :

« Bravo, vous avez gagné… Renvoyez GAIN au 54321 »,

« Votre compte est à découvert suite à un débit de 4000 Dhs… »,

« Votre carte de crédit a été utilisée pour des paiements suspects ».

MES DONNÉES BANCAIRES

QUELLES INFORMATIONS PROTÉGER ?

LES INFORMATIONS BANCAIRES

Tout d'abord, vous devez considérer comme **hautement confidentiel l'ensemble de vos codes et identifiants bancaires** qui vous permettent de vous connecter aux services en ligne ou d'effectuer des règlements :

LES MOTS DE PASSE DE CONNEXION

Ne doivent jamais être communiqués afin d'assurer la sécurité de vos données et opérations bancaires, sauf sur :

- Le site Internet de votre banque,
- Les autres services d'accès (téléphone, applications bancaires pour Smartphone) de votre banque.

LES CODES DE SÉCURITÉ À USAGE UNIQUE

Ne doivent jamais être communiqués afin d'assurer la sécurité de vos opérations bancaires, sauf sur :

- Le site internet de votre banque, si vous êtes à l'origine de cette demande de code pour effectuer une opération protégée,
- Le site marchand ou le site de paiement utilisé par le marchand, si vous êtes à l'origine de cet achat.

ATTENTION

Si vous avez reçu un code de sécurité en dehors des deux cas précédents, alors il s'agit d'une tentative de fraude ou d'une erreur de coordonnées téléphoniques. Contactez rapidement votre agence pour vérification.

LE CODE CONFIDENTIEL DE VOTRE CARTE DE CRÉDIT (CODE PIN)

Ne doit jamais être communiqué, sauf sur :

- Les Distributeurs Automatiques de Billet,
- Les Terminaux de Paiement Électroniques chez les commerçants, ainsi que les caisses automatiques (station service,…),
- Les Guichets Automatiques Bancaires de votre banque.

SONT ÉGALEMENT À PROTÉGER…

- Le numéro de la carte de crédit
- La date de fin de validité de la carte de crédit
- Le cryptogramme de la carte de crédit (3 derniers chiffres au dos de la carte)
- Le numéro de compte
- Toute information contenue dans le Relevé d'Identité Bancaire (RIB ou IBAN)

LES INFORMATIONS PERSONNELLES

Mais au-delà de ces précautions, certaines données personnelles non sensibles individuellement, se révèlent être potentiellement dangereuses dès lors qu'elles sont associées aux données bancaires. Par exemple : vos noms et prénoms associés à votre numéro de RIB peuvent permettre aux pirates de lancer des campagnes de phishing particulièrement efficaces.

CES INFORMATIONS PERSONNELLES SONT…

- Vos noms et prénoms
- Votre adresse postale
- Vos numéros de téléphone
- Votre date de naissance
- Votre adresse email

Toute modification de vos informations personnelles doit être signalée sans délai à votre banque.

POURQUOI LES PROTÉGER ?

Certaines de vos informations bancaires vous permettent d'accéder à vos services en ligne (Numéro de compte + mot de passe) ou d'effectuer des paiements en ligne (Numéro de carte bancaire, date de validité et code cryptogramme). Si quelqu'un de mal intentionné est en possession de ces informations, il pourra les utiliser à votre insu.

De même, les codes de sécurité à usage unique sont la cible des pirates, car ils permettent d'effectuer des opérations frauduleuses. Ces codes sont généralement reçus par SMS, ou par synthèse vocale sur un téléphone fixe, ou par email. Ils permettent de sécuriser des opérations effectuées sur Internet telles que :

- Des opérations sensibles sur le site de votre banque en ligne, comme par exemple la création de RIB pour effectuer un virement,
- Des achats sur Internet, protégés par un dispositif complémentaire tel que 3Dsecure.

Les pirates tentent de dérober ces codes par différents moyens techniques plus ou moins complexes, tel que l'affichage d'une fenêtre vous demandant ce code sous de faux prétextes de sécurité, ou le piratage de votre messagerie par le vol de votre identifiant de messagerie et son mot de passe.

COMMENT LES PROTÉGER ?

Quelques bons réflexes peuvent vous éviter de nombreux désagréments :

- Éviter de conserver sur du papier vos codes d'accès, numéros de la carte bancaire ou mots de passe associés,
- Refusez la mémorisation des mots de passe quel que soit l'ordinateur que vous utilisez,
- Ne communiquez jamais à un tiers non identifié ou dont la réputation n'est pas sûre, des informations bancaires ou personnelles telles que les numéros bancaires, emails ou téléphones,
- Ne communiquez vos données bancaires que sur des sites fiables et à travers des modes de communications sécurisés (https),
- Évitez de transmettre vos données bancaires par email et messagerie instantanée,
- Évitez de conserver sur votre ordinateur des données confidentielles,
- Signalez sans délai à votre banque toute modification de vos informations personnelles,
- Supprimez régulièrement les cookies et fichiers Internet temporaires de votre ordinateur.

Ma banque partout avec moi :

En Agence

Avec votre conseiller Crédit du Maroc
Liste et horaires des agences disponibles sur www.creditdumaroc.ma

Via notre Centre de Relation Clients

3232
Du lundi au samedi de 8h à 20h

Via notre site internet

www.creditdumaroc.ma

Via nos Guichets Automatiques Bancaires

Plus de 400 GAB dans tout le Royaume

Crédit du Maroc, société anonyme à directoire et conseil de surveillance, au capital social de 1.088.121.400,00 Dhs, RC n° : 28.717, établissement agréé en qualité de banque par Bank Al Maghrib en vertu de l'arrêté n°2348-94 du 23 août 1994.
Siège social : 48-58, boulevard Mohammed V Casablanca.

مصرف المغرب
CRÉDIT DU MAROC