Messages et appels téléphoniques frauduleux

Le phishing – ou hameçonnage – reste l'une des armes favorites des cybercriminels. Ils essaient, par de faux messages, de détourner de l'argent ou des données personnelles. Découvrez ici quelles formes peut prendre le phishing. Nous vous expliquons aussi comment déjouer les arnaques téléphoniques.

Les messages frauduleux sont une part importante des arnaques en ligne. Les criminels les envoient pour collecter des données privées ou vous piéger avec des malwares. Encore récemment, ils procédaient surtout par e-mail. Aujourd'hui, ils utilisent aussi le SMS, WhatsApp, Facebook Messenger, etc.. Ces messages ne sont pas un phénomène nouveau. Jadis, ils étaient envoyés par la poste et par fax. Le fax a pratiquemment disparu, mais il subsiste des arnaques par lettre.

Nous allons voir comment identifier les faux messages et appels téléphoniques. Au fil des chapitres suivants, nous vous exposerons le fonctionnement d'autres fraudes. Bon à savoir : les criminels combinent souvent plusieurs formes d'arnaque. Par exemple, du phishing suivi d'une transaction de cryptomonnaies malhonnête.

Phishing

Les criminels envoient un nombre incalculable de messages de phishing. À titre indicatif, Google en supprime 100 millions par jour. Les filtres antispam en arrêtent aussi beaucoup, mais il arrive que certains passent à travers les mailles. Le phishing transite par tous les canaux en ligne : e-mail, WhatsApp, Facebook Messenger, Instagram, etc. Les messages de phishing arrivent également par SMS. D'où aussi le terme de smishing (contraction de SMS et de phishing).

Avec ces messages, les criminels cherchent à dérober de l'argent ou des données. Ce sont souvent des messages urgents invitant à se connecter à un site comme celui d'une banque, d'une boutique ou d'une agence gouvernementale. La ressemblance entre le faux site et le site authentique est à s'y méprendre. Or, en vous y connectant, vous confiez vos identifiants à des criminels.

Attention au phishing de carte bancaire

Vous avez entendu parler du phishing de carte bancaire ? Les fraudeurs vous demandent dans un e-mail ou un SMS, au nom de la banque, de renvoyer votre carte bancaire, sous prétexte qu'elle deviendrait inutilisable sous peu. Ils vous envoient aussi un lien pour récupérer votre code PIN. Ce lien mène à une page de formulaire, sur un site factice. Vous êtes invité à introduire vos coordonnées bancaires (données personnelles, numéro de carte, code PIN). Pour paraître plus crédible, le fraudeur vous demande parfois de couper la carte en deux, en son milieu. Mais ceci n'invalide pas la carte. Il faudrait pour cela couper la puce métallique. Jamais une banque ne vous demandera de renvoyer votre carte bancaire.

Les malfrats du web recourent aussi aux messages frauduleux pour propager des virus. Ils vous demandent par exemple d'installer un logiciel pour suivre un colis postal. Il s'agit souvent de ransomwares, des logiciels qui verrouillent les fichiers de votre PC. Les criminels ne les libèrent que contre une rançon.

Méfiez-vous particulièrement des messages au nom de banques, de services de livraison, d'agences de recouvrement, d'agences gouvernementales, de fournisseurs d'énergie et d'opérateurs internet. Ces messages concernent souvent des recouvrements, créances, cartes bancaires, problèmes de sécurité, amendes, factures, comptes expirés, erreurs de paiement, livraisons manquées et déclarations de dommages automobiles. Les déclarations de gains, envoyées au nom de grandes enseignes ou d'e-shops sont aussi souvent mensongères.

Pour éviter tout problème, évitez de cliquer sur des liens malveillants dans les messages de phishing. Vous trouverez ici quelques astuces pour les identifier.

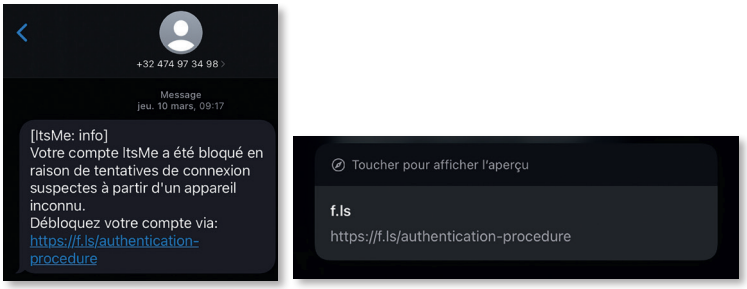
Liens incorrects

Beaucoup de messages de phishing incluent un lien qui mène à un site où vous êtes invité à saisir des données, comme vos identifiants bancaires. Le lien peut aussi déboucher sur un site contenant des malwares. Comment savoir si un lien est fiable ? L'adresse à laquelle il mène doit avoir une certaine logique. Prenons par exemple un message de phishing au nom de Netflix. Le lien du message correspond à une adresse étrange. L'indice ne laisse aucun doute : c'est un message frauduleux, car la véritable adresse web de Netflix est netflix.com.

Le lien figurant dans cet e-mail ne mène manifestement pas au site officiel de Netflix

Vérifiez le lien

Soyez bien conscient que l'adresse web affichée ne correspond pas toujours à celle où mène le lien. Comment vérifier un lien dans un e-mail ? Tout dépend de l'appareil sur lequel vous recevez le message.



Le lien contenu dans ce SMS mène à tout sauf au site officiel d'itsme

- **Sur ordinateur :** déplacez le curseur sur le lien. L'adresse s'affichera dans le bas de la fenêtre. Parfois, la véritable adresse apparaîtra dans une petite fenêtre à droite du curseur, comme dans l'exemple de Netflix à la page précédente.
- **Sur smartphone ou tablette :** laissez votre doigt appuyé sur le lien pendant un moment. Une sorte de pop-up apparaîtra avec l'adresse complète, comme ici.

Dans le chapitre 3, vous pourrez apprendre à identifier un lien frauduleux.

Expéditeur incorrect

Un expéditeur incorrect est souvent révélateur d'une tentative de phishing. Dans notre exemple (voir image ci-dessous), l'adresse n'est pas d'Amazon. Malheureusement, les criminels ne vous facilitent pas la tâche. En effet, des spammeurs peuvent falsifier l'adresse d'expédition. Ils utilisent pour cela la technique du spoofing, qui transforme l'adresse en une alternative crédible.

Un e-mail d'Amazon ? L'adresse @proximus.com laisse penser le contraire

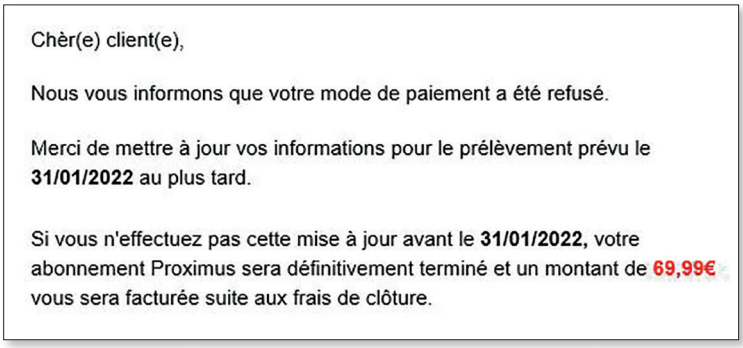
Faux code QR

Le phishing par code QR est assez nouveau. Scanner un code QR permet d'accéder rapidement à un site web. Les criminels peuvent l'utiliser pour vous attirer vers de faux sites, par exemple le site contrefait d'une banque ou celui d'un fournisseur d'énergie. Vous pouvez tomber sur des codes QR frauduleux dans divers messages en ligne, comme des e-mails ou des messages WhatsApp.

Quand vous scannez un code QR avec l'appli photo de votre smartphone (ou avec une appli faite pour scanner les codes QR), l'adresse web qu'il contient apparaît. Vérifiez qu'elle est correcte avant de vous rendre sur le site en question.

Salutations non personnalisées

Les spammeurs n'ont souvent que votre e-mail. Ils ne peuvent donc pas s'adresser à vous personnellement, par vos nom et prénom. De nombreux e-mails de phishing commencent par une formule de salutation impersonnelle comme "Cher Client".



Chèr(e) client(e),

Nous vous informons que votre mode de paiement a été refusé.

Merci de mettre à jour vos informations pour le prélèvement prévu le **31/01/2022** au plus tard.

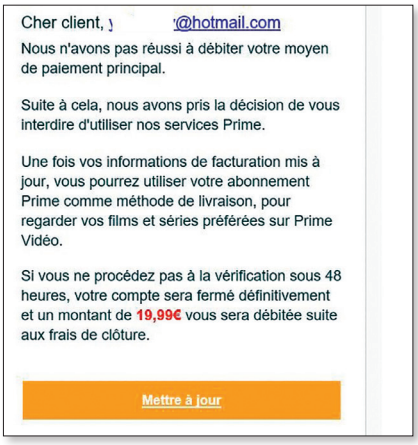
Si vous n'effectuez pas cette mise à jour avant le **31/01/2022,** votre abonnement Proximus sera définitivement terminé et un montant de **69,99€** vous sera facturée suite aux frais de clôture.

C'est à la suite de fuites de données que les cybercriminels obtiennent leurs listes d'e-mails, de noms, de prénoms et d'autres données personnelles. Les messages frauduleux avec salutations personnalisées deviennent donc de plus en plus fréquents.

Urgence et menace

Un moyen de pression bien connu pour inciter les victimes à réagir consiste à invoquer l'urgence. Les faux e-mails envoyés au nom d'une banque, par exemple, menacent souvent de bloquer un compte.

Ou alors, les e-mails de phishing provenant d'agences de recouvrement utilisent des techniques d'intimidation en annonçant des frais élevés en cas de non-paiement. Il existe aussi des faux e-mails citant la fermeture imminente d'un compte "pour raisons de sécurité".



Cet e-mail prétend que votre compte sera fermé si vous n'agissez pas dans les 48 heures

Promesse irréaliste

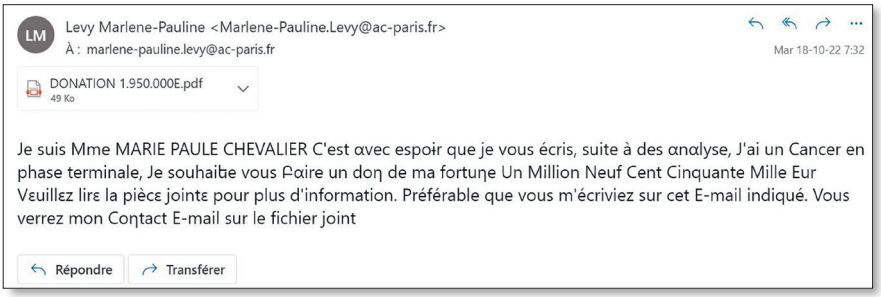
Bon nombre de spams promettent de gagner un prix ou un bon d'achat. Quand vous cliquez sur le lien, les spammeurs demandent de compléter diverses infos privées. Il arrive qu'ils vous fassent appeler un numéro surtaxé ou acheter un abonnement SMS. Le bon d'achat est un leurre, vous ne le recevrez jamais.

Ne participez pas aux campagnes de cadeaux, sauf si elles figurent sur le site officiel du vendeur ou ses réseaux sociaux. Se désabonner de faux e-mails vous promettant des gains peut se retourner contre vous : en cliquant pour vous désabonner, vous indiquez aux spammeurs que vous avez lu leur e-mail.

Un e-mail de phishing au nom d'IKEA vous promettant une carte cadeau de 1000 €

Fautes de langue

Le langage utilisé par les spammeurs s'est amélioré. Un message rédigé dans un français correct peut être une tentative de phishing. Cependant, les messages écrits dans un français douteux, comme ci-dessous, sont encore légion.



On ne peut pas dire que cet e-mail de phishing soit bien rédigé.

E-mail avec pièce jointe

Certains courriers électroniques non sollicités contiennent en pièce jointe un fichier susceptible de contenir des malwares. Lorsque vous l'ouvrez, il contamine votre appareil. Ne cliquez donc jamais sur une pièce jointe provenant d'un expéditeur en qui vous n'avez pas confiance. Prêtez attention au format du fichier. Les fichiers .zip, .exe et javascript (.js), entre autres, sont pour le moins suspects.

Scannez ce code QR pour apprendre à démasquer les tentatives de phishing
www.testachats.be/phishing

Harponnage

Souvent, les fraudeurs ciblent de nombreuses victimes lors d'une opération de phishing, avec des milliers d'e-mails. La plupart des destinataires ne répondent pas, mais quelques-uns se font piéger. Le phishing ciblé, aussi nommé spear phishing ou harponnage, est plus efficace. Cette méthode est en plein essor.

Le criminel fait des recherches. Il examine vos comptes sur les réseaux sociaux et exploite ces connaissances pour gagner votre confiance. Il existe de nombreuses variantes de cette technique. Par exemple, une personne vous appelle au nom de la banque, disant que votre compte présente un problème. Au départ, le spear phishing visait surtout les entreprises et les institutions. Les criminels envoyaient des messages à un directeur ou un membre du département finances. En pièce jointe, ils incluaient un malware ou une facture d'apparence crédible. Aujourd'hui, les particuliers sont aussi la cible du harponnage. Une personne se fait passer pour un ami proche ou un employé de banque et utilise un prétexte pour demander de l'argent ou des identifiants, comme pour la fraude à la demande d'aide et les appels bancaires frauduleux.

Fraude à la demande d'aide

Pour cette fraude, les criminels se font passer pour l'une de vos connaissances et demandent de l'argent sous un faux prétexte. Dans certains cas, ils prétendent être votre enfant. Ils prétendent avoir un "nouveau numéro" parce que leur ancien téléphone est cassé. Peu après, ils se plaignent de ne pas pouvoir payer une facture. Est-ce que maman ou papa peut leur avancer la somme ?

Phishing par photo

Super, vous avez eu votre permis de conduire ! Nombreux sont ceux qui aiment partager cette bonne nouvelle sur Facebook, Twitter ou Instagram avec une photo du document. Ne tombez pas dans ce piège. Si vous souhaitez que votre permis ou passeport soit sur la photo, prenez au moins la précaution de masquer vos détails personnels.

Parfois, cette fraude se veut aussi raffinée sur le plan technologique. Les fraudeurs enregistrent la voix des personnes dont ils veulent usurper l'identité et utilisent ensuite ceci pour convaincre leurs victimes. Ce type d'arnaque sévit surtout sur WhatsApp mais d'autres canaux y sont exposés, comme Messenger.

Voici comment déjouer les tentatives de fraude à la demande d'aide.

- **Méfiance face à un nouveau numéro** : soyez sur vos gardes si quelqu'un prétend être une "connaissance" qui vient de changer de numéro. Il peut s'agir d'une fraude. Le fait que la photo de la personne soit bien la sienne n'est pas une preuve. Elle peut avoir été copiée des réseaux sociaux. Un message vocal ne prouve rien non plus. Il pourrait s'agir d'un enregistrement détourné.
- **Pas d'avance d'argent :** si le nouveau contact demande une avance d'argent, il y a anguille sous roche. Etant donné que cette méthode d'escroquerie est très connue, les criminels attendent parfois avant de demander de l'argent. Les premiers jours, les contacts sont normaux et les conversations banales.
- **Appel en cas de doute :** vous ne savez pas si vous avez affaire à un fraudeur ? Appelez la personne en utilisant son ancien numéro. Si elle décroche, il est clair que le nouveau numéro est un malfrat. Signalez la fraude. Si vous appelez le nouveau numéro, vous entendrez sûrement un enregistrement de la voix de votre connaissance. Cela ne veut pas dire qu'elle a vraiment changé de numéro. Ayez une vraie conversation et évitez de marquer votre accord juste parce que vous avez reconnu le son d'une voix, ou que la connexion est mauvaise.
- **Vérification du numéro :** vous n'arrivez pas à joindre votre connaissance ? Véri-

fiez le nouveau numéro dans un moteur de recherche. Si quelqu'un a déjà commis une fraude avec ce numéro, il y a des chances que vous en trouviez trace.
- **Ne transmettez pas de code** : quelqu'un vous demande de lui faire suivre un code de vérification WhatsApp soi-disant envoyé par erreur ? Ne répondez pas. La personne essaie de prendre le contrôle de votre compte. Le code est destiné à associer un nouveau numéro de téléphone à votre compte WhatsApp.

Appels téléphoniques frauduleux

Le phishing passe aussi par téléphone. Ces appels frauduleux sont connus sous le nom de vishing, contraction de voice et phishing. Un criminel vous appelle de façon intrusive. Il peut s'agir d'un soi-disant employé de Microsoft, de la banque ou de la police qui vous téléphone à l'improviste avec un propos frauduleux.

Les faux appels sont répandus

Les appels téléphoniques pour le compte d'une banque sont très répandus. Un prétendu employé de banque vous informe d'une menace de cyberattaque. Pour éviter d'en être la victime, vous devez "sécuriser" votre épargne en la transférant sur un autre compte. Et comme par hasard, il s'agit du numéro de compte du criminel que vous avez au bout du fil. Les appels pour le compte d'un service d'assistance de Microsoft ou d'une autre société informatique sont une variante bien connue. L'appelant prétend que des problèmes ont été détectés sur votre PC et vous propose gentiment de les résoudre. En réalité, votre PC ne présente aucune défaillance. Vous avez affaire à un criminel qui veut vous dérober de l'argent, par exemple en installant un malware sur votre ordinateur.

Logiciels d'accès à distance

Ces logiciels interviennent souvent dans les appels téléphoniques frauduleux, y compris ceux passés au nom de Microsoft. Pour résoudre le soi-disant problème, le prétendu employé du service d'assistance vous demande d'installer un logiciel qui lui permet de suivre ce qui se passe sur votre écran. Il s'agit souvent de Teamviewer ou Anydesk. Après l'installation, le criminel peut voir ce qui se passe sur l'écran, y compris quand vous saisissez vos données bancaires.

Robocalls

Les "robocalls" sont un phénomène récent. Vous recevez un appel d'une voix automatisée qui prétend (souvent en anglais) appeler au nom d'un service comme la police ou une agence gouvernementale. Le message prétend que vous êtes l'auteur d'une infraction grave (blanchiment d'argent...) ou que vous faites l'objet d'un mandat d'arrêt. Après avoir appuyé sur une touche, vous parlez aux escrocs, qui tentent de vous soustraire des données ou de l'argent.

Usurpation d'identité (spoofing)

Ce terme a déjà été évoqué quand nous avons parlé d'e-mails frauduleux. L'usurpation d'identité est aussi utilisée lors de faux appels téléphoniques. Les criminels peuvent falsifier le numéro avec lequel ils appellent. L'écran du téléphone affiche le vrai numéro de la banque, de la police ou d'une autre autorité, alors que vous parlez à un criminel. Voilà qui rend l'arnaque très crédible.

Prévenir la fraude bancaire

Gardez ces règles de base à l'esprit pour éviter d'être victime de fraude bancaire.

- La banque (ou un autre organisme) n'appellera jamais pour vous demander de mettre votre argent à l'abri, ni de le transférer sur un "compte sécurisé".
- Même si le numéro ou le nom de votre banque apparaît à l'écran de votre téléphone, il peut toujours s'agir d'un fraudeur qui aurait modifié le numéro avec lequel il appelle, via spoofing (ou usurpation d'identité).
- N'envoyez votre carte bancaire nulle part (même découpée). Ne la faites pas enlever non plus.
- En cas de doute, demandez le nom de l'employé, raccrochez et rappelez vous-même la banque.
- Ne vous laissez pas berner par les informations qui tendent à prouver que c'est soi-disant la banque qui vous appelle. L'escroc connaît parfois des détails personnels vous concernant, qu'il a obtenues par phishing ou sur internet.
- Évitez de conserver un solde trop élevé sur votre compte courant. Vous réduirez ainsi le risque d'une perte importante si vous êtes victime d'autres types d'escroquerie (comme le vol de votre carte de banque).
- Fixez une limite peu élevée à vos transactions quotidiennes. Et ne l'augmentez pas sur l'insistance d'un (faux) employé de banque.
- Vous constatez un retrait d'argent involontaire depuis votre compte ? Contactez la banque dès que possible, faites une déclaration à la police et signalez-le à **https://pointdecontact.belgique.be/**.

Fraude par rappel téléphonique

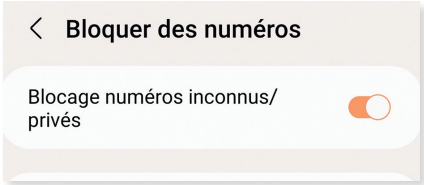
Les criminels qui usent de cette fraude appellent avec un numéro inconnu, souvent de l'étranger. Ils laissent le téléphone sonner deux fois et raccrochent. Ils espèrent que vous les rappellerez. C'est alors que le compteur commence à tourner. Le numéro en question est lié à un service surtaxé. Plus vous restez en ligne, plus le criminel gagne de l'argent. Vous avez l'impression que personne

ne décroche mais, en réalité, la connexion est établie. Les criminels passent une cassette avec la tonalité d'appel et se remplissent ainsi les poches.

Pour éviter ce type de fraude, vous pouvez régler le téléphone pour qu'il ne sonne pas lorsqu'un appel provient d'un numéro inconnu. L'appelant sera alors automatiquement redirigé vers votre messagerie vocale. Cette solution permet aussi d'éviter les appels de vendeurs indésirables.

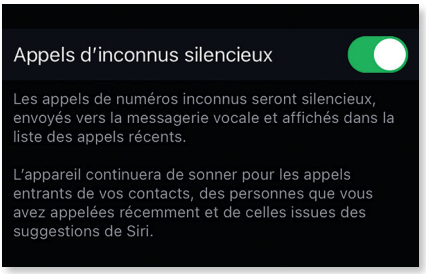
Android

1. Lancez l'appli **Téléphone** et appuyez sur ⋮.
2. Sélectionnez **Paramètres**.
3. Choisissez **Bloquer des numéros**.
4. Activez le curseur pour **Bloquer des numéros inconnus/privés**.



iOS

1. Allez dans **Réglages**.
2. Faites défiler vers le bas et choisissez **Téléphone**.
3. Faites défiler vers le bas et choisissez **Appels d'inconnus silencieux**.
4. Activez le curseur.



Offres de gain

Les fraudeurs utilisent les réseaux sociaux et applis pour diffuser des messages comme des offres de gain. Si vous y réagissez, on vous demande de communiquer vos détails de paiement. Les pirates utilisent souvent des noms de chaînes de magasins connues. Signalez ces messages. De nombreux sites de réseaux sociaux proposent un bouton réservé à cet effet.