

ALERTE AUX NOUVELLES ARNAQUES CYBER

À l'affût de vos habitudes et des nouvelles technologies, les escrocs se dotent d'outils techniques, bravent les systèmes de sécurité et vous manipulent brillamment pour obtenir vos données personnelles et vous dépouiller. Gare à leurs nouvelles arnaques.

Faux conseiller bancaire, deepfake ou encore QR Code frauduleux, les escrocs ne manquent pas d'imagination lorsqu'il s'agit de nous soutirer de l'argent. Ces professionnels de la manipulation jouent sur les peurs, la confiance et l'inattention des gens pour s'emparer de leurs données et de leur argent. Ils les contactent directement, se présentant comme un conseiller antifraude de leur banque, et puisent du côté des innovations techniques avec l'IA. Un nouvel outil précieux, fort utile pour usurper l'identité de personnalités. Le quotidien reste également une source d'inspiration pour leurs escroqueries. En témoigne la génération de QR Codes frauduleux.

Un Français sur deux

52 % des Français, soit plus d'un sur deux, auraient déjà été victimes d'une tentative d'arnaque aux données bancaires et 8 % reconnaîtraient

s'être fait piéger par ce type de pratique, d'après une étude de la Fédération bancaire française. La fraude aux moyens de paiement scripturaux représenterait « à peu près 1,2 milliard d'euros par an. Une masse qu'il faut rapporter à 42 000 milliards d'euros de paiements annuels », précise Julien Lasalle, secrétaire de l'Observatoire de la sécurité des moyens de paiement.

Face aux escrocs, les autorités ne sont pas en reste. « On n'est jamais à court d'idées, comme les fraudeurs, on est assez inventifs », indique Julien Lasalle. Organismes et institutions multiplient ainsi les sensibilisations à l'égard de la population. Et à l'instar de la loi Naegelen, des moyens concrets sont également mis en place pour faire face aux arnaques. Cette loi de 2020, dont certains principes n'ont pas encore été mis en application, impose notamment aux opérateurs l'authentification des numéros de téléphone. Sans compter que « les forces de sécurité ne sont pas inactives, même si on n'en parle pas beaucoup. Elles ont récemment démantelé iSpooof, un site utilisé par les escrocs pour leurs arnaques. Il y a des arrestations », rappelle Jean-Jacques Latour, directeur d'expertise chez Cybermalveillance, la plateforme gouvernementale d'assistance et de prévention du risque du numérique. La vigilance reste cependant de mise. Pour ne pas se faire piéger, il est nécessaire de bien connaître les nouvelles pratiques des escrocs, que nous précisons dans ce dossier. ■ **Adrienne Chupin**



3300 €

Il s'agit du **montant unitaire moyen de la fraude au faux conseiller bancaire** par virement.

Source : Observatoire de la sécurité Financière et bancaire

280 000

demandes d'assistance

ont été enregistrées par la plateforme Cybermalveillance en 2023.

Source : CIP ANOVA, rapport d'activité 2023

1,2 milliard

C'est à peu près ce que représente chaque année **la fraude aux moyens de paiement scripturaux.**

Un chiffre qu'il faut rapporter à 42000 milliards d'euros de paiements annuels.

Source : Observatoire de la sécurité des moyens de paiement



LES ARNAQUES

BANCAIRES	P. 38
PAR DEEPFAKE	P. 41
AU QISHING	P. 42
LES RECOURS	P. 43

Je reçois
un message
de mon banquier

Surtout,
ne communiquez jamais
vos codes d'accès
personnels.

EN PRATIQUE

Aucun vrai conseiller ne vous demandera vos identifiants. Il n'en a pas besoin pour intervenir sur vos comptes. Aussi convaincant soit votre interlocuteur, ne divulguez donc jamais ces informations. De même, ne validez aucune opération bancaire lorsque vous êtes au téléphone.

DE FAUX CONSEILLERS QUI VIDENT VOS COMPTES

Prisée des escrocs ces derniers temps, la fraude au faux conseiller bancaire fait chaque jour de nouvelles victimes. Explications.



C'est l'escroquerie du moment : l'ancien juge antiterroriste Jean-Louis Bruguière et sa femme peuvent en témoigner. À l'instar de nombreux Français, le couple a été victime d'un faux conseiller bancaire qui leur a fait perdre près de 200 000 euros. Une arnaque autrefois marginale qui s'est fortement développée ces dernières années. Chiffres à l'appui, Jean-Jacques Latour, directeur d'expertise chez Cybermalveillance, parle de « véritable phénomène. Au second semestre 2022, la fraude au faux conseiller représentait 1 400 demandes d'assistance sur la plateforme. On est passé à plus de 5 000 en 2023, soit une augmentation de presque 80 % ».

« Ils lavent le cerveau des gens »

Si cette arnaque fonctionne autant, c'est parce qu'elle repose sur un fort degré de manipulation. Les escrocs « lavent le cerveau des gens en les prenant dans un tourbillon qui leur fait perdre tout sens commun et critique », lance Jean-Jacques Latour. Leur mode opératoire est à la fois simple

**Cette arnaque repose
sur un fort degré
de manipulation.**

et recherché. L'arnaqueur appelle sa victime en faisant du *spoofing* (voir encadré), il usurpe ainsi le numéro de la banque de l'intéressée. Il se présente comme un conseiller du service antifraude et informe que des mouvements suspects ont été détectés sur ses comptes. Au choix, d'importantes transactions vers l'Afrique ou l'Europe de l'Est. Si sa proie émet des doutes, l'escroc la met en confiance. Il lui dit qu'elle peut vérifier que le numéro qui s'affiche sur son téléphone est bien celui de sa banque et la bombarde ensuite d'informations personnelles obtenues grâce à des techniques dites d'« ingénierie sociale », tel un préalable *phishing* (voir encadré), pour finir de la convaincre. La personne est alors sous pression. Elle a peur de voir son argent disparaître, mais l'arnaqueur est là pour la rassurer. « Il se présente comme un sauveur », indique le directeur d'expertise de Cybermalveillance. À partir de là, il va chercher à se procurer mots de passe et identifiants bancaires, demander de valider des opérations pour annuler des transactions, voire de transférer les fonds sur un nouveau compte dit « sécurisé ». Il fait alors ajouter un nouveau bénéficiaire à sa victime, l'IBAN étant à son nom, celle-ci ne se méfie pas. Elle est ensuite poussée

**On n'appelle
pour mettre à jour
mes informations**

*Vérifiez l'émetteur!
N'hésitez pas
à raccrocher puis
à rappeler.*

EN PRATIQUE

Lorsque vous recevez un appel, vérifiez à qui vous avez affaire. Pour cela, quand bien même le numéro affiché est celui de votre conseiller, n'hésitez pas à raccrocher puis à rappeler pour vous assurer que vous n'êtes pas victime de *spoofing* (lire l'encadré).

1234 5678 90

**Mon conseiller
m'envoie un lien,
par mail ou SMS**

*Dans tous les cas
de figure,
ne cliquez pas !*

EN PRATIQUE

Partez du principe que tous les liens sont suspects. Donc, ne cliquez pas. Pour consulter les derniers messages de votre banque, accédez à vos comptes avec votre appli bancaire ou un navigateur.

LEXIQUE DU PHISHING AU SPOOFING

Célèbre et répandu, le *phishing*, aussi connu sous le nom d'« hameçonnage », reste une mine d'or pour les escrocs. Via des liens envoyés par mail ou par SMS, ils implantent des virus appelés « infostealers » dans les appareils des utilisateurs ou les renvoient vers des sites plus vrais que les originaux. Logos, charte graphique, codes de sécurité avec le fameux cadenas vert en haut de page : tout est fait pour tomber dans le panneau et permettre aux arnaqueurs de récolter diverses données personnelles (nom, mots de passe, identifiants bancaires...). Des informations dont ils se servent ensuite dans leurs combines, notamment au travers du *spoofing* : une technique qui consiste à usurper l'identité d'un émetteur. Très populaire chez les escrocs, elle peut revêtir différentes formes, permettant entre autres d'afficher n'importe quel numéro de téléphone sur l'écran de la victime, souvent celui d'une institution comme la banque. L'objectif est de la mettre en confiance avec un numéro qu'elle connaît pour mieux l'arnaquer. Et pour finir de convaincre leur proie qu'elle a affaire au bon interlocuteur, les fraudeurs la bombardent ensuite de renseignements obtenus lors du *phishing*.

à envoyer son argent sur le compte rattaché à cet IBAN pour le sauver. En réalité, le compte où sont déplacés les fonds ne lui appartient pas. Ce n'est pas parce que vous rentrez un IBAN en le mettant à votre nom que le compte qui y est associé vous appartient car « *actuellement, il n'y a pas de concordance des IBAN. C'est-à-dire qu'il n'y a pas de tests de cohérence entre le nom d'un bénéficiaire que l'on va ajouter et l'IBAN auquel il va être associé* », explique Julien Lasalle, secrétaire de l'Observatoire de la sécurité des moyens de paiement.

Une organisation bien huilée

Les transferts de fonds ne sont pas le seul moyen utilisé par les escrocs pour dérober de l'argent. Certains vont en plus chercher à récupérer les cartes bancaires de leurs cibles, ce qui donne parfois lieu à de véritables et invraisemblables scènes de films. Dans l'affaire du juge, entre autres, ils ont exigé que les cartes soient découpées, déposées dans une enveloppe et confiées à un taxi appartenant à une société en partenariat avec la banque attendant en bas du domicile. L'idée est de faire croire à la victime qu'elle a détruit les cartes. En réalité, ce n'est pas le cas. Ils auront demandé que « *la carte bleue soit coupée dans le sens de la largeur, de manière assez précise, pour pouvoir la recoller ensuite. Puis ils vont faire le tour des distributeurs* » ■ ■ ■



LES ARNAQUES PAR DEEPFAKE



DES PEOPLE MIS EN SCÈNE POUR VOUS PIÉGER

L'IA est un bel outil, les escrocs l'ont remarqué. Ils l'utilisent désormais pour l'une de leurs nouvelles arnaques, le deepfake de célébrités.

**ANNE-CLAIRE
COUDRAY**

présentatrice du JT de TF1, mise en scène dans un deepfake vidéo pour vanter les mérites d'une appli de jeu d'argent, soit disant lancée par le chanteur Maître Gims.



mais dans l'apparence qu'il peut revêtir », explique Jean-Jacques Latour, docteur en expertise chez Cybermalveillance. Ce dernier le considère en quelque sorte comme une « nouvelle forme de l'arnaque au président ». Une escroquerie où l'identité, la voix d'une personne connue, faisant autorité, étaient utilisées pour escroquer des gens.

« Les deepfakes sont très faciles à générer »

Les deepfakes ne sont pas toujours bien réalisés comme « la vidéo de Kylian Mbappé qui restait encore assez grossière, mais ils tendent à se développer », d'après Jean-Jacques Latour. D'autant plus qu'ils « sont très faciles à générer », indique Florent Curtet, cofondateur de Hackers Sans Frontières et directeur de l'agence de cybersécurité NEO Cyber. Il précise : « Plus l'empreinte numérique de la personne est forte, plus c'est simple et l'IA générera un deepfake performant ». Pour créer un deepfake, il suffit « de quelques photos et vidéos prises sur les réseaux sociaux et d'un minimum de vingt secondes de la voix de la personne, qui peut en partie se trouver sur son répondeur ». L'émergence de l'IA a facilité la création de deepfakes en la rendant accessible à tous. « Canteloup fait cela depuis des années, remarque Jean-Jacques Latour. Mais quand il a commencé, il fallait des moyens de production comme ceux de TF1. Tandis que maintenant... » ●

Kylilan Mbappé, Anne-Claire Coudray ou encore Omar Sy, ces personnalités ont toutes fait l'objet de deepfakes. Ces vidéos truquées qui mettent en scène une célébrité vantant les mérites d'un produit, d'une marque, etc. Les escrocs prennent ici de vrais extraits vidéo issus de journaux télévisés ou des réseaux sociaux. Ils y modifient ensuite le discours et le mouvement des lèvres pour que celui-ci colle aux propos rapportés. Ils utilisent alors le pouvoir d'influence que ces stars ont sur leur public. Celui-ci, mis en confiance par une personnalité de son quotidien, un artiste ou un sportif qu'il apprécie, va acheter le produit ou se rendre sur le site et se fera ainsi piéger. Il s'agit d'un procédé qui « n'est pas inédit sur le plan de la méthode,

EN PRATIQUE

Vérifiez l'adresse web vers laquelle vous êtes redirigé : elle doit être officielle. Dans tous les cas, au moindre doute, à la moindre faute d'orthographe, ne flashez pas !

Je suis invité à flasher

Vérifiez d'abord l'URL d'arrivée !

DES QR CODES QUI ASPIRENT VOS DONNÉES

Les escrocs ont trouvé un nouveau moyen de récolter vos infos personnelles : le faux QR Code. Mais comment fonctionne cette arnaque qui tend à se développer ?

Après les liens par SMS et par mails, les escrocs s'attaquent au QR Code. Le scan de ce carré blanc et noir est entré dans les habitudes des Français avec la pandémie de Covid-19. Aujourd'hui, celui-ci est omniprésent, dans la rue, sur les bornes de recharge électriques, au restaurant ou encore derrière certains emballages alimentaires et cosmétiques. Les arnaqueurs ne sont pas passés à côté de cette nouvelle pratique et ils l'utilisent désormais pour récolter vos données.

Dans vos mails, à l'extérieur, dans les banques... le *quishing*, fruit du mélange entre le QR Code et le *phishing*, est partout et requiert une vigilance particulière. Récemment, certains faux QR Codes ont pris la forme de stickers collés sur des vrais. Difficile de ne pas tomber dans le piège. Une fois scanné, il renvoie vers un site frauduleux ressemblant trait pour trait à une page officielle. Reprenant parfois même l'esthétique d'institutions ou d'entreprises connues de tous. La seule différence se trouve généralement dans l'URL

du site, qui, à une lettre près, peut différer de l'adresse originale. Une fois sur le site, la personne est incitée à y entrer un certain nombre de données qui seront ensuite enregistrées (nom, identifiants, mots de passe, etc.). Le scan de ces QR Codes frauduleux peut aussi entraîner « l'installation de virus, d'infostealers, qui enregistreront directement les informations des gens », précise le hacker éthique Florent Curtet.

Un outil de phishing facile à fabriquer

Si le QR Code séduit autant les escrocs, c'est aussi parce qu'il est très simple à générer. Il suffit de « taper "générateur de QR Code en ligne" dans votre moteur de recherche, et de cliquer sur "créer un QR Code". Vous ajoutez le site web sur lequel vous voulez qu'il renvoie, le design, et ça va le générer automatiquement », explique Florent Curtet. Une fois qu'il est créé, il ne reste plus qu'à le disposer un peu partout ou à l'envoyer à ses cibles. ●

L'ÉCLAIRAGE DE FLORENT CURTET, hacker éthique

“ L'escroquerie s'est industrialisée ”

Ceux qui cherchent à vous soutirer de l'argent ne sont pas tous des as en informatique. Ils ont à leur disposition

des solutions clés en main, comme nous l'explique Florent Curtet, cofondateur de Hackers Sans Frontières et directeur de l'agence de cybersécurité NED Cyber.

« Aujourd'hui, il est très facile de se lancer dans l'escroquerie ; ce n'est pas que ça s'est démocratisé, mais industrialisé ! Les escrocs passent par des sites peu recommandables, leur permettant d'acheter un type de phishing ou d'arnaque. Ces sites vont fournir un domaine,

toute une méthodologie à respecter et un virus qui sera indétectable. Ceux qui ont moins d'argent peuvent aussi louer ces services. Ils sont alors hébergés par des pirates qui créent un tableau de bord propre, avec page d'accueil, options... Il y a en outre le développement de l'IA,

COMMENT RÉAGIR QUAND IL EST TROP TARD ?

Voici les recours auxquels vous pouvez prétendre pour récupérer votre argent ou du moins en limiter la perte. Vous avez tout intérêt à agir au plus vite.

FAIRE OPPOSITION

En cas de fraude, **n'attendez pas et faites opposition le plus rapidement possible.**

Cette action bloquera immédiatement paiements ou prélèvements.

ANNULER LE VIREMENT

Il s'agit d'un rappel des fonds.

Cette procédure peut vous permettre de récupérer au moins une partie de votre argent. Votre banque joint la banque destinataire des virements frauduleux, et s'ils sont encore sur le compte en question, celle-ci les renverra à votre banque.

ANNULER LE PAIEMENT PAR CARTE

Appelé « rétrofacturation », **ce dispositif vous permet de revenir sur votre ordre de paiement** et d'être remboursé par le réseau de votre carte bancaire (Visa ou autre) ou par votre banque.

RECOURIR À UN MÉDIATEUR

À la suite d'une demande de remboursement infructueuse auprès de votre banque, vous pouvez faire appel à un médiateur. **Celui-ci va chercher et proposer des solutions** pour résoudre votre litige.

PORTER PLAINTE

Le dépôt de plainte **ouvre la voie à une enquête policière** et peut donc, sans garantie toutefois, vous permettre de récupérer vos biens et éviter que d'autres ne soient victimes des mêmes escrocs que vous.

ALLER AU TRIBUNAL

Si tous les recours ont été épuisés, **vous pouvez toujours tenter une action en justice** devant les tribunaux sans garantie qu'elle aboutira.

LES ADRESSES À RETENIR

CYBERMALVEILLANCE

Sur cette plateforme d'assistance de prévention face au risque numérique, vous trouverez des informations sur les arnaques, comment s'en prémunir ou encore des conseils techniques sur les marches à suivre lorsqu'il est trop tard.

www.cybermalveillance.gouv.fr

PERCEVAL

Via Perceval, vous pourrez opérer un signalement pour fraude à la carte bancaire. Attention, il ne dispense pas de porter plainte.

bit.ly/3wxjog5

avec plusieurs modules qui sont copiés sur ChatGPT, comme Fraude GPT, globalement spécialisés dans la mise en place d'arnaques très sophistiquées ou dans la création de virus. En revanche, ce qui reste dur techniquement aujourd'hui, c'est par exemple de rendre un infostealer indétectable

par l'antivirus ou le pare-feu. Mais là encore, il existe des plateformes qui proposent des solutions techniques spécialement prévues pour les arnaques. Elles se louent ou s'achètent, plus ou moins cher, seules ou par pack. Et n'importe qui, vous, moi, un gamin de 15 ans, peut se les procurer.

En échange de 50 €, vous obtenez une plateforme toute prête. Il n'y a plus qu'à diffuser le virus par des QR Codes, SMS, mails... Il n'y a aucune technicité derrière tout ça*.

* L'escroquerie est un délit passible de cinq ans de prison et 375 000 € d'amende, et jusqu'à dix ans de prison et un million d'euros si elle a été commise en bande organisée.

POURQUOI MA BANQUE REFUSE-T-ELLE DE ME REMBOURSER ?

Si, des suites d'une fraude, « près de 85 % des demandes adressées par les clients en cas d'opérations de paiement par carte contestées » sont remboursées par les banques, le remboursement n'est pas automatique et chaque cas nécessite une instruction du dossier, rappelle la Fédération bancaire française (FBF). Et dans certains cas, les victimes ne parviennent pas à récupérer leur argent auprès de leur banque. La FBF rapporte cinq raisons pouvant conduire à un non-remboursement.

« Certaines contestations ne sont pas justifiées car elles ont pour origine un litige commercial. »

Un différend avec un commerçant doit être réglé avec ce dernier ou devant les tribunaux.

« Parfois, la victime a fait preuve de négligence grave. »

Ne communiquez jamais à qui que ce soit vos codes de carte, identifiants ou mots de passe.

« Les victimes se manifestent parfois hors des délais légaux. »

Pour une fraude à la carte bancaire, par exemple, « vous devez signaler la fraude à votre banque au plus tard treize mois après la date de débit », rappelle le site du ministère de l'Économie.

« Incomplètes ou erronées, les contestations ne sont pas exploitables. »

Au moment de votre demande, veillez à n'oublier aucun des documents ou preuves demandés par votre établissement bancaire pour le remboursement.

« En mentant, les victimes rendent de fait leur demande de remboursement illégitime. »

Soyez toujours rigoureux et de bonne foi lors de vos réclamations.