Table des matières

Dossier réalisé en partie avec la BPBFC

Le phishing

Pour vous prémunir contre cette forme d'escroquerie de plus en plus répandue sur internet, la Banque Populaire vous livre ses bonnes pratiques.

Qu'est-ce que c'est ?

Le Phishing (ou hameçonnage) est une technique frauduleuse consistant à envoyer de manière massive un message semblant légitime (il peut s'agir de mail le plus souvent, ou de SMS) pour inciter la victime à cliquer sur un lien ou une pièce jointe potentiellement malveillants.

L'identité d'organismes ou d'entités connues (Netflix, organismes d'état comme le site des impôts, etc.) tout comme celui de la Banque Populaire, qu'il s'agisse de sa dénomination ou de son logo, est régulièrement utilisée par des tiers à des fins frauduleuses auprès de particuliers ou de PME/TPE.

Les menaces

L'ouverture d'une pièce jointe ou l'accès à un lien peuvent conduire à l'installation d'un malware ou ransomware(*) sur votre ordinateur.

L'accès à un lien non sécurisé peut permettre le vol et/ou la fuite de données confidentielles comme vos identifiants/mots de passe, numéros et codes de cartes bancaires, etc.

Ces données peuvent ensuite permettre au fraudeur de réaliser de l'ingénierie sociale : par exemple vous pouvez recevoir des appels de faux conseiller clientèle ou de faux service client, prétextant des paiements frauduleux ou des virements à annuler, qui seront en réalité validés par les codes que vous transmettrez.

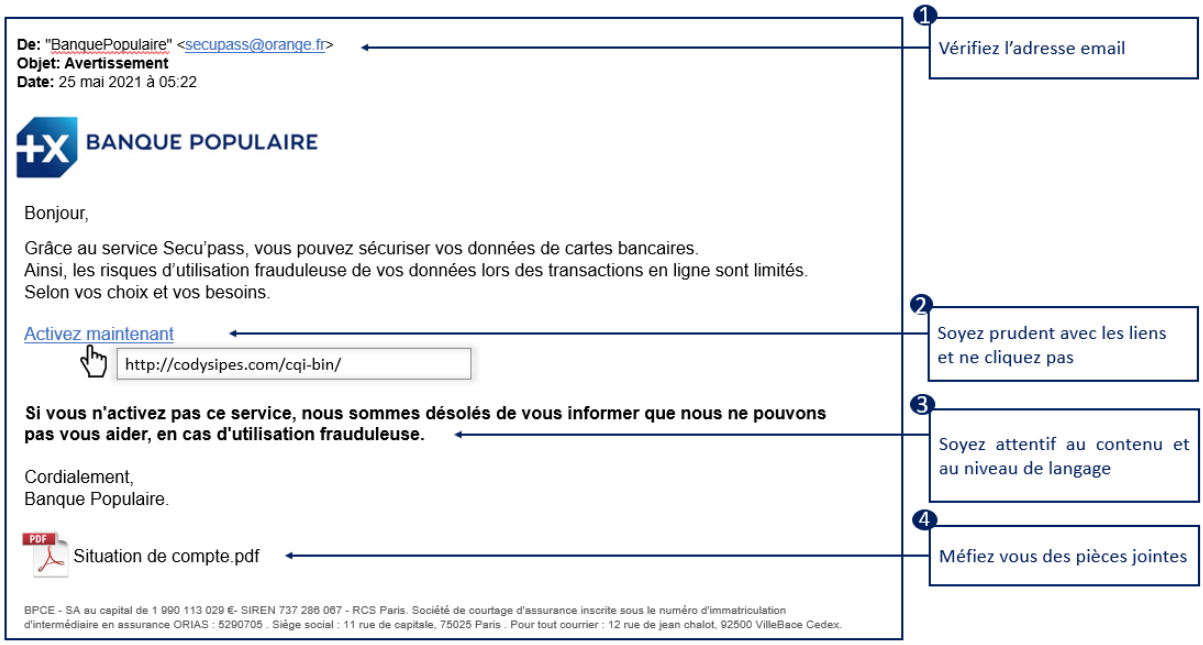
(*) chiffrement des données de l'ordinateur et réclamation d'une rançon contre le décryptage de ces données.

Les bonnes pratiques

Limitez la diffusion de votre adresse email.

- Nettoyez régulièrement votre ordinateur à l'aide d'un antivirus à jour.
- N'ouvrez pas les pièces jointes d'un e-mail non sollicité ou douteux.
- Ne cliquez pas sur les liens sans vous être assuré de leur origine.
- En cas de réception d'un phishing, signalez le mail sur https://www.cybermalveillance.gouv.fr/ et supprimez le mail.
- En ce qui concerne l'accès à votre compte, privilégiez l'accès direct par l'application mobile ou la page d'accueil de votre banque en ligne (en saisissant l'adresse du site internet ou via votre favori), sans cliquer sur un lien transmis par mail ou sms.
- Un conseiller clientèle ou téléopérateur ne vous demandera jamais de données de connexion ou d'informations bancaires de type identifiant/mot de passe, numéro de carte bancaire, code de validation reçu par SMS, etc.
- Parlez–en autour de vous.
- Consultez régulièrement les conseils en matière de sécurité de votre banque.

Reconnaitre un mail de phishing (exemple avec la banque populaire)



Vérifiez l'adresse email : si l'expéditeur ou si l'adresse email vous semble suspecte, il s'agit certainement d'une tentative de Phishing.

Soyez prudents avec les liens et ne cliquez pas sans vous assurer de leur véritable destination : positionnez le curseur de votre souris sur le lien, cela vous révèlera la véritable adresse du site sur lequel vous arriverez en cliquant. Sur un smartphone un appui long vous donnera le même résultat.

Soyez attentif au contenu et au niveau de langage : faites preuve de méfiance si le message contient des fautes de grammaire ou d'orthographe (même si ce critère est de moins en moins déterminant). Méfiez-vous des demandes étranges, urgentes, illégitimes, alléchantes, ou vous demandant vos informations personnelles (codes, identifiants, mots de passe, N° de CB, etc.).

Méfiez-vous des pièces jointes **:** n'ouvrez que celles que vous attendez et ne cliquez jamais sur un document qui vous parait suspect.

La fraude à la carte bancaire

Qu'est-ce que c'est ?

La fraude à la carte bancaire désigne un débit de votre carte réalisé à votre insu.

Elle peut résulter, soit de la perte ou du vol de votre carte, soit de la récupération des informations de celle-ci alors qu'elle est toujours en votre possession (par exemple sur internet, sur votre ordinateur, par une photo d'un commerçant malhonnête, etc.).

Contre la fraude, adoptez les bons réflexes

Contre la fraude, adoptez les bons réflexes
– Ne communiquez jamais vos données bancaires : mot de passe de banque à distance, code Sécur'Pass ou code reçu par SMS, code secret de la carte, numéro de compte…
– Ne validez pas un paiement en ligne dont vous n'êtes pas à l'origine.
– Consultez régulièrement vos comptes.

Les menaces

En cas de récupération des informations de votre carte bancaire, le fraudeur peut réaliser des achats sur internet.

En cas de vol physique, le voleur pourrait réaliser des paiements sans contact, des achats en ligne, et éventuellement retirer de l'espèce s'il a pu obtenir votre code confidentiel.

Les bonnes pratiques

- **Nettoyez** régulièrement votre ordinateur à l'aide d'un antivirus à jour,
- **Vérifiez** régulièrement et fréquemment votre compte bancaire pour identifier tout débit suspect,
- **Signez** votre carte bancaire dès sa réception. Vous éviterez ainsi qu'un fraudeur appose sa propre signature en cas de perte ou de vol par exemple,
- **Conservez** précieusement votre carte bancaire, ne la prêtez à personne,
- **Mémorisez** votre code confidentiel et ne l'écrivez pas,
- **Cachez** le clavier du terminal ou du distributeur lorsque vous effectuez une opération, et ne vous laissez pas distraire par des inconnus,
- Chez un commerçant, **ne quittez jamais votre carte des yeux** et vérifiez le montant affiché par le terminal avant de valider l'opération,
- **Vérifiez la notoriété du site Internet** avant de réaliser votre achat (recherche sur Internet ou d'avis par exemple), et ne mémorisez pas vos informations bancaires sur Internet,
- **Ne communiquez jamais vos données bancaires** (numéro de carte ou autres) ou un code d'authentification en réponse, notamment, à :
- – **un email**, même s'il semble provenir d'une administration ou d'une banque,
  – **un appel téléphonique** lorsque votre interlocuteur indique, par exemple, être au service de votre banque et propose de débloquer votre compte ou de le sécuriser,
  – **un sms** contenant, ou non, un lien vers un site internet,
- **Privilégiez les moyens de paiement sécurisés** (e-Carte Bleue, Paylib, Secur'Pass, etc.).

Consultez régulièrement nos conseils en matière de sécurité sur le site de votre banque.

Que faire si j'en ai été victime ?

Faites immédiatement opposition à votre carte bancaire sur votre application mobile, en appelant le numéro fourni par votre banque, ou à défaut le 0 892 705 705 (ouvert 7 jours/7 et 24h/24 , numéro surtaxé) et conservez la référence de votre opposition. Si vous ne pouvez pas mettre en opposition votre carte rapidement, désactivez le paiement à distance ou les retraits sur votre appli mobile ou sur l'espace internet.

- Alertez votre banque au plus vite et demandez le remboursement.
- Déposez une plainte auprès de la gendarmerie ou de la police nationale, qui vous demandera la référence de votre opposition.
- Si possible, signalez la fraude auprès de la plateforme gouvernementale PERCEVAL.

Les mesures de sécurité optimales sont appliquées au site internet et à l'application mobile de votre banque, et prennent en compte l'évolution des risques et des méthodes des fraudeurs.

Votre conseiller clientèle reste votre interlocuteur privilégié pour vous apporter tous les conseils en matière de sécurité, et pour vous guider et vous accompagner dans vos démarches.

Escroquerie

Faux noms, manœuvres frauduleuses, l'escroquerie est le fait d'obtenir un bien, un service ou de l'argent par une tromperie. Pour vous prémunir contre ce danger en pleine expansion, Banque Populaire Bourgogne Franche-Comté vous partage ses bonnes pratiques.

Les principales escroqueries recensées

Les faux appels

L'ingénierie sociale fait référence à des pratiques de manipulation psychologique à des fins d'escroquerie. Les arnaques au faux support technique, faux fournisseurs, faux banquiers, avocats ou commissaires aux comptes…l'attaquant cherche à abuser de la confiance, de l'ignorance et de la crédulité des personnes possédant ce qu'il souhaite obtenir. Chaque contact aura pour objectif un changement de coordonnées bancaires avant

l'envoi d'un virement inhabituel ou de faire ouvrir un lien dangereux contenant un virus.

Les faux placements financiers / bitcoins

Ils consistent à proposer aux victimes, démarchées par téléphone, de réaliser des investissements en bitcoins ou en euros sur de faux sites internet faisant rapidement apparaître des plus-values promises et assez importantes. Les fonds des victimes sont ensuite virés sur des "comptes bancaires rebonds" ouverts dans divers États de l'Union Européenne avant d'être transférés rapidement sur des comptes hors UE et donc difficilement récupérables.

Les fausses petites annonces

Il s'agit du paiement de marchandises via des chèques volés, paiements via Western Union, vente en urgence, arnaque PayPal, règlement supérieur au montant de base…

Escroquerie sentimentale

Les escrocs approchent les victimes généralement sur des sites de rencontre, mais aussi via les médias sociaux ou par courriel afin de les amadouer, les séduire dans le but de leur soutirer de l'argent.

La fraude 419 (aussi appelée scam 419…)

Un inconnu – ou quelqu'un se faisant passer pour un ami – demande votre aide pour transférer des fonds sur un compte étranger (par exemple, un héritage). Il vous promet une forte récompense à condition que vous lui fassiez d'abord parvenir une avance en argent. Bien entendu, la victime qui a versé son argent ne reçoit jamais un seul centime et n'entend plus parler de cet « ami ».

La fraude au président

Elle consiste à l'escroc de se rapprocher des services comptables en se faisant passer pour le dirigeant sous couvert d'une opération requérant « discrétion » et à solliciter un virement dans l'urgence à destination de comptes ouverts par l'escroc dans une banque étrangère.

FRAUDE AU PRÉSIDENT

La fraude au Président consiste à piéger un collaborateur habilité à effectuer les paiements de l'entreprise, le but étant qu'il paie une fausse facture ou réalise un transfert d'argent non autorisé.

COMMENT ÇA MARCHE ?

Par téléphone ou courriel, un fraudeur se fait passer pour un dirigeant de la société ou un directeur administratif et financier.

Les fraudeurs connaisssent bien l'entreprise ciblée.

L'arnaqueur réclame un paiement urgent.

Les expressions courantes utilisées: «confidentialité», «la société vous fait confiance».

Ils font référence à une situation sensible (par ex. contrôle fiscal, fusion, acquisition).

L'arnaqueur demande des paiements internationaux vers des banques en dehors de l'Europe.

L'employé transfère les fonds vers un compte géré par le fraudeur.

Le collaborateur est invité à ne pas respecter les procédures d'autorisation prévues dans l'entreprise.

COMMENT DÉTECTER L'ARNAQUE ?

- Contact direct d'un dirigeant avec lequel vous n'êtes normalement pas en contact
- Demande inhabituelle contraire aux procédures internes
- Demande de confidentialité absolue
- Menaces ou flatteries / promesses de récompense inhabituelles

QUE FAIRE EN CAS DE TENTATIVE D'ESCROQUERIE ?

SI VOUS ÊTES DIRIGEANT/E D'UNE SOCIÉTÉ

Soyez attentif/ve aux risques et assurez-vous que les collaborateurs soient conscients de ce type de risque.

Invitez votre personnel à la prudence concernant les demandes de paiement.

Prévoyez des protocoles internes pour les paiements.

Prévoyez une procédure pour vérifier l'authenticité des demandes de paiement reçues par courriel.

Ne dérogez jamais aux procédures que vous avez mises en place.

Contrôlez les informations publiées sur le site de votre société, limitez-les et soyez prudent/e vis-à-vis des médias sociaux.

Actualisez et améliorez la sécurité technique du process de validation d'un paiement.

Contactez toujours la police en cas de tentative de fraude, même si vous n'êtes pas tombé/e dans le piège.

SI VOUS ÊTES COLLABORATEUR

Appliquez strictement les procédures de sécurité prévues pour les paiements et les acquisitions. **Ne sautez aucune étape et résistez à la pression.**

Vérifiez toujours attentivement les adresses courriel lorsque vous traitez des informations sensibles / paiements.

En cas de doute sur un ordre de transfert, **consultez un collègue compétent.**

N'ouvrez jamais de liens / documents attachés douteux reçus par courriel. Soyez très vigilant/e lorsque vous vérifiez vos courriels privés sur un ordinateur de la société.

Limitez les informations et soyez attentif/ve en ce qui concerne les médias sociaux.

Ne partagez pas d'informations sur la hiérarchie dans l'entreprise, la sécurité ou les procédures.

Si vous recevez un courriel ou appel douteux, informez toujours votre service informatique.

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · POLICE NATIONALE · FÉDÉRATION BANCAIRE FRANÇAISE · #CyberScams

La fraude au RIB/IBAN

Elle consiste à un changement frauduleux des coordonnées de paiement d'un fournisseur au profit d'un tiers escroc ou complice.

FRAUDE AU RIB/IBAN

COMMENT CELA SE PASSE-T-IL ?

- Une entreprise est contactée par quelqu'un prétendant être un fournisseur.
- Il peut y avoir plusieurs approches combinées : téléphone, lettre, courriel, etc.
- L'escroc demande que les données bancaires (du bénéficiaire) pour le paiement des futures factures soient modifiées. Le nouveau numéro de compte donné est contrôlé par l'escroc.

QUE FAIRE ?

EN TANT QU'ENTREPRISE

Assurez-vous que vos **collaborateurs soient informés et attentifs** à ce type de fraude et sachent s'en prémunir.

Recommandez au chargé de paiement des factures de **toujours vérifier que celles-ci ne présentent pas d'irrégularités.**

Prévoyez plusieurs personnes pour valider un paiement important.

Prévoyez une **procédure pour vérifier** l'authenticité des demandes de paiement (par ex. contrôle de la réalité de la prestation, historique des relations avec le fournisseur...).

Surveillez les informations publiées sur le site de votre entreprise et évitez de parler de vos contrats et de vos fournisseurs. Veillez à ce que vos collaborateurs limitent les informations sur la société qu'ils partagent sur les réseaux sociaux.

Mettez en place des **formations sécurité** pour votre service financier et comptable.

EN TANT QUE COLLABORATEUR

Vérifiez toutes les demandes supposées émaner de vos créanciers, surtout si vous êtes invité/e à modifier leurs données bancaires pour les paiements à venir.

Pour les paiements au-delà d'un certain seuil, **prévoyez une procédure pour confirmer** le numéro de compte et le bénéficiaire (par ex. une réunion avec la société).

N'utilisez pas les données de contact reprises dans les lettre/fax/courriel demandant des modifications. Réutilisez celles de **précédents messages.**

Après le paiement d'une facture, **informez le destinataire** par courriel. Par sécurité, indiquez le nom de la banque du bénéficiaire et les quatre derniers chiffres du compte utilisé.

Prévoyez **un point de contact unique dédié** auprès des sociétés auxquelles vous faites des versements **réguliers.**

Limitez les informations sur votre employeur **que vous partagez** sur les médias sociaux.

Rapportez toujours à la police toute tentative de fraude, même si vous n'en avez pas été victime.

EUROPOL EC3 European Cybercrime Centre — EBF — POLICE NATIONALE — FÉDÉRATION BANCAIRE FRANÇAISE — #CyberScams

Le Quishing

QR hameçonnage

Le Quishing est essentiellement une forme d'attaque par hameçonnage qui utilise astucieusement les codes QR pour inciter les utilisateurs à visiter des sites web malveillants. Lorsqu'un utilisateur scanne un code QR malveillant, son navigateur se rend sur le site web indiqué par le code QR.

Que se passe-t-il si vous scannez un code QR frauduleux ?

Les codes QR sont conçus comme un moyen simple et peu encombrant de diriger les utilisateurs vers un site web. Au lieu de saisir une URL, l'utilisateur peut scanner le code QR à l'aide de l'appareil photo de son appareil mobile. Une application compatible avec le code QR peut décoder l'image en une URL qui peut ensuite être ouverte dans le navigateur de l'utilisateur.

La visite d'un site web malveillant par le biais d'un code QR a les mêmes conséquences possibles sur l'utilisateur et son appareil que s'il l'avait visité par d'autres moyens, par exemple en cliquant sur un lien dans un courriel d'hameçonnage. Le site de hameçonnage peut être conçu pour inciter l'utilisateur à entrer ses identifiants de connexion ou à installer des logiciels malveillants sur son appareil.


C'EST QUOI ?
LE QUISHING
LE PHISHING PAR QR CODE
Vous trouvez un QR code dans un lieu public, collé sur : la table d'un bar, un parcmètre, une borne de recharge, une affiche, un ascenseur, un point information.
Vous scannez le QR code :
• Soit on vous demande de saisir des informations personnelles ou bancaires.
• Soit on vous renvoie sur un faux site.
• Soit vous téléchargez un fichier infecté.
ATTENTION
Le QR code détourné permet à l'escroc de récupérer vos données ou votre argent.
RESTEZ VIGILANTS
• Vérifiez l'URL de la page web vers laquelle vous êtes dirigés
• Méfiez vous des indices comme un QR code sur un autocollant
Bureau Prévention et Protection