Se connecter

Proposer un contenu

Identifiant
Identifiant

Mot de passe
Mot de passe

Connexion automatique

Se connecter

Pas de compte ? S'inscrire...

Journal : BPCE et les paiements avec authentification à deux facteurs

4 avr. 2022

65

Posté par **Glandos** le 04 avril 2022 à 21:59. **Licence CC By-SA.**
Étiquettes : **banque**, **paiement**, **3dsecure**, **dsp2**, **bpce**, **credit_cooperatif**

Je suis scandalisé. Voilà.

Depuis quelques semaines, ma banque me prévient qu'ils vont activer l'authentification à deux facteurs lors des paiements. Ça ne m'inquiète pas plus que ça, j'ai déjà ça chez Boursorama depuis récemment, et ça se passe à peu près comme ça :

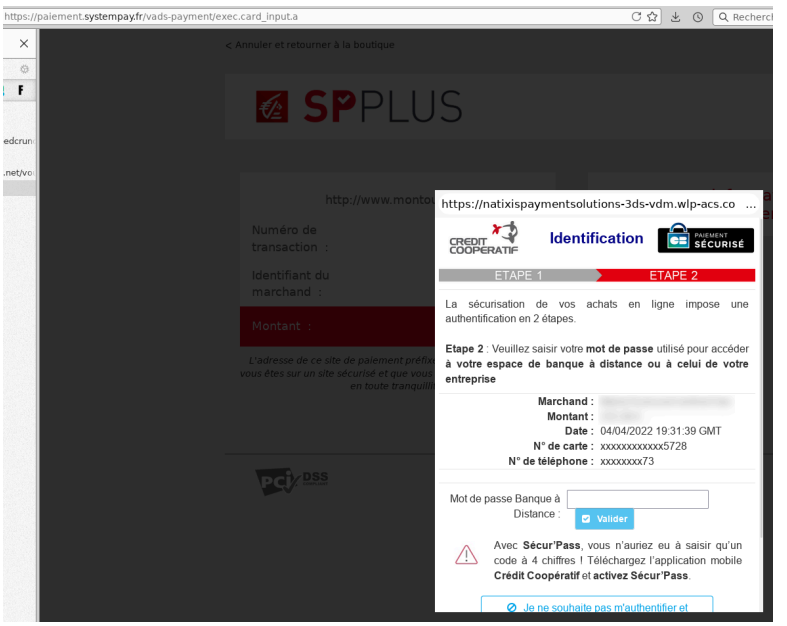
1. On rentre ses informations de carte sur le site marchand.
2. 3D-Secure se met en marche, avec une *iframe*, et celle de Boursorama dit qu'il faut se connecter sur son espace client, dans un nouvel onglet.
3. Sur l'accueil de l'espace client apparaît le paiement avec le détail.
4. Pour valider le paiement, il y a l'envoi d'un SMS ou d'un courriel.
5. Retour sur l'onglet du paiement, c'est validé.

C'est un peu fastidieux, mais je sais que la sécurité a un prix, et franchement, ça me semble difficile de faire plus simple en restant sécurisé.

Aujourd'hui, je dois payer autre chose avec mon compte chez Crédit Coopératif, groupe BPCE. Et ça se passe comme ça :

1. On rentre ses informations de carte sur le site marchand.
2. 3D-Secure se met en marche, avec une *iframe*, et celle de Crédit Coopératif dit qu'il faut rentrer le code reçu par SMS.
3. Après, il y a une deuxième étape, **toujours dans le même contexte** disant qu'il faut rentrer son mot de passe.
4. Je ne suis pas allé plus loin.

Oui, il faut rentrer son mot de passe de connexion à sa banque dans une fenêtre de site marchand. Parfois, c'est pire, c'est dans une fenêtre de prestataire de paiement, qui inspire une très douteuse confiance :



Mon navigateur a ouvert `systempay.fr` (c'est qui ?), dans laquelle il y a une *iframe* qui me **fait croire** que mon navigateur affiche la barre d'adresse (c'est une fausse, émulée) qui affiche un nom de domaine même pas entier, mais qui fait partie de `wlp-acs.com`. J'en ai déjà parlé maintes fois, c'est un nom de domaine qui n'a rien à voir avec ma banque, le site sur lequel je paie, le prestataire de paiement qui intègre l'*iframe*, et qui s'amuse à mettre le logo de ma banque dedans.

J'ai passé un temps de dingue à expliquer à mon entourage non technophile les méandres des arnaques sur Internet, ce qui est louche de ce qui ne l'est pas. Il y a des arnaques vachement bien montées pour lesquelles il faut sortir des requêtes `dig` et `whois` avec un peu de `curl -v` pour les débusquer. Et là, tout ce que je vois, c'est un massacre de cette éducation, avec tout ce qu'il ne faut pas faire. Ou en tout cas, tout ce qu'il faut faire pour brouiller les lignes entre ce qui peut être de confiance et ce qui ne l'est pas.

Je suis scandalisé. Voilà.

(75 commentaires). Markdown EPUB

Qui est wlp-acs...

Posté par **Pinaraf** le 04 avril 2022 à 22:40. Évalué à 10.

> wlp-acs, en non-abrégé World Line Payment - Access Control Server, est le service de contrôle d'accès fourni par Atos et utilisé par (toutes ?) les banques françaises pour l'implémentation, côté banque, d'ACS. Cette page n'est absolument pas liée au site marchand. Par contre, de là à l'admettre comme étant une page de sa banque sur laquelle on peut sereinement saisir son code... non, faut pas déconner.
>
> Sinon systempay est un PSP comme il en existe tant, un prestataire de services de paiement, qui donne une API simple pour éviter à tous les commerçants d'avoir à être certifié PCI-DSS et d'avoir à implémenter une horreur type CB2A.

[^] # Re: Qui est wlp-acs...

Posté par **Glandos** le 04 avril 2022 à 22:46. Évalué à 10.

> Et pourquoi ce n'est pas expliqué sur le site du marchand avant ? Et pourquoi ce n'est pas banque qui me le dit ? Pourquoi l'utilisateur doit faire confiance à une pile d'acteurs sans aucune information ?
>
> La confiance, ça se mérite.

[^] # Re: Qui est wlp-acs...

Posté par **Pinaraf** le 04 avril 2022 à 22:59. Évalué à 10.

> > Et pourquoi ce n'est pas banque qui me le dit ?
>
> Tu serais rassuré de savoir que 3DS dépend de serveurs aux US (je sais plus pour quel service de 3DS) ?
> Tu serais rassuré de savoir que les banques françaises se déconnectent de swift au fur et à mesure pour plutôt mutualiser/centraliser l'accès chez un nombre de guichets swift limité ?
>
> > La confiance, ça se mérite.
>
> Aie confiance, crois en eux :)

[^] # Re: Qui est wlp-acs...

Posté par **Glandos** le 04 avril 2022 à 23:06. Évalué à 10.

> Tu serais rassuré de savoir que 3DS dépend de serveurs aux US (je sais plus pour quel service de 3DS) ?

D'après Wikipédia : https://fr.wikipedia.org/wiki/3-D_Secure[w]

> 3-D Secure a été développé par Visa et MasterCard

Donc oui, évidemment, c'est américain. Ça fait longtemps que je le sais, ça fait longtemps que je trouve que 3D Secure est une mauvaise implémentation, de base. Mais là, c'est un pas de plus, qui est d'autant plus exaspérant qu'il touche au cœur de la confiance : le fameux mot de passe. Enfin, le code numérique de longueur fixe. Ahahah.

[^] # Re: Qui est wlp-acs...

Posté par **StyMaar** le 07 avril 2022 à 00:27. Évalué à 4.

> Une remarque en passant, parce que plein de gens n'en ont pas conscience: 3D-Secure c'est un produit commercial de Visa et Mastercard **à destination des commerçants** et destinée à **réduire le nombre d'impayés**, ce n'est pas une protection pour le client mais pour le vendeur vis-à-vis d'une opposition de la part de son client.

[^] # Commentaire supprimé

Posté par **Anonyme** le 11 mai 2022 à 11:51.
Évalué à 1.

> *Ce commentaire a été supprimé par l'équipe de modération.*

[^] # Re: Qui est wlp-acs...

Posté par **Glandos** le 11 mai 2022 à 12:22.
Évalué à 5.

> Oui et non. Je laisse les professionnels en parler : https://aide.trainline.fr/article/215-verification-3d-secure
>
> > À part rendre l'achat plus pénible, la vérification 3DSecure ne change pas grand chose pour vous. Elle est là pour protéger le commerçant, car c'est à lui de rembourser les victimes en cas d'utilisation frauduleuse d'une carte bancaire. Avec ou sans 3DS, la transaction sera toujours aussi sécurisée pour vous.

[^] # Re: Qui est wlp-acs...

Posté par **Christie Poutrelle** (**site web personnel**) le 05 avril 2022 à 10:01. Évalué à 9.

> Va expliquer que la base du 3D-secure c'est une communication n-tiers (en l'occurrence ici n est 3, j'ai implémenté un client 3D-secure pour DataCash il y a longtemps) sur des connexion chiffrés SSL ou TLS avec des échanges de tokens bidirectionnels de tokens entre chacune des parties. C'est complexe et chiant. Dans la pratique, le site marchant peut remplacer l'iframe par une redirection pour l'utilisateur, l'iframe ne fait que rendre le truc encore plus flou et bancale à mon avis.

[^] # Re: Qui est wlp-acs...

Posté par **bbo** le 05 avril 2022 à 21:20. Évalué à 4.

> > est le service de contrôle d'accès fourni par Atos
>
> Petite précision : Worldline [w] est désormais une entreprise indépendante d'Atos (depuis mai 2019).
>
> Et pour systempay, le whois indique Natixis [w] (groupe BPCE).

[^] # Re: Qui est wlp-acs...

Posté par **Astaoth** le 30 avril 2022 à 20:17. Évalué à 2.

Pour l'anecdote Natixis reste lié à Atos, c'est la banque qu'ils utilisent pour les épargnent salariales.

--

Emacs le fait depuis 30 ans, et sans pubs ni télémétrie.

On se sent moins seul

Posté par **Glaeken** (**site web personnel**) le 05 avril 2022 à 05:55.
Évalué à 10. Dernière modification le 05 avril 2022 à 05:55.

J'ai eu exactement la même réaction que l'auteur du journal.
J'aide fréquemment ma mère pour faire ses achats sur le net, elle est chez BPCE.
La première fois que j'ai été confronté à ce problème, je n'en croyais pas mes yeux : un site inconnu demandait à ma mère de saisir le mot de passe qu'elle utilise pour consulter son compte bancaire en ligne (en plus du traditionnel code reçu par SMS).
La transaction s'est arrêté là et j'ai pagayé ferme avec ma mère pour lui expliquer pourquoi je ne pouvais pas acheter ses tickets de musée en ligne.
Si l'utilisation d'un code jetable reçu par sms me semble raisonnable, je ne vois pas en quoi saisir son précieux mot de passe bancaire sur un autre site que celui de sa banque pourrait sécuriser quoi que ce soit.
Au contraire, il me semble que saisir ses mots de passe sur des sites inconnus est par définition une mauvaise pratique qui ne peut conduire qu'à des tentatives d'usurpation d'identité.
Je n'avais pas remarqué que l'iframe falsifiait en plus la barre d'adresse mais finalement, ce n'est pas très étonnant, compte tenu de la débilité globale de la démarche.
Alors, je me suis renseigné et sur le site de la banque, j'ai vu qu'il fallait installer une application sécurisée qui authentifierait le payement sans avoir à saisir ce mot de passe. Fantastique, sauf que ma mère n'utilise pas de smartphone, elle a un simple téléphone portable bâton sans Androïd ni Ios. Impossible d'installer leur application sécurisé, et ça doit être le cas pour toutes les personnes qui n'ont pas de "smartphone". Ils sont plus nombreux qu'on le croit, beaucoup plus nombreux qu'on le croit.

N'ayant pas d'autres solutions, on saisit désormais son précieux mot de passe un peu partout, quand il faut régler un achat, et puis elle croise les doigts pendant que moi, je serre les fesses.

Et je vous passe les cas difficiles, comme par exemple :
- Lorsqu'il y a un timer de 10 minutes pour valider la transaction, et que le site vous demande de rentrer au préalable les noms, prénoms, adresse, date de naissance des 5 personnes qui vont visiter le musée + les numéros de CB + le SMS + le mot de passe bancaire.
- Lorsque vous validez la transaction dans l'iframe de payement, que l'iframe vous affiche fièrement "Transaction autorisé" et vous renvoie sur le site marchand qui vous annonce "Votre banque a refusé le payement". Dans ce cas, il n'y a plus qu'à attendre une semaine en vérifiant si oui ou non le montant a été prélevé sur votre compte et recommencer si rien n'a été prélevé.
On vit une époque formidable, formidable.

[^] # Re: On se sent moins seul
Posté par **Zenitram** (**site web personnel**) le 05 avril 2022 à 08:29. Évalué à -10. Dernière modification le 05 avril 2022 à 08:30.

[^] # Re: On se sent moins seul
Posté par **devnewton** 🍺 (**site web personnel**) le 05 avril 2022 à 08:55. Évalué à 10. Dernière modification le 05 avril 2022 à 08:56.

> Mais perso je note que Boursorama, une banque en ligne qui cible des gens plus éduqués sur la technologie, s'intéresse bien plus aux gens sans smartphone (leur processus est prévu pour) que nombre de banques "traditionnelles" avec plein de vieux ayant des difficultés avec la technologie, il doit bien y avoir une raison derrière.

Normal, les gens éduqués sur la technologie ne veulent pas d'applications privatrices sur leur téléphone.

Et même les gens normaux vu que ce n'est pas pratique de jongler entre deux périphériques.

--

Le post ci-dessus est une grosse connerie, ne le lisez pas sérieusement.

[^] # Re: On se sent moins seul
Posté par **cypX** le 05 avril 2022 à 09:57. Évalué à 10.

> Sinon, le journal est assez trompeur, pou ce que je connais, chez Boursorama pour la grande majorité de leur clients :
>
> On rentre ses informations de carte sur le site marchand.
> 3D-Secure se met en marche, avec une iframe, et celle de Boursorama dit qu'il faut regarder son smartphone.
> Pour valider le paiement, on met son doigt sur le capteur du smartphone qui va bien, on a l'habitude.
> L'onglet du paiement, resté affiché, dit automatiquement que c'est validé.

Je crois que tu passes à coté de l'avertissement principal de ce journal, la solution prévoit que l'on fournissent ses identifiants bancaires à un site qui n'est pas sa banque et qui utilise des solutions dangereuse pour faire croire que c'est le cas.
Alors certes la validation via le smartphone est moins risqué mais puisque son contournement est prévu dans le dispositif on ne peut pas dire qu'elle améliore significativement la sécurité. Sur un site e-commerce piraté, il suffira par exemple que la fausse iframe indique qu'elle a bien envoyé la demande à l'application, si il ne se passe rien l'utilisateur sera tenté de cliquer sur le lien utilisant la solution SMS (qui enverra un faux SMS) pour terminer son achat.

A noter que j'ai vu le même fonctionnement chez la Banque Postale (les identifiants du site sont demandé) mais qu'en revanche au Crédit Agricole il m'ont fournit un mot de passe distinct dédié à cet usage (au moins si il est détourné on n'aura pas le contrôle complet de mes comptes, on pourra "uniquement" alléger mes comptes du montant plafond de carte comme avec le fonctionnement précédent...).

[^] # Re: On se sent moins seul

Posté par **Zenitram** (**site web personnel**) le 05 avril 2022 à 10:58. Évalué à -10. Dernière modification le 05 avril 2022 à 11:00.

[^] # Re: On se sent moins seul

Posté par **sebas** le 05 avril 2022 à 11:21. Évalué à 10.

> Le mieux plutôt que de balancer des phrases génériques alors qu'on n'a aucune idée de ce que les gens croient ou pas tout comme on n'a aucune idée de la réalité, c'est de donner des nombres, surtout quand une recherche de 30 secondes donne des nombres, c'est plus factuel et plus un outil pour débattre

Le mieux, quand on répond à quelqu'un, c'est de ne pas faire ce qu'on lui reproche et d'être comme toi catégoriquement catégorique, et de faire comme si tu étais le maître absolu de la vérité que tu distilles complaisamment aux imbéciles qui ne pensent pas comme toi.

Il se trouve par exemple que je n'ai pas de spyphone justement parce que j'ai quelques notions d'informatique et que je n'aime pas du tout ce que je vois. Et, à ce que je sache, je ne compte pas dans les pourcents que tu cites, personne n'est venu me sonder pour voir si j'en avais un ou non.

Il se trouve aussi que ma femme, qui n'a pas autant de prévention que moi au sujet de ce truc, en a suffisamment pour se refuser à installer toute appli bancaire sur un engin dont tout le monde sait que c'est un aspirateur de tes données personnelles, et que n'importe quel dictateur du XXe siècle aurait rêvé d'avoir le quart de la moitié du dixième des infos que google ou apple possède sur toi, sans oublier les devs d'une bête appli de lampe de poche, laquelle se permet, d'après ce que j'ai lu ici, de demander des permissions aberrantes et pas en relation avec les besoins réels de cette appli.

Elle non plus ne compte pas dans tes pourcents. Et elle n'est sûrement pas la seule (désolé, je n'ai pas de sacro-saints pourcents à te proposer).

> Désolé, mais oui, je ne regrette absolument pas le "avant", aujourd'hui je fais tellement plus de choses en tellement moins de temps (entre autres grâce aux smartphones ;-)).

Et bien moi, vois-tu, j'en regrette une bonne partie, par exemple, des acteurs privés ont accès à des données qu'il y a encore peu de temps, il était anticonstitutionnel de fournir sans raison à la police (les empreintes digitales associées à son identité, ça ne se faisait qu'en cas de procédure judiciaire ou policière), que le moindre site marchand que je visite par spyphone en sait plus sur moi que mon employeur au siècle dernier, que je n'arrive plus à expliquer le chemin pour venir chez moi sans qu'on me demande "c'est quoi ton point gps" ou pire "envoie-moi ton google-maps par whatsnaze", que je ne peux plus aller dans un endroit public sans voir une nuée de gogos faire des sourires crétins et forcés le bras tendu, et pire encore, à obliger leurs gamins de 2 ans à faire la même chose, et donc les habituer à passer leur vie en représentation.

Quant à la praticité dont tu parles, je passe une après-midi pour pouvoir acheter un billet d'avion, alors que dans l'"avant" que tu conchies, il me suffisait d'aller chez un agent de voyage et c'était torché en 20 mn (OK, on payait probablement les billets plus chers, mais les raisons sont autres). Quant aux sites marchands mal faits qui plantent ou retournent à la page de début après une heure de galère dans le labyrinthe de leurs pages...

Et on sait qu'on aura jamais de dictateur en France, pays de la liberté, mais quand ça arrivera, bonjour les dégâts. Je pense que les Russes doivent actuellement goûter au plaisir de voir l'État connaître beaucoup plus ce qu'ils sont et ce qu'ils pensent qu'au temps de Staline.

Bref, il y a sûrement des trucs plus pratiques maintenant qu'au siècle passé, mais le spyphone n'en est pas un, ou plus exactement ce qu'il amène de praticité est fortement empoisonné et se paye très cher. Et pas seulement en terme de surveillance (je pense aussi à la non-sollicitation de la mémoire, aux prises de décisions plus difficiles en mode autonome, au raisonnement horizontal, au mode de communication globalement plus superficiel, etc.)

[^] # Re: On se sent moins seul

Posté par **Glaeken** (**site web personnel**) le 05 avril 2022 à 15:21. Évalué à 0.

Restons calmes, la réponse si catégorique postée par "Zenitram" me semble trop proche d'une tentative de (bon vieux) troll à l'ancienne pour que ça vaille le coup d'hausser ne-serait-ce qu'un sourcil.
Sa réponse m'a même fait doucement sourire, étant donné que les chiffres en question, je les connais parfaitement et je n'ai nul besoin d'aller faire une recherche internet pour me les remémorer.
Mais merci quand même à Zenitram pour son précieux conseil, je n'aurais jamais pensé à aller chercher des chiffres sur internet tout seul !

Il se trouve que ça fait partie de mon job de connaitre ce type de statistiques, lol.

Si je ne les cite pas dans mon commentaire, c'est justement pour titiller l'intérêt des lecteurs afin qu'ils se renseignent sur le sujet par eux-mêmes, ce qu'a fait Zenitram, visiblement : objectif atteint.

Un peu de lecture pour terminer, plein de jolis chiffres bien précis si chers au compère Zenitram !

Rapport de la Défenseure des Droits - Dématérialisation des services publics : trois ans après où en est-on ? (PDF, 2 Mo)

[^] # Re: On se sent moins seul

Posté par **Stéphane Ascoët** (**site web personnel**) le 11 mai 2022 à 11:14. Évalué à 2.

Content de lire Sebas, même si j'aurais encore bien d'autres méfaits des idiotphones à ajouter à sa liste. Pour l'instant, le Crédit Coopératif me demande encore d'utiliser le terminal qu'ils avaient fourni originellement et quant à Paypal, après moultes difficultés, on peut saisir le code par téléphone fixe. Le document PDF a l'air de dénoncer plein de choses fort justement mais bon... encore un rapport qui a certainement fini dans la poubelle d'un des sous-fiffres de macron...

[^] # Commentaire supprimé

Posté par **Anonyme** le 11 mai 2022 à 11:59. Évalué à -1.

[^] # Commentaire supprimé
Posté par **sebas** le 05 avril 2022 à 11:21. Évalué à 2.
Dernière modification le 05 avril 2022 à 11:51.

> *Ce commentaire a été supprimé par l'équipe de modération.*

[^] # Re: On se sent moins seul
Posté par **sebas** le 05 avril 2022 à 11:40. Évalué à 3.
Dernière modification le 05 avril 2022 à 11:44.

> Pourquoi mon message est-il sorti deux fois ???
> Si un modo passe par ici, est-ce qu'il pourrait supprimer une des deux copies (elles sont parfaitement identique, je n'ai cliqué qu'une fois sur le bouton d'envoi. Ou alors je suis bien bourré !). Merci.

[^] # Re: On se sent moins seul
Posté par **gUI** (**Mastodon**) le 05 avril 2022 à 11:52.
Évalué à 5. Dernière modification le 05 avril 2022 à 11:52.

> Fait !
>
>
>
> Perso je penche pour la 2e hypothèse :)
>
> --
>
> En théorie, la théorie et la pratique c'est pareil. En pratique c'est pas vrai.

[^] # Re: On se sent moins seul
Posté par **sebas** le 05 avril 2022 à 16:46.
Évalué à 0.

> Y a des gens qui moinsent vraiment n'importe quoi. J'aimerais bien connaître la motivation de celui qui t'a moinsé pour avoir supprimé un message sur ma demande.
>
> Je te rassure, ça n'est pas moi (au contraire), je suis content de mon essat, euh, je buis sien conscient de mon état, euh, enfin, je pas ne suis vexé, d'ailleurs, mercips ;-)
>
> (même chose, j'ai un message plus bas qui donne la combine de gnirehtet pour pouvoir éviter le wifi qui a été moinsé deux fois, je me demande vraiment pourquoi ; d'autres de mes messages plus polémiques, je peux encore comprendre, mais une combine technique sur un petit soft libre et excellent, gratgrat (pas que ça me dérange, c'est juste de la curiosité)).

[^] # Re: On se sent moins seul

Posté par **Gil Cot** ✔ (**site web personnel**, **Mastodon**) le 05 avril 2022 à 16:51. Évalué à 4.

> Bienvenue sur LinuxFr ; tu comprendras vite que c'est parfois à la tête du pseudo et au cycle lunaire ou que sais-je. Mais ne vas surtout pas critiquer ; les gens ne mettent pas que c'est impertinent pour dire qu'ils ou elles n'aiment pas (ta personne) ou ne sont pas d'accord avec ton propos. :-/
>
> --
>
> “It is seldom that liberty of any kind is lost all at once.” — David Hume

[^] # Re: On se sent moins seul

Posté par **gUI** (**Mastodon**) le 05 avril 2022 à 17:02. Évalué à 5. Dernière modification le 05 avril 2022 à 17:02.

> Dans le cas de mon message ce serait peut-être pour la remarque sur ton alcoolisme présumé, jugée déplacée par le moinseur ?
>
> --
>
> En théorie, la théorie et la pratique c'est pareil. En pratique c'est pas vrai.

[^] # Re: On se sent moins seul

Posté par **bbo** le 06 avril 2022 à 09:05. Évalué à 7.

> ou peut être que le moinseur ou la moinseuse était bourré(e) aussi !

[^] # Re: On se sent moins seul

Posté par **fearan** le 06 avril 2022 à 13:30. Évalué à 4.

> Perso je penche pour cette hypothèse :)
>
> --
>
> Il ne faut pas décorner les boeufs avant d'avoir semé le vent

[^] # Re: On se sent moins seul

Posté par **Ysabeau** (**site web personnel**, **Mastodon**) le 05 avril 2022 à 17:54. Évalué à 1. Dernière modification le 05 avril 2022 à 17:54.

> Ça m'est arrivé une fois, et je n'ai pas encore compris pourquoi. Je ne bois que du thé et de la chicorée :-)
>
> --
>
> « Tak ne veut pas qu'on pense à lui, il veut qu'on pense », Terry Pratchett, Déraillé.

[^] # Re: On se sent moins seul

Posté par **Glandos** le 05 avril 2022 à 11:37. Évalué à 8.

> Effectivement, je n'ai pas de smartphone, pour ceux qui suivent ;)
>
> Et même si j'en avais un, je n'installerai pas l'application de ma banque. Que ce soit celle de Boursorama Banque ou du Crédit Coopératif, c'est enfreindre les règles de base de la sécurité informatique : la compartimentation. L'application d'authentification à deux facteurs devrait ne faire que ça. Rien d'autre.
>
> Et dans ces applications, il y a du code que les banques elles-mêmes ne maîtrise pas. Le smartphone est très loin d'être une solution. Les jetons matériels RSA existaient depuis bien longtemps. Le T-OTP est standardisé et existe dans plein d'implémentation open-source. La solution ne peut pas être retenue dans le cadre des transactions bancaires car le contexte est requis, mais honnêtement, il y a également ce que fait Cozy Cloud ou Scaleway : l'envoi d'un jeton ou lien unique par courriel. Car quand on paie sur Internet, on a normalement accès à son compte de messagerie. Mais pas forcément à son téléphone.

[^] # Re: On se sent moins seul

Posté par **Zenitram** (**site web personnel**) le 05 avril 2022 à 12:03. Évalué à -5. Dernière modification le 05 avril 2022 à 12:04.

[^] # Re: On se sent moins seul

Posté par **Glandos** le 05 avril 2022 à 12:24.
Évalué à 10.

> T-OTP était un truc bien à une époque du offline, complètement hors sujet ici où on fait du push en indiquant le nom du commerçant et le montant, et où on a juste à appuyer sur "j'approuve" (communication bidirectionnelle), pas à se faire chier à entrer un code à la main

Oui, avec Bitwarden, je ne le rentre pas à la main. C'est très facile. Mais là, ma banque me l'envoie par SMS, c'est très fastidieux. Sinon, la solution du lien cliquable dans le courriel, c'est encore mieux. J'ai juste à lire et à cliquer.

> "avant on avait un agent de voyage, c'était mieux", d'une il en existe toujours et de 2 personne ne les a interdits, s'il y en a moins c'est juste que les gens trouvent ça dépassé

Il y a le contre-exemple de la SNCF. Quand on va sur le site en ligne, on trouve difficilement ce qu'on veut. Quand on va en gare, il y a trop peu de guichets d'ouverts pour la masse de gens qui patientent. La conclusion est que les gens **veulent** des humains, mais que l'entreprise qui les paye trouve sûrement ça trop cher, et supprime ces postes. Ce n'est pas dépassé, c'est trop cher.
Dans un bureau de La Poste aujourd'hui, il y a des gens qui nous expliquent comment se servir d'un automate.

La technologie est une solution, mais c'est une solution pour travailler moins, par pour faire faire aux utilisateurs le travail pour lequel l'entreprise ne veut plus payer : l'agent de voyage est capable de trouver en moins de deux minutes un Savigny-sur-Orge -> Bangkok -> Lima. Maintenant, c'est à l'utilisateur d'apprendre à se servir du logiciel de l'entreprise, qui est certes plus performant, mais c'est quand même à lui de faire le travail.

[^] # Re: On se sent moins seul

Posté par **Zenitram** (**site web personnel**) le 05 avril 2022 à 12:50. Évalué à -2. Dernière modification le 05 avril 2022 à 12:54.

[^] # Re: On se sent moins seul

Posté par **Ysabeau** (**site web personnel**, **Mastodon**) le 05 avril 2022 à 17:55. Évalué à 4.

>
>
> Dans un bureau de La Poste aujourd'hui, il y a des gens qui nous expliquent comment se servir d'un automate.

Et, du coup, tu fais la queue devant l'automate… c'est pas mieux.

--

« Tak ne veut pas qu'on pense à lui, il veut qu'on pense », Terry Pratchett, Déraillé.

[^] # Re: On se sent moins seul

Posté par **Gil Cot** ✔ (**site web personnel**, **Mastodon**) le 05 avril 2022 à 20:45. Évalué à 0.

>
>
> Mais l'automate tu lui gueule pas dessus comme certaines personnes, et tu te plaindras pas de sa froideur (même si je trouve, perso, les humain-e-s qui tirent la tronche plus rassurant-e-s en tout cas pas encore déshumanisé-e-s) en plus de finir par faire le boulot toi-même et de payer pour cela. Les pauvres derrière les guichets n'ont plus qu'à traverser la rue comme dit leur président (qui a trouvé l'Élysée en traversant.)
>
> --
>
> "It is seldom that liberty of any kind is lost all at once." — David Hume

[^] # Re: On se sent moins seul

Posté par **Stéphane Ascoët** (**site web personnel**) le 11 mai 2022 à 11:25. Évalué à 2. Dernière modification le 11 mai 2022 à 11:28.

> La conclusion est que les gens veulent des humains

Je n'en suis hélas absolument pas persuadé, au contraire même, mais pas pour les mêmes raisons que Zenitram, qui a un discours profondément capitalisto-égoiste que je n'ai pas le courage de démonter ici. C'est à cause de gens comme lui qu'on vit dans un monde de merde. Par exemple, on préfère donc payer les ex-employés des guichets à rester chez eux au chômage avec toutes les conséquences sociales induites qu'à travailler. Mais Mr Zenitram pensera payer son billet de train moins cher...

> Dans un bureau de La Poste aujourd'hui, il y a des gens qui nous expliquent comment se servir d'un automate.

L'autre jour il y en a un qui a grondé une dame(d'un niveau social clairement faible) parce qu'elle venait demander de l'aide pour comprendre son compte bancaire plutôt que d'utiliser l'application sur idiotphone...

Je suis tellement heureux de lire ta dernière phrase, pour une fois que ce n'est pas moi qui le dit... on est quand même quelques uns à réfléchir encore un peu en ce monde...

Et pour les technologies d'OTP dont vous parlez, etc. sachez que LaNef est enfin(une fois de plus...) à deux centimètres de devenir une vraie banque. Et si des pro du sujet comme vous s'y impliquaient pour leur conseiller les bonnes pratiques?

[^] # Re: On se sent moins seul

Posté par **sebas** le 05 avril 2022 à 14:10. Évalué à 5.
Dernière modification le 05 avril 2022 à 14:12.

> et vous laisser entre vous en victime des méchants (ça m'a bien fait sourire le coup de "avant on avait un agent de voyage, c'était mieux", [...] si il y en a moins c'est juste que les gens trouvent ça dépassé

Quand on veut noyer son chien etc. Facile d'interpréter à ton goût ce que les autres disent pour ensuite prouver que tu avais raison. Lis mieux ce que j'ai écrit, je ne disais pas que les agences de voyage étaient mieux ou moins bien, je répondais juste à ton affirmation de praticité (et je soulignais que les billets étaient plus chers) :

> > Quant à la praticité dont tu parles, je passe une après-midi pour pouvoir acheter un billet d'avion, alors que dans l'"avant" que tu conchies, il me suffisait d'aller chez un agent de voyage et c'était torché en 20 mn

Après, s'il n'y en a plus, c'est aussi parce qu'il y a un forcing tous azimuts pour habituer les gens à travailler pour le compte de l'agent de commerce (self-service dans les pompes à essence et les supermarchés dans les années 1960, auto-payement aux caisses des supermarchés dans les années 90, auto-choix du matos à acheter (par navigateur) sans l'aide (certes discutable) du vendeur dans les magasins, auto-choix des trajets dans l'achat des billets ou des transhumances touristiques, enfin... On fournit un travail gratuit pour avoir le droit de payer, si tu trouves ça normal et pratique, eh bien pas moi. Ça n'est pas refuser le progrès que de critiquer ses excès, je ne pense pas être un vieux croûton qui refuse la technologie, si c'était le cas que ferais-je ici à mouler ? (en vrai, si, je peux en critiquer beaucoup d'aspects, mais pas au motif qu'avant c'était mieux, mais au motif que la direction que prend l'organisation de la société est fortement suspecte, et c'est une toute autre discussion).

Uber est moins cher que les taxis le temps de tuer la pratique des taxis, ensuite il sera plus cher. C'est ce qui s'est déjà passé avec les supermarchés vs petits commerces et les agences de voyage vs achat par web. Ce qui explique en grande partie la disparition de ces dernières.

D'ailleurs, puisque tu n'as pas lu mon message (ou juste ce qui t'en intéressait pour essayer de me ridiculiser) :

> > Bref, il y a sûrement des trucs plus pratiques maintenant qu'au siècle passé, mais le spyphone n'en est pas un, ou plus exactement ce qu'il amène de praticité est fortement empoisonné et se paye très cher.

[^] # Re: On se sent moins seul

Posté par **devnewton** (**site web personnel**) le 05 avril 2022 à 16:18. Évalué à 10. Dernière modification le 05 avril 2022 à 16:18.

> Au lieu de faire caliméro, tu pourrais remarquer les autres problèmes de l'appli mobile comme second facteur d'authentification:
>
> - c'est de la dématérialisation à base de matériel spécifique ;
> - les deux facteurs se retrouvent sur le même périphérique facile à voler/perdre.
>
> --
>
> Le post ci-dessus est une grosse connerie, ne le lisez pas sérieusement.

[^] # Re: On se sent moins seul

Posté par **GG** (**site web personnel**) le 07 avril 2022 à 16:28. Évalué à 2.

> > > c'est enfreindre les règles de base de la sécurité informatique : la compartimentation. L'application d'authentification à deux facteurs devrait ne faire que ça. Rien d'autre.
>
> Sur ça, on sera d'accord, je n'aime pas du tout cette idée (surtout que du coup ça casse le principe de double authentification, faudra que le régulateur se penche

> sur ça un jour...), mais pas trouvé de banque acceptable qui compartimente. On 'est pas asse nombreux à trouver ça utile, la il va falloir compter sur le régulateur qui à la base demande 2 authentifications.

J'ai acheté un nouveau smartphone pour pouvoir y installer tous les scrapware bancaires dont j'ai besoin, et pour bien les séparer avec mon autre smartphone.

Sachant que sur Android il est possible d'activer le profil professionnel, donc, sur le nouveau je vais même pouvoir cloisonner un peu.

Et, j'ai un utilisateur NextCloud pour chacun, avec évidement un dossier partagé entre ces "utilisateurs" et moi, un pour chacun. Du coup, ça me permet de séparer mes activités pro et perso.

Bon, je reconnais, ça coûte plus cher, puisqu'il faut acheter un smartphone rien que pour ça.

--

Pourquoi bloquer la publicité et les traqueurs : https://greboca.com/Pourquoi-bloquer-la-publicite-et-les-traqueurs.html

[^] # Re: On se sent moins seul

Posté par **jihele** le 05 avril 2022 à 14:51. Évalué à 4.

> Le T-OTP est standardisé et existe dans plein d'implémentation open-source. La solution ne peut pas être retenue dans le cadre des transactions bancaires car le contexte est requis

Tu saurais détailler ça ?

Je râle depuis longtemps sur le 2FA pour les accès aux sites bancaires ou aux paiements sur internet parce que ça nécessite un téléphone (SMS), voire une appli (parce que SMS est pas assez sécurisé).

Chez Paypal, j'utilise OTP. Dans mon profil j'ai demandé un numéro qui doit faire une dizaine de caractères et que je donne à une appli

(libre) d'OTP pour me connecter. Ce mécanisme ne convient-il pas ?

[^] # Re: On se sent moins seul

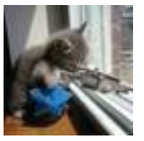
Posté par **Glandos** le 05 avril 2022 à 15:24.
Évalué à 6.

> Alors je n'ai pas de sources, mais ça fait partie de la DSP2 qui introduisait et « normalisait » l'usage d'un deuxième facteur d'authentification, notamment pour les paiements, **mais avec la contextualisation**. Ça veut dire que lors de l'envoi du jeton, il doit y avoir les détails de la transaction associée. Et ça, ce n'est pas possible avec T-OTP, puisqu'il n'y a que le jeton, il ne peut pas y avoir le montant, le bénéficiaire, etc.

[^] # Re: On se sent moins seul

Posté par **claudex** le 05 avril 2022 à 19:23.
Évalué à 6.

> > Alors je n'ai pas de sources, mais ça fait partie de la DSP2
>
> Article 97, paragrahe 2 de la DSP2: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32015L2366 (le gras est de moi):
>
> > > En ce qui concerne l'initiation des opérations de paiement électronique visée au paragraphe 1, point b), les États membres veillent à ce que, pour les opérations de paiement électronique à distance, les prestataires de services de paiement appliquent l'authentification forte du client comprenant des éléments qui établissent **un lien dynamique entre l'opération, le montant et le bénéficiaire donnés**.
>
> --
>
> « Rappelez-vous toujours que si la Gestapo avait les moyens de vous faire parler, les politiciens ont, eux, les moyens de vous faire taire. » Coluche



[^] # Re: On se sent moins seul

Posté par **Nodeus** le 05 avril 2022 à 15:27. Évalué à 6.

Chez BPCE pour les Achat avec authentification à deux facteurs, vous pouvez demander un lecteur cap qui permet de générer un code que vous pouvez taper sur le site de la banque et donc pas de problème si vous ne possédez pas de smartphone.

Ce lecteur vous sera facturé 19€ si je me souviens bien. Demandez à votre conseillé bancaire.

Ce lecteur vous évite le téléchargement de l'appli voir l'achat d'un smartphone.

[^] # Re: On se sent moins seul

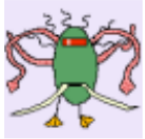
Posté par **Stéphane Ascoët** (**site web personnel**) le 11 mai 2022 à 11:29. Évalué à 1. Dernière modification le 11 mai 2022 à 11:30.

Dire qu'à l'époque je l'avais eu gratuitement... vive le progrès.

Et je n'évoque même pas l'impact écologique désastreux du double-idiot-phone, du terminal OTP par banque, etc.

[^] # Re: On se sent moins seul

Posté par **le_silmarillion** le 07 avril 2022 à 11:40. Évalué à 3.



Dans la même situation avec mon père qui n'a pas de smartphone et moi qui a une LineageOS non-reconnu par l'application comme sécurisé (et donc délégue à Google la sécurité du terminal)... Les solutions proposé par les deux banques sont:
1. l'envoie par courrier d'un code (fixe) à saisir en plus à l'issu du SMS de validation (Crédit Agricole)
2. l'envoie d'un terminal de paiement à la maison (si j'ai bien compris le dispositif et facile à installer), tu fais ta commande, à la validation par SMS, puis tu utilise ta carte comme au magasin. Pas de configuration à faire sur l'ordianteur... (Caisse Épargne)

Bon courage !!!

Et dans les zones blanches ?

Posté par **Philippe F** (**site web personnel**) le 05 avril 2022 à 10:14. Évalué à 10.

> Je réagis sur cette partie de ton message qui laisse filer un troll bien involontaire:
>
> > Pour valider le paiement, il y a l'envoi d'un SMS ou d'un courriel.
> > C'est un peu fastidieux [...] mais ça me semble difficile de faire plus simple en restant sécurisé.
>
> Bof.
>
> J'habite à la campagne. Dans mon jardin, je capte péniblement l'antenne SFR du village (située à trois kilomètres). Je suis passé chez SFR exprès pour ça, les autres étant catastrophiques. Dans la maison aux murs épais à l'ancienne, le réseau ne passe pas ou très mal. Quand il pleut, pas de réseau dans la maison et un seul endroit dans le jardin où je capte.
>
> Malgré ça, j'ai un accès ADSL pas trop mal et il m'arrive de commander des trucs sur internet ou de payer tout simplement la cantine de mes enfants. En ai-je le droit ? C'est pas sûr... Le fameux SMS du Crédit Coopératif met entre 2 minutes et 20 minutes à arriver jusqu'à mon téléphone. Pour un paiement qui expire en cinq minutes ! Je fais souvent ce type de paiement le soir et je suis moyennement motivé pour sortir dans la nuit sous la pluie juste pour recevoir mon SMS.
>
> C'est un peu mieux avec l'application dédiée, il semble que la consommation en bande passante soit plus faible qu'un SMS. Ah oui, parce qu'on aime pas les ondes chez moi, donc on active le wifi qu'en situation de nécessité. Et un téléphone n'a pas de moyen de se connecter au nain ternet autrement qu'en wifi.
>
> Bref, en vivant depuis quelques années à la campagne, je découvre à quel point notre monde dit moderne est très centré sur le mode de vie des citadins/banlieusards et complètement ignorant ou méprisant des réalités de la campagne.

[^] # Re: Gnirehtet

Posté par **sebas** le 05 avril 2022 à 10:47. Évalué à 9. Dernière modification le 05 avril 2022 à 10:48.

Je n'ai pas de wifi chez moi pour une raison différente, je n'ai pas envie de voir traîner cette cochonnerie dans toute la maison, l'informatique, c'est dans le bureau, point à la ligne. De plus, quand des amis viennent à la maison, ça leur fait une cure de désintox, et on peut discuter sans avoir besoin de voir les photos débiles de leur dernière dose de tourisme, ou de voir cet engin surgir au cours de discussions pour connaître des détails inintéressants, style la date de naissance de Churchill parce qu'on parle du rôle de l'UK durant la 2e GM.

Alors une bonne nouvelle pour toi, il y a un petit utilitaire libre qui marche très bien et qui permet de faire du reverse tethering, c'est à dire que c'est l'ordi qui passe la connexion au spyphone par usb. Et du coup ce dernier a un fil à la patte et ne sort plus du bureau que pour sortir de la maison. :-p

C'est ici : Gnirehtet. La dernière actualisation est d'août 2020, mais c'est tout simplement parce qu'il n'y a pas eu besoin d'actualiser depuis, j'ai vu passer 2 actualisations suite à des difficultés de connexion venant de changements dans android. Bravo et grand merci à Romain, l'auteur, s'il passe par ici.

[^] # Re: Gnirehtet

Posté par **sebas** le 05 avril 2022 à 11:29. Évalué à 6.
Dernière modification le 05 avril 2022 à 11:32.

> > quand des amis viennent à la maison, ça leur fait une cure de désintox

PS: J'oubliais de dire que j'habite dans une zone blanche, oui, ça a quand même ses avantages. Donc, quand ils viennent chez moi, il n'y a ni 4g ni wifi.

Pour les SMS de confirmation, j'ai un téléphone avec une antenne délocalisée, mais avant que je trouve cette solution, ça n'était pas du tout pratique.

[^] # Re: Gnirehtet

Posté par **joel** le 07 avril 2022 à 15:07. Évalué à 1.

Merci beaucoup pour l'info, sebas.
Même moi, qui ne comprend pas l'anglais, et qui n'ai aucune formation en informatique, j'ai pu l'installer et l'utiliser...

[^] # Re: Gnirehtet

Posté par **Stéphane Ascoët** (**site web personnel**) le 11 mai 2022 à 11:33. Évalué à 1.

Ça m'interresserait aussi mais je n'ai rien compris sur la page Web de l'outil, il doit manquer des étapes pour les idiotphonophobes comme moi.

[^] # Re: Gnirehtet

Posté par **Astaoth** le 30 avril 2022 à 20:33. Évalué à 2.

> Alors une bonne nouvelle pour toi, il y a un petit utilitaire libre qui marche très bien et qui permet de faire du reverse tethering, c'est à dire que c'est l'ordi qui passe la connexion au spyphone par usb. Et du coup ce dernier a un fil à la patte et ne sort plus du bureau que pour sortir de la maison. :-p C'est ici : Gnirehtet.

Ah ? Ce n'est pas Network Manager ?

--

Emacs le fait depuis 30 ans, et sans pubs ni télémétrie.

Boîtier sésame

Posté par **quent57** le 05 avril 2022 à 12:30. Évalué à 10.

Le crédit coopératif propose aussi le boîtier sésame pour sécuriser la connexion à son espace perso et pour les paiements en ligne.

Lors de la connexion à sa banque ou de l'achat en ligne, on doit insérer sa carte dans le boîtier, composer son code CB, et le boîtier nous donne un mot de passe à usage unique (OTP) à 8 chiffres.

Cela oblige donc :
- à avoir sa CB lors d'un achat en ligne
- à connaître le code de la CB
- et à avoir le boîtier avec soi (le plus contraignant).

J'adore le principe d'obliger a posséder la CB (une emprunte n'est pas suffisante) et à connaître son code (voler la CB n'est pas suffisant) pour faire un achat en ligne. J'ai l'impression que c'est aussi sécurisé qu'un achat en magasin du coup.

Cela remplace le sms / l'app mobile et me semble plus sécurisé (confiance moyenne dans le réseau téléphonique et en Android ...) et plus besoin de composer son mot de passe banque lors d'un achat 3DS.

En dehors de cela, je suis d'accord sur l'absurdité de la vrai/fausse iframe...
Autant rediriger sur le site de la banque, c'est plus rassurant.

7

« Mes Comptes » est adaptée à tous les écrans, smartphones et tablettes. La dernière version de l'application a aussi gagné en confort d'utilisation et en fonctionnalités, puisqu'elle propose maintenant l'affichage des opérations en cours et des encours de carte bancaire.

En finir avec le papier
Enfin, comme près de 60 % de nos clients particuliers abonnés aux services de banque en ligne, vous pouvez vous simplifier la vie en choisissant de recevoir des relevés de compte dématérialisés. D'autant que le Crédit Coopératif a décidé de partager les économies réalisées grâce aux e-relevés. Résultat ? Si vous optez pour cette solution, votre abonnement aux services de banque en ligne vous sera remboursé.

+d'infos :
Détail des offres et conditions disponibles en agence.

Crédit Coopératif _ février 2015

[^] # Re: Boîtier sésame
Posté par **Glandos** le 05 avril 2022 à 12:39. Évalué à 7.

Je fais partie des gens qui aimeraient bien ça. Et ma compagne, qui est Belge, a baigné là-dedans.
Ils appellent ça le PC Banking, et tout le monde a un lecteur de carte chez soi. Bon, ça a peut-être changé depuis 10 ans.

En tout cas, au Crédit Coopératif, quand j'ai ouvert ce compte en 2019, on nous a dit que ce n'était disponible que pour les clients professionnels.

Je crois qu'ils ne veulent pas ;)

[^] # Re: Boîtier sésame
Posté par **Misc** (**site web personnel**) le 05 avril 2022 à 14:58. Évalué à 5.

Perso, j'ai dit à ma banque que j'ai pas de smartphone pour leur application (DSP2), et comme dit dans le prospectus, je voudrais un boitier. Je suis visiblement le seul client de Moselle qui demande ça, et j'attends encore.

La raison que je donne, c'est que le seul smartphone que j'ai est celui de mon employeur, je veux pas faire d'opérations bancaires dessus pour des raisons évidentes.

J'attends de pouvoir à nouveau voyager pour faire pareil avec ma carte pro (Bank of Ireland), mais ce coup ci en disant que j'ai pas de tel pro pour l'appli, et que je vais pas mettre une appli du boulot sur mon tel perso, donc que j'ai besoin du boitier. Je suis sur que je vais aussi attendre pendant un bout de temps :)

[^] # Re: Boîtier sésame
Posté par **quent57** le 05 avril 2022 à 15:10. Évalué à 5.
Dernière modification le 05 avril 2022 à 15:10.

> En tant que particulier, j'ai effectivement eu le boîtier en prétendant ne pas avoir de smartphone.
> Ce qui n'est pas exactement vrai, mais pas faux non plus car j'ai un Android sans les GoogleApps et il ne fait pas tourner l'appli bancaire...
> Pareil dans une autre banque, en prétendant ne pas avoir de smartphone, ils finissent par proposer un boîtier.

[^] # Re: Boîtier sésame
Posté par **claudex** le 05 avril 2022 à 19:27. Évalué à 7.

> > Bon, ça a peut-être changé depuis 10 ans.
>
>
>
> C'est toujours très répandu, même les applications sur smartphone existent aussi.
>
> --
>
> « Rappelez-vous toujours que si la Gestapo avait les moyens de vous faire parler, les politiciens ont, eux, les moyens de vous faire taire. » Coluche

[^] # Re: Boîtier sésame
Posté par **cypX** le 05 avril 2022 à 14:25. Évalué à 2.

> J'ai ça pour un compte pro Banque Populaire https://aide.bpalc.fr/articles/pass-cyberplus/ et il me semble que c'est (c'était?) assez généralisé pour les comptes pro.
>
> Par contre le souci est le même sur les paiement en ligne, il se substitue à la validation via l'application mobile mais la validation par SMS et authentification reste proposé en alternative.

[^] # Re: Boîtier sésame
Posté par **jihele** le 05 avril 2022 à 14:55. Évalué à 4.

J'utilise ça aussi (j'ai pas de mobile). J'ai un boîtier à la maison et un au bureau.

Mais je reconnais que si un jour je suis coincé quelque part et je dois acheter un billet de train par internet, par exemple, je suis emmerdé.

Et depuis quelques temps je dois l'utiliser pour entrer dans l'interface web de la banque même pour juste une consultation, ce qui est bien relou, si bien que je vérifie moins souvent mes comptes qu'avant.

[^] # Re: Boîtier sésame

Posté par **Gabbro** le 05 avril 2022 à 15:20. Évalué à 5.

J'ai pareil à la banque populaire (compte perso). On m'a envoyé le boitier quand j'ai ouvert mon compte il y a près de 10 ans, et ça marche très bien. Il faudra que je change les piles un jour, c'est tout.

Et si tu n'as pas le boitié avec toi, il y a un la possibilité de recevoir un SMS sur ton portable (je ne sais pas comment ça marche, je n'ai jamais eu à utiliser).

[^] # Re: Boîtier sésame

Posté par **Glaeken** (**site web personnel**) le 05 avril 2022 à 20:33. Évalué à 6.

Pour ma part, je suis au crédit coopératif depuis le début des années 2000. Vers 2014-2015, la banque m'a effectivement fourni un boitier sésame et à l'usage, ça marche assez bien.
Je précise qu'on m'a fourni cet outil gratuitement, sur un compte personnel sans que je n'ai rien à demander.
Les seules contraintes ont été cités dans les commentaires précédents : il faut se balader avec pour jouir du droit de dépenser ses sous, et en vacances comme en amour, le poids compte. C'est pas toujours pratique de se trimbaler la calculette sésame à l'étranger, ou sous une grosse pluie tropicale à moto.
Mais ça marche, pas besoin de connexion internet, globalement si tu as une pile bouton fonctionnelle, ta calculette sésame et le code bancaire qui va avec la carte utilisée, ça te permet d'accéder à la thune bien à l'aise, dans la limite des stocks disponibles.

Maintenant, j'ai eu quand même des déboires avec, de divers types.

Des transactions refusés malgré l'usage correct du boitier par exemple.

Ah oui, j'étais en train d'acheter un jeu sur steam (facturé au Luxembourg à l'époque) alors que j'étais physiquement localisable dans un pays fort éloigné : refus de la banque direct, lol !

[réglage du robot vérificateur de la banque en cours...]

Ah oui, la banque refuse le payement des tickets d'avion très onéreux mais dont le montant est largement inférieur au limites maximales liées à ma carte de payement. Problème rapidement réglé quand j'ai fait remarquer que la limite maximale de payement de ma carte bancaire (théoriquement dans les 7K€) était en fait limité vers les 3 000 €.

[réglage du robot vérificateur de la banque en cours..., joie d'apprendre que je paye pour pouvoir dépenser 7 k€ sans soucis chaque semaine et que ma banque me limitait en réalité à 3K€ par semaine à mon insu]

Heureusement que je n'étais pas en galère à l'étranger et qu'à aucun moment je n'ai eu l'impression d'être pris pour un con par ma banque...

Vers 2017, j'ai commencé à avoir des problèmes purement mécaniques avec le boitier sésame.

Ça a commencé tout bêtement, le boitier est équipé d'un clavier gomme (façon TO7 pour les vieilles moules) et les touches restaient enfoncées quand j'appuyais dessus, elles ne remontaient plus. Ça de venait difficile d'arriver à taper le code sans galérer mais la banque m'a renvoyé une calculette sésame toute neuve, toujours gratuitement, toujours sans compte pro'.

La nouvelle calculette marche bien, encore que...

Suite à un renouvellement de ma carte bancaire (visa), un nouveau problème est apparu, hardware ce coup-ci, visiblement...

Quand j'insère ma délicieuse carte de payement dans l'orifice du sésame, ce dernier me demande quelle fonction je souhaite mettre en branle et, quoi que je lui demande, il me réponds toujours "EMV AUTH" au début, façon sainte nitouche.

Ensuite, ça marche, je peux utiliser le sésame afin d'ouvrir les cuisses de mon compte bancaire mais il commence toujours par me dire "EMV AUTH" et disons que comme préliminaires, j'ai déjà connu mieux, nitouche.

Maintenant, la question que je me pose, c'est de savoir pourquoi la BPCE n'a jamais proposé à ma mère un boitier de ce type, peut-être parce qu'elle n'a pas un compte pro'. C'est dommage parce que ça lui aurait franchement facilité la vie.

Encore que...

Le souci, c'est qu'elle est vieille ma mère, elle y voit plus rien.
Déjà qu'elle galère pour arriver à lire le code que la banque envoie par SMS, je ne suis pas certain qu'elle arrive à recopier le code de contrôle affiché sur le boitier sésame.
Pas sur non plus qu'elle parvienne à taper son code sur les petites touches en gomme du boitier sésame.
Pas sur non plus qu'elle ne panique pas devant le superbe message "EMV AUTH" s'il se présente à elle.

Enfin, heureusement, elle n'est pas aveugle.

[^] # Re: Boîtier sésame

Posté par **xoddark** le 05 avril 2022 à 20:57. Évalué à 4.

J'ai également un boîtier pour mon compte perso au crédit coopératif créé il y a 7/8 ans je dirais. Pendant une période je l'avais avec moi tous les jours pour aller au travail, et il n'a pas trop aimé et fini par ne plus fonctionner.
J'en ai demandé un nouveau il y a 1 an ou moins, et on m'en a envoyé un sans poser de question.

Comme d'autre, j'aime bien le principe, reste la problématique de l'avoir avec soi ou pas, si on veut pouvoir valider des commandes en ligne quand on est pas chez soi.

[^] # Re: Boîtier sésame

Posté par **jsbjr** le 06 avril 2022 à 14:26. Évalué à 2.

> Est-ce que ce boitier sésame est spécifique à une carte bancaire ou il peut être utilisé avec différentes cartes?

[^] # Re: Boîtier sésame

Posté par **Glandos** le 06 avril 2022 à 14:35. Évalué à 3.

> Je crois même qu'il n'est pas spécifique à une banque. Si je ne me trompe pas (merci de me corriger sinon), il implémente un protocole de génération de jeton de validation à base :
> - d'un secret (le code de la carte)
> - d'un périphérique physique (la puce de la carte)
> - d'un code initial (fourni par le vendeur/boutique/créancier)
>
> Et le jeton final permet, par des algorithmes cryptographiques, de valider que le code initial a bien été validé par le possesseur de la carte.

[^] # Re: Boîtier sésame

Posté par **Glaeken** (**site web personnel**) le 06 avril 2022 à 17:04. Évalué à 6.

> Le boitier sésame n'est pas spécifique à une carte bancaire, j'avais fait le test.
> Les codes à 8 chiffres générés vont toujours en ordre croissant, d'après mes observations.
> Si on n'utilise pas l'un des codes générés, le suivant fonctionnera sans soucis.
> Je m'étais déjà amusé à générer des codes de réponses à l'avance, à les noter sur un bout de papier pour les utiliser sans avoir à me trimballer le boitier.
> Je me suis souvent demandé s'il y avait un nombre maximal de codes réponses qu'on pouvait sauter sans les utiliser, je suppose que oui, enfin j'espère que oui...

[^] # Re: Boîtier sésame

Posté par **quent57** le 07 avril 2022 à 14:34. Évalué à 4.

J'ai déjà utilisé un boîtier d'une banque différente, et donc d'une carte différente pour réaliser un paiement 3DSecure.
Je n'avais pas autorisé auprès de ma banque un quelconque code spécifique au boîtier comme ou pourrait le faire par une clé OTP.
J'ai l'impression que tout passe par la puce de la CB, le boîtier n'est qu'un intermédiaire pour communiquer avec elle.

[^] # Re: Boîtier sésame

Posté par **mahikeulbody** le 08 avril 2022 à 10:25.
Évalué à 2.

> Je n'avais pas autorisé auprès de ma banque un quelconque code spécifique au boîtier comme ou pourrait le faire par une clé OTP.

Du coup, quelle est la protection apportée par un tel boîtier ???

(j'avoue que je ne suis pas sûr de comprendre, ma question est donc peut-être stupide)

[^] # Re: Boîtier sésame

Posté par **quent57** le 08 avril 2022 à 12:46.
Évalué à 10.

La protection est qu'il est indispensable de posséder la CB et de connaître son code pour faire un achat 3DS sur internet, le boîtier n'est qu'un intermédiaire, l'intelligence est dans la CB.

Le fonctionnement est que
1. j'introduis ma carte CB dans le boîtier,
2. je compose mon code confidentiel
3. le boîtier envoie le code à la CB,
3.1 si c'est erroné, j'ai cramé une tentative, et au bout de 3 c'est la CB qui est cramée (comme le ferait un distributeur de billets).
3.2 si c'est le bon la puce de la CB retourne un code
4. et le boîtier m'affiche code.

Donc, pour faire l'achat 3Dsecure, j'ai besoin :

- de posséder physiquement ma carte CB (pas juste une emprunte / une photo)
- de connaître le code (et je ne peux donc pas les essayer tous)

On a bien 2 facteurs nécessaires à l'authentification forte sur les 3 possibles :
1. Ce que je sais → L'authentifiant (mot de passe) **-> le mot de passe CB**
2. Ce que je possède → un certificat, un badge ou une carte à puce **-> la CB**
3. Ce que je suis → une empreinte biométrique

Cela me convient bien car j'exclue d'enregistrer mes empreintes biométriques dans mon smartphone (possiblement vérolé), (et de toute façon l'appli de la banque ne fonctionne pas sur mon smartphone sans googleapps).

Le code SMS seul, n'est pas forcément aussi sûr. Selon moi il peut ne respecter
- aucun des 3 point si le SMS est détourné sur le réseau
- uniquement le point 2. si le SMS s'affiche sans avoir besoin de déverrouiller le téléphone.
C'est probablement pour cela qu'il est complété par le mot de passe banque en ligne, sans cela l'accès ne respecte probablement pas la norme bancaire DSP2.

L'appli bancaire n'est pas aussi sûr si le smartphone est vérolé.
Là le boîtier est complètement hors ligne, donc pas de piratage possible (sauf si j'ai une camera/quelqu'un derrière mois, ou si quelqu'un à modifier/échangé mon boîtier pour y ajouter une antenne...).

Est-ce que j'ai répondu à la question ?

[^] # Re: Boîtier sésame

Posté par **Glandos** le 08 avril 2022 à 14:19.
Évalué à 5.

> l'intelligence est dans la CB.

Je serais tatillon : l'intelligence est dans le boîtier, mais le secret est dans la puce de la CB.

[^] # Re: Boîtier sésame

Posté par **mahikeulbody** le 08 avril 2022 à 16:38. Évalué à 3.

> Est-ce que j'ai répondu à la question ?

Oui, merci pour ta réponse très détaillée.

Dans mes bras !

Posté par **ll0zz** (**Mastodon**) le 08 mai 2022 à 22:22. Évalué à 2.

> Étant à la BNP, j'ai eu exactement la même réaction que toi.
> J'ai essayé d'en discuter sur la ML de mon GUL sans retour (j'avais peut-être pas aussi bien expliqué ceci-dit).
> J'ai écrit à la BNP, sans réponse.
> J'ai fini par être plus ou coincé, alors j'ai activé Paypal puis changé le mot de passe dans la foulée. Depuis je passe par Paypal, ça me semble moins craignos que de donner accès à mon compte bancaire à n'importe qui.
>
> Je suis preneur de la banque la moins librophobe du marché...

[^] # Re: Dans mes bras !

Posté par **Stéphane Ascoët** (**site web personnel**) le 11 mai 2022 à 11:39. Évalué à 1.

> Elle est en cours de création, c'est LaNef(voir autre message plus haut), mais il faut que des libristes compétents et très motivés s'y investissent pour qu'ils fassent les bons choix.

Même bateau avec BNP/Hellobank

Posté par **xryl669** le 09 mai 2022 à 17:14. Évalué à 3. Dernière modification le 09 mai 2022 à 17:15.

> Le fonctionnement sur Hellobank / BNP est identique, voire moins sécurisé, vu qu'ils demandent le mot de passe du compte avant d'envoyer le SMS (il n'y a pas de petites économies, hein?)
>
> Ce qui me rends dingue, c'est qu'il n'y a pas de moyen d'éviter cette daube.
>
> Comment un informaticien peut coder ça, sérieux ?
> Une simple capture du HTML + CSS et c'est le paradis du phishing.
> 1. Tu proposes un site bidon avec de la vente de produit ~~pas~~ moins cher que d'habitude.
> 2. Puis tu demandes de payer avec ta CB. Avec les 4 premiers numéro de la CB, tu identifies que la CB provient du réseau BNP.
> 3. Tu balances une fausse iframe avec les bons logos et autre DOM/CSS que tu as capturé, et une iframe (inaccessible, dans la marge) sur le site d'Hellobank/BNP pour capturer les formulaires enregistrés (l'identifiant du compte n'est pas codé, il est en clair).
> 4. L'utilisateur va entrer son mot de passe de connexion. Avec l'identifiant capturé dans l'iframe plus le mot de passe de l'utilisateur, tu te loggues sur Hellobank.
> 5. Hellobank/BNP va détecter que ce n'est pas la même origine que d'habitude et va donc t'envoyer un SMS avec un code de connexion.
> 6. Tu demandes à l'utilisateur sur le deuxième page de l'iframe le code reçu.
> 7. L'utilisateur va entrer le code, forcément (même si le montant de l'achat n'est pas spécifié, car quoi, lui ne sait pas comment doit être le SMS).
> 8. Voilà, tu peux donc accéder au compte de l'utilisateur. Lui pomper ces données et ses sous.
> 9. Si tu veux pousser le vice encore plus, tu envoies un pseudo message d'erreur à l'utilisateur dans la troisième page de l'iframe, avec un bouton pour qu'il demande le renvoi du code reçu. (Forcément, aucune banque n'accepte de retaper un code, c'est supposé être du one-shot)
> 10. L'utilisateur va très probablement cliquer sur le bouton. Parallèlement tu procèdes à un vrai achat pendant ce temps, vu que tu as tout ce qu'il te faut

(mot de passe + code SMS entré par l'utilisateur, cette fois pour le "vrai" achat).
11. Voilà, l'utilisateur va recevoir un mail légitime de la banque lui indiquant qu'il a dépensé X€ chez machin chose.

Toi, t'as gagné un accès direct sur son compte pour 3 mois.

C'est franchement donner le bâton pour se faire battre à ce niveau.

Réponse du service client

Posté par **Glandos** le 01 juin 2022 à 16:13. Évalué à 7.

J'avais écrit ceci, le jour même, au service client :

> Bonjour,
>
> Je viens de constater que Crédit Coopératif vient de mettre en place l'authentification à deux facteurs lors du paiement en ligne. Théoriquement, c'est une bonne chose, mais ce que j'ai vu m'impose de tirer la sonnette d'alarme : votre implémentation est dangereuse. Elle rompt la confiance et force les utilisateurs à devenir moins méfiant face aux arnaques.
>
> En effet, j'ai un paiement à effectuer sur montoulouse.fr Pour le paiement, celui-ci me redirige sur paiement.systempay.fr qui semble être son prestataire de paiement. Il est déjà difficile pour un utilisateur de savoir s'il peut rentrer ses informations sur un site qui n'est ni celui de ses achats, ni celui de sa banque, et qui a un nom qui ne se rapporte à aucun groupe bancaire connu.
>
> Ensuite, lors de la mise en place de 3D-Secure, une iframe s'affiche au milieu de la page, avec une fausse barre d'adresse pour indiquer l'adresse de ce cadre, qui est un sous-domaine de wlp-acs.com. C'est dans ce cadre que je dois d'abord rentrer mon code reçu par SMS, puis ensuite vient la deuxième étape problématique : je dois fournir mon mot de passe à un site tiers.
>
> Je tiens à vous rappeler que, selon les termes des conditions générales (disponibles sur https://www.credit-cooperatif.coop/votre-banque/tarifs-et-informations-reglementaires/conditions-generales-produits-services/) au paragraphe 5.2 :

En cas d'utilisation d'un dispositif d'authentification mis en place par le Crédit Coopératif, le Client doit prendre
toutes les mesures nécessaires afin d'éviter (i) la divulgation à des tiers non autorisés, et/ou (ii) la copie, et/ou (iii)
toute utilisation non autorisée des facteurs d'authentification.

Je suis développeur informatique depuis plus de 15 ans. Je gère mon propre hébergement de ressources Internet (courriel, cloud, etc.). J'ai donc une expérience certaines des transferts de données, des noms de domaines et du chiffrement. Et pourtant, il m'est impossible de satisfaire cette clause lors du paiement :

- Je ne sais pas qui est wlp-acs.com et personne n'explique qui ils sont
- Il n'y a pas non plus d'explication sur la gestion des données
- En gros : mon mot de passe d'accès au compte personnel transite sur Internet à des tiers.

Il se trouve que j'ai également un compte bancaire chez Boursorama Banque qui ont implémenté le paiement avec authentification à deux facteurs de la façons suivante :
On rentre ses informations de carte sur le site marchand.
3D-Secure se met en marche, avec une iframe, et celle de Boursorama dit qu'il faut se connecter sur son espace client, dans un nouvel onglet.
Sur l'accueil de l'espace client apparaît le paiement avec le détail.
Pour valider le paiement, il y a l'envoi d'un SMS ou d'un courriel.
Retour sur l'onglet du paiement, c'est validé.

Dans ce cas-là, je me connecte comme d'habitude à mon espace client, et je ne transmet donc mon mot de passe qu'à ma banque, qui se charge de faire le lien avec le prestataire de paiement. La confiance est garantie.

De manière plus personnelle, tout au long de ma

> vie, je me suis échiné à faire de la prévention aux arnaques sur Internet, en mentionnant la confiance, les URL (et pas les images affichées qui ne veulent rien dire) et les informations transmises. Dans ce cas d'utilisation, tout est piétiné : les URL ne sont pas connues, la confiance ne peut pas être établie, et les données transmises sont hautement sensibles.
>
> Merci donc de corriger cela au plus vite. Il me semble très douteux que ce genre d'expérience utilisateur aie pu être validé par un audit de sécurité externe. C'est dangereux, et très contre-productif pour la sécurité de vos clients.

Oui, j'étais un peu agacé, j'ai même laissé les fautes dedans :)

La réponse est arrivée aujourd'hui :

> J'ai pris connaissance de vos échanges avec votre conseiller de clientèle, Monsieur Maxime GRESLE, par lesquels vous exprimez votre insatisfaction portant sur la sécurisation de nos paiements en ligne.
>
> Je comprends votre sentiment et tiens à vous assurer que vos interrogations ont été pleinement prises en considération.
>
> En effet, le système de sécurisation évoqué dans vos échanges semble concerner l'authentification à 2 facteurs avec saisie du code reçu par SMS et du mot de passe « banque en ligne » (OTP SMS renforcé).
>
> Celle-ci répond à un besoin de disposer d'une solution complémentaire afin de couvrir une part de nos clients ne disposant pas de smartphone par exemple, afin de répondre à la réglementation européenne DSP2.
>
> Aussi, pour reprendre les éléments de comparaison de votre mail, je souhaite vous confirmer que nous proposons une solution équivalente à celle proposée par Boursorama.
>
> Cette solution nommée SECUR'PASS a été préconisée par le Groupe BPCE pour assurer un niveau de sécurité optimal dans le cadre de la validation des opérations de paiement.
>
> Vous trouverez en pièce-jointe de ce mail une Foire

> Aux Questions qui, je l'espère, permettra de répondre à vos interrogations.

Donc voilà, on se fout de moi, mais ça ne sera pas le premier service client qui répond à côté, ni le dernier. Évidemment, entre répondre à côté de la plaque et ne pas me répondre du tout, je ne sais pas ce qui est le pire...

[^] # Re: Réponse du service client

Posté par **Ysabeau** (**site web personnel**, **Mastodon**) le 01 juin 2022 à 18:50. Évalué à 4.

> Je les excuse un peu. Ils ne sont sûrement ni outillés ni formés pour répondre à des questions aussi pointues que les tiennes. Alors ils répondent avec des trucs standard parce qu'en plus ils n'ont probablement pas le temps de chercher à faire une vraie réponse adaptée. C'est le problème de tous les services clients (ou presque).
>
> Cela n'en reste pas moins inadmissible et inquiétant pour une banque.
>
> --
>
> « Tak ne veut pas qu'on pense à lui, il veut qu'on pense », Terry Pratchett, Déraillé.

[^] # Re: Réponse du service client

Posté par **Gil Cot ✔** (**site web personnel**, **Mastodon**) le 04 juin 2022 à 02:27. Évalué à 3.

> Donc, on fait une réponse de forme et pas une remonté d'information. Tant qu'on prend les sous de la clientèle ça va, le reste on s'en tamponne.
>
> --
>
> "It is seldom that liberty of any kind is lost all at once." — David Hume

[^] # Re: Réponse du service client

Posté par **Stéphane Ascoët** (**site web personnel**) le 15 juin 2022 à 11:31. Évalué à 3.

> J'ai bossé un trimestre en banque en 2002, et déjà à l'époque ça m'a retiré toute envie de faire appel aux services de ladite banque comme client...

Suivre le flux des commentaires

Note : les commentaires appartiennent à celles et ceux qui les ont postés. Nous n'en sommes pas responsables.

Revenir en haut de page

Derniers commentaires

- Re: LoRa supporte l…
- LoRa supporte le chi…
- Autres liens
- Fork d'Organic Maps
- Re: Contresens hist…
- Re: Contresens hist…
- metaverse
- Re: /e/OS, Graphen…
- Re: Il y a des options…
- Re: Un peu de confu…
- quid novis?
- Pensez à envoyer de…

Étiquettes (tags) populaires

- intelligence_artificielle
- merdification
- microsoft
- grands_modèles_de…
- linux
- sortie_version
- bigtech
- cybersécurité
- sécurité
- google
- wayland
- administration_fran…

Sites amis

- April
- Agenda du Libre
- Framasoft
- Éditions D-BookeR
- Éditions Eyrolles
- Éditions Diamond
- Éditions ENI
- La Quadrature du Net
- Lea-Linux
- En Vente Libre
- Grafik Plus
- Open Source Initiative

À propos de LinuxFr.org

- Mentions légales
- Faire un don
- L'équipe de LinuxFr.…
- Informations sur le s…
- Aide / Foire aux que…
- Suivi des suggestion…
- Règles de modération
- Statistiques
- API pour le dévelop…
- Code source du site
- Plan du site