Cybercrime

Le phishing (hameçonnage), gare aux faux sites !


©DGPN/SICoP

Cette technique est très utilisée sur Internet par des fraudeurs via des emails, des liens, des faux sites web et des pièces jointes... pour obtenir des informations personnelles : mots de passe, numéros de comptes bancaires, codes...

Comment s'en prémunir ?

Pour se prémunir du **phishing**, adoptez les bons réflexes en détectant immédiatement la tentative d'escroquerie :

- Les organismes bancaires ne vous demanderont JAMAIS vos coordonnées bancaires par internet.
- Le Trésor Public, la CAF ou tout autre organisme d'État ne vous demandera JAMAIS d'informations personnelles ou vos coordonnées bancaires par internet.
- Les sociétés de téléphonie ne vous demanderont JAMAIS de renouveler votre abonnement par internet.
- La "Loterie nationale" qui vous annonce que vous avez gagné plusieurs milliers d'euros N'EXISTE PAS.

Cette liste n'est pas du tout exhaustive. Dans tous les cas, il ne vous sera jamais demandé d'envoyer vos coordonnées bancaires, vos mots de passe ou tout autre information personnelle.

Comment reconnaître une tentative de phishing ?

Pour tromper les utilisateurs, les messages reçus peuvent avoir différentes formes et émaner de sources très diverses :

- notifications de réseaux sociaux
- relevés de comptes bancaires
- alertes virus
- messages de banques
- du Trésor Public
- fournisseur d'accès Internet, téléphonie
- sites de ventes aux enchères ou payement en ligne

Le phishing s'adapte chaque année à l'actualité (faux site imitant celui des impôts, de la CAF...), à l'apparition de nouveaux services mis à la disposition des internautes et des abonnés téléphoniques.

Même logos, même slogans, tout y est !

Les techniques de **phishing** se sont nettement améliorées. Un simple clic sur un lien vous amène sur la réplique exacte du site d'une **administration,** d'une **banque,** d'un **fournisseur de service ou de tout autre organisme pouvant détenir vos informations bancaires et personnelles.**

avis au remboursement.

impots.gouv.fr <dg-fip@recouvrement-fp.net> 20 août (Il y a 9 jours)

impots.gouv.fr
un site de la direction générale des finances publiques

Bonjour,

Après les derniers calculs annuels de l'exercice de votre activité, nous avons determiné que vous êtes admissible à recevoir un remboursement de 50.80 €.
Veuillez nous soumettre s'il vous plaît la demande de remboursement d'impôt pour nous permettre de la traiter dans un plus bref délai.

>> Pour accéder au formulaire , cliquez ici .

Un remboursement peut être retadré pour diverses raisons. Par exemple, une soumission de dossiers non valides ou une inscription après une certaine limite.

Philippe BERGER
Conciliateur fiscal adjoint

© Direction générale des finances publiques - 2014

Attention, les messages frauduleux sont maintenant rédigés dans un **français parfait.** Les fautes d'orthographe ne permettent plus d'identifier ou non une tentative de **phishing**.

Après étude de votre déclaration de ressources, nous vous informons que vous avez droit à une prime d'aides vacances versés par votre CAF , afin de bénéficier de cette prime , nous vous invitons à suivre les étapes en cliquant sur le lien ci-dessous :

Cliquez ici

- Le montant d'aide est égal à 250,80 € pour une personne seule , majoré de 50% à la présence de deux personne et de 30% pour chaque personne supplémentaire .

Le site www.caf.fr est édité et hébergé par la Caisse nationale des Allocations familiales (Cnaf) dont le siège social est situé 32, avenue de la Sibelle,
75685 PARIS CEDEX 14.
Identifiant SIREN : Cnaf n° 180 035 065
Identifiant SIRET : 180 0350 65 000 36
Téléphone : +33 1 45 65 52 52
Directeur de la publication : Hervé Drouet.

Les bons réflexes

Ne pas cliquer avant d'avoir lu l'intégralité du message reçu, même si ce message vous semble émaner d'une source sûre et connue.
Se méfier des messages de type « Nous suspectons une transaction non autorisée sur votre compte ». Il s'agit très certainement d'une tentative de **phishing** basée sur la crainte et la peur.

Dans ce type de cas, l'internaute est ensuite amené à cliquer sur un lien le menant sur un faux site. Arrivé sur le site frauduleux, l'**internaute est pris au piège** grâce à des repères visuels identiques aux sites officiels (logos, images, slogans). Il est alors invité à remplir un formulaire avec ses informations personnelles, mots de passe et identifiants de comptes bancaires par exemple. Le piège se referme.

Ne jamais transmettre d'informations bancaires par courrier électronique.

Ne jamais répondre à un courrier électronique vous demandant des informations personnelles.

Vérifier l'url dans la barre d'adresse du navigateur. Il peut exister une légère faute de saisie dans l'adresse du site. Dans la majorité des navigateurs, un **cadenas vert** précise l'existence d'une connexion sécurisée utilisant **SSL**, ce qui est une indication supplémentaire de légitimité du site.

Les navigateurs Internet possèdent une **protection anti-phishing**. Comment l'activer ?
Aller dans l'onglet : Préférences / Sécurité
Cocher la case : Prévenir lorsque les sites essaient d'installer des modules complémentaires
Cocher la case : Bloquer les sites signalés comme étant des sites d'attaque
Cocher la case : Bloquer les sites signalés comme étant des contrefaçons

Que faire si j'ai déjà cliqué ?

Connectez-vous le plus rapidement possible sur votre compte et **changez** votre mot de passe pour le site en question.

Appelez **immédiatement** votre banque pour prévenir de la situation, même en cas de doute.

En cas de doute sur un courrier électronique, signalez-le sur **internet-signalement.gouv.fr** puis supprimez le de votre boite mail.

Vous pouvez aussi contacter : **INFO ESCROQUERIES** au 0805 805 817 (appel gratuit) pour être conseillé par des policiers et des gendarmes spécialisés.

Pour aller plus loin, effectuez un **scan** de votre ordinateur avec un **anti-virus à jour**.

Comment porter plainte en cas d'escroquerie sur Internet ?

Si vous êtes victime d'une escroquerie sur Internet, **déposez plainte au commissariat** ou à la gendarmerie la plus proche. Pour gagner du temps, pensez à la pré-plainte en ligne .

Munissez-vous de tous les renseignements suivants :

- références du (ou des) transfert(s) d'argent effectué(s).
- références de la (ou des) personne(s) contactée(s): adresse de messagerie ou adresse postale, pseudos utilisés, numéros de téléphone, fax, copie des courriels ou courriers échangés...
- tout autre renseignement pouvant aider à l'identification de l'escroc.

Actualités
L'actu police
Communiqués de presse
Dossiers
14 juillet 2015 - Le 20è
Contre les vols de voitures et d'accessoires, les bons réflexes !
Cybercrime
Interviews / portraits

Conseils de prévention sur Internet
Comment choisir ses mots de passe ?
Le vishing, gare aux appels frauduleux !
Cyberattaques, sur les smartphones aussi !
Arnaque à la webcam
Réseaux sociaux : arnaque aux comptes désactivés
Réseaux sociaux : arnaque aux faux amis
Arnaques par SMS
Arnaque à l'appel en absence