Vacaf, France Travail : le second facteur qui se vole

Le 12 novembre 2026, le CERT-FR (centre gouvernemental de veille et de réponse aux incidents de l'Agence nationale de la sécurité des systèmes d'information, ANSSI) a décrit deux fuites d'octobre que tout semble opposer. Chez Vacaf, des comptes partenaires dépourvus de second facteur ont servi à extraire près de 1,2 million de dossiers. Chez France Travail, le compte d'un agent a été compromis alors qu'un code envoyé par SMS le protégeait. Le premier cas se lit comme un retard de déploiement, le second dément que le déploiement suffise. Relue avec le principe d'acceptabilité psychologique formulé par Jerome Saltzer et Michael Schroeder en 1975, la série cesse de relever d'une consigne mal suivie et révèle une propriété d'architecture : un accès volé reste indiscernable d'un accès légitime tant que le contrôle repose sur ce que l'usager peut se faire dérober.

Par Alexandre Berge · 26 novembre 2026 · 14 min de lecture · Chronique

Avec ou sans second facteur, l'intrus entre comme un usager légitime

Vacaf est le dispositif d'aide aux vacances des caisses d'allocations familiales, opéré par la Caf de l'Hérault pour le compte de la branche. Selon le deuxième point de situation de l'opération REACTIV publié par le CERT-FR, la violation a été détectée le 9 octobre 2026, après la mise en vente de bases de données. Le mode opératoire tient en deux temps. Des identifiants de comptes de partenaires, récupérés par des logiciels voleurs d'informations (*infostealers*, programmes qui collectent sur le poste infecté les identifiants et les jetons de session), ont ouvert la porte, ces comptes ne disposant d'aucune double authentification. Une adresse web exposant directement les identifiants des dossiers (faille dite IDOR, référence directe à un objet sans contrôle d'autorisation) a ensuite permis une extraction automatisée entre le 8 et le 10 octobre. Le bulletin dénombre près de 1,2 million de dossiers, contenant noms, matricules, quotient familial, identités de mineurs, aides et réservations, sans données bancaires ni mots de passe. La Caisse nationale a pour sa part suspendu vacaf.org le 10 octobre, déposé plainte le 11 avec la Caf de l'Hérault, puis rouvert la plateforme le 2 novembre après des tests d'intrusion, en chiffrant à 1 619 893 le nombre d'allocataires concernés.

Le cas France Travail appartient au même bulletin et procède d'une autre configuration. Le 8 octobre, la vente de données portant sur plus de 60 000 agents et professionnels a été revendiquée sur un forum cybercriminel. L'exfiltration remonte au 26 septembre et résulte,

écrit le CERT-FR, de « la compromission, avec validation du second facteur (SMS), du compte d'un agent ». Les données emportées décrivent l'organisation elle-même : noms, adresses électroniques professionnelles, téléphones, fonctions, agences, identifiants internes. Le compte a été révoqué et les adresses IP malveillantes bloquées. Le bulletin ne précise pas comment le code a été obtenu ou validé, et rien n'autorise à le supposer.

Les deux affaires ne s'inscrivent donc pas sur une échelle allant du moins au mieux protégé. Elles décrivent le même geste. Dans les deux cas, le système d'information a reçu des secrets valides, présentés dans l'ordre attendu, et il a ouvert une session conforme à ses règles. Le bulletin le formule en creux en rangeant les *infostealers* parmi les causes récurrentes de compromission et l'absence d'authentification multifacteur ou l'authentification faible parmi les vulnérabilités récurrentes, sur un total de 64 nouvelles violations portées à la connaissance de l'agence depuis le 30 septembre, dont cinq dans des ministères ou organismes sous tutelle. **Le second facteur par SMS n'a pas séparé l'intrus de l'agent, il a seulement ajouté une étape à franchir.** La question n'est plus de savoir si un compte dispose d'un second facteur, mais de savoir si ce facteur peut être transmis, relayé ou recopié par quelqu'un d'autre que son titulaire.

Le SMS est acceptable parce qu'il confie la sécurité au discernement de l'usager

En 1975, dans les *Proceedings of the IEEE*, Jerome H. Saltzer et Michael D. Schroeder, alors au Project MAC du Massachusetts Institute of Technology, publient « The Protection of Information in Computer Systems ». L'article énonce huit principes de conception des mécanismes de protection, que les auteurs présentent comme des avertissements plutôt que comme des règles absolues. Le dernier, l'*acceptabilité psychologique*, porte sur l'interface entre le mécanisme et la personne qui s'en sert.

> **L'acceptabilité psychologique (Saltzer et Schroeder, 1975)**
>
> Le principe pose que « It is essential that the human interface be designed for ease of use » (il est essentiel que l'interface humaine soit conçue pour être facile à utiliser), afin que les utilisateurs appliquent correctement les mécanismes de protection, par routine et sans y penser. Les auteurs ajoutent que les erreurs diminuent lorsque la représentation que l'utilisateur se fait de ses objectifs de protection coïncide avec le fonctionnement du mécanisme, et qu'elles augmentent lorsqu'il doit traduire ces objectifs dans un langage qui lui est étranger. La facilité d'usage n'est donc pas une concession au confort. Elle est la condition pour que le comportement correct soit aussi le comportement spontané.

Le code à usage unique envoyé par SMS satisfait en apparence ce principe. Il ne demande aucun matériel supplémentaire, repose sur un objet que chacun possède déjà et ne requiert qu'une recopie de six chiffres. C'est précisément pour cette raison qu'il s'est imposé comme second facteur par défaut. Mais la lecture de Saltzer et Schroeder déplace la question. Leur

critère n'est pas que le mécanisme soit facile, il est que l'usage facile soit aussi l'usage correct. Or le code reçu par SMS est valable partout où il est saisi. Son bon emploi suppose que l'agent vérifie lui-même, à chaque connexion, que la page qui le lui demande est bien celle de son employeur, et que rien sur son poste n'intercepte la saisie. **La facilité est obtenue en transférant à la vigilance humaine la vérification que le mécanisme ne fait pas.** Le principe d'acceptabilité psychologique se trouve ainsi respecté dans sa lettre et inversé dans son intention : le geste routinier est exactement celui que l'attaquant sait exploiter.

Les facteurs dits résistants à l'hameçonnage (clés physiques FIDO2, clés d'accès ou *passkeys* fondées sur le standard WebAuthn du W3C) renversent cette répartition. La réponse cryptographique y est liée au site qui la sollicite, si bien qu'une page frauduleuse n'obtient rien d'utilisable, quel que soit le degré d'attention de l'usager. La vérification que le SMS délègue à la personne est ici absorbée par l'architecture. C'est le sens exact du principe de 1975 : rendre la sécurité indépendante de la vertu de chacun. Le retour d'expérience publié par le CERT-FR le 20 octobre 2026 en marque toutefois la limite, en rappelant qu'un attaquant maître du poste de travail peut usurper l'identité de l'utilisateur légitime quel que soit le second facteur qui y est connecté. L'architecture déplace le risque, elle ne l'abolit pas.

L'ANSSI écarte le SMS depuis 2021, son indicateur de progrès ne le distingue pas

La doctrine existe et elle est ancienne. Le guide de l'ANSSI « Recommandations relatives à l'authentification multifacteur et aux mots de passe », réécrit en version 2.0 le 8 octobre 2021 avec un avant-propos de la CNIL, range explicitement l'association d'un mot de passe et d'un code temporaire reçu par SMS parmi les authentifications multifacteurs qui ne sont pas fortes. Il cite à l'inverse les protocoles FIDO2 et FIDO U2F parmi les mécanismes d'authentification forte, et recommande de privilégier un facteur de possession doté d'un composant de sécurité ayant reçu un visa de l'agence. Le même guide demande que l'analyse de risque intègre l'expérience utilisateur et la facilité d'utilisation, au motif que des contraintes excessives conduisent les utilisateurs à les contourner. L'ANSSI a donc formulé, dans ses propres termes, la tension que Saltzer et Schroeder avaient nommée.

> **Ce que dit la recommandation R8 (ANSSI, 2021)**
>
> La recommandation R8 du guide ANSSI-PG-078 conseille de « ne pas utiliser le SMS comme moyen de réception d'un facteur d'authentification ». Le guide justifie cette position par les vulnérabilités intrinsèques des protocoles de signalisation téléphonique SS7 et par les attaques d'ingénierie sociale visant la carte SIM. Il admet le code SMS, faute d'alternative, comme un moyen de limiter ou de détecter les connexions frauduleuses, non comme une sécurité suffisante.

Le retour d'expérience du CERT-FR sur les violations de données applicatives, publié le 20 octobre 2026, durcit le constat cinq ans plus tard. Il tient l'authentification par identifiant

et mot de passe pour obsolète et pose que « tous les facteurs d'authentification qui doivent être manuellement saisis sont vulnérables à l'hameçonnage ». Il ajoute que les codes saisis à la main ne sont pas durablement efficaces contre une attaque ciblée, et décrit les *passkeys* comme des secrets stockés par le navigateur, dont le vol exige de contourner un composant de confiance. La référence américaine converge. La publication spéciale 800-63B du National Institute of Standards and Technology classe l'usage du réseau téléphonique pour l'authentification hors bande comme restreint et énonce que « Out-of-band authentication is not phishing-resistant » (l'authentification hors bande n'est pas résistante à l'hameçonnage).

Le décalage apparaît lorsque cette doctrine est confrontée à la manière dont l'État mesure son effort. Le bulletin REACTIV du 12 novembre 2026 qualifie de significatifs les progrès des mesures de sécurisation, en citant notamment la mise en œuvre de l'authentification multifacteur, et fait état d'un avancement de 70 % au niveau interministériel. Il recommande une authentification forte mise en place de façon systématique. Dans les pages de ce bulletin, l'indicateur de progrès porte sur la présence d'un second facteur, sans distinguer les facteurs que la doctrine de l'agence juge faibles de ceux qu'elle juge résistants. **Le compte compromis chez France Travail aurait figuré du côté des comptes équipés.** C'est l'angle mort du discours institutionnel : la distinction que l'ANSSI établit dans ses guides depuis 2021 ne descend pas jusqu'à l'instrument qui pilote le rattrapage. Un indicateur binaire récompense le déploiement le plus acceptable au sens ordinaire, donc le plus facile, c'est-à-dire le SMS.

La banque a quitté le SMS par une échéance, non par une recommandation

Le secteur bancaire français a déjà traversé ce passage, avec une proximité structurelle rare. Il s'agissait d'un public massif, habitué au code SMS comme validation par défaut, et d'une autorité qui avait jugé ce code insuffisant. Dans un avis de juin 2018, rappelé par le ministère de l'Économie dans une réponse à une question écrite publiée au Journal officiel le 6 octobre 2020, l'Autorité bancaire européenne a estimé que la saisie des données de la carte associée à un code temporaire reçu par SMS ne pouvait constituer une authentification forte au sens de la deuxième directive sur les services de paiement. L'échéance de mise en conformité des paiements en ligne avait été reportée au 31 décembre 2020.

L'Observatoire de la sécurité des moyens de paiement, placé auprès de la Banque de France, a alors piloté un plan de migration à deux volets : le remplacement du code SMS par des techniques d'authentification forte, et le passage du protocole 3-D Secure de sa première à sa deuxième version. Un groupe de travail réunissait chaque mois banques, prestataires techniques, commerçants, Banque de France, Autorité de contrôle prudentiel et de résolution et direction générale du Trésor. Une période de flexibilité de trois mois a été accordée à la mi-2020 en raison de la crise sanitaire. Le 6 juillet 2021, l'Observatoire constatait que plus de quatre porteurs de carte sur cinq achetant sur internet utilisaient un dispositif d'authentification forte « en remplacement de la saisie d'un code reçu par SMS comme seul facteur d'authentification », et qu'environ 95 % des flux des e-commerçants français étaient

conformes. Son rapport annuel, mis en ligne le 18 octobre 2021, validait la fin du plan de migration de Place.

Le précédent ne dit pas que la banque aurait trouvé la solution parfaite. Il montre ce qui a rendu la sortie possible. La qualification du SMS comme insuffisant était adossée à une obligation juridique, à une date opposable et à une instance de suivi qui mesurait la nature du facteur et non sa simple présence. **La doctrine publique dispose de la qualification, elle ne dispose ni de l'échéance ni de la mesure.** La recommandation R8 a cinq ans, et l'indicateur qui accompagne le rattrapage de l'État compte encore des comptes équipés.

La frontière passe par ce qu'un compte permet d'extraire, pas par son titulaire

Le retour d'expérience du CERT-FR ne prétend pas que l'authentification forte puisse être imposée partout. Il observe qu'elle ne peut pas être rendue impérative pour toute application destinée à un large public et recommande, pour les usagers, des parcours alternatifs, y compris hors ligne. C'est l'acceptabilité psychologique dans sa version administrative : un service public universel ne peut exiger de chaque allocataire une clé matérielle. Le même document pose en revanche que les accès transverses ou privilégiés doivent être contrôlés par des moyens d'authentification forte.

Les deux cas d'octobre se situent précisément de ce côté de la frontière. Le compte France Travail était celui d'un agent, c'est-à-dire d'un utilisateur interne à qui l'employeur peut fournir un équipement. Les comptes Vacaf étaient des comptes de partenaires professionnels, et non d'allocataires. Leur portée réelle tenait moins à leurs droits nominaux qu'à une seconde défaillance : une fois la session ouverte, l'application servait les dossiers par simple incrémentation d'identifiants. Saltzer et Schroeder avaient nommé ce principe dans le même article, sous le terme de *médiation complète* : chaque accès à chaque objet doit être vérifié au regard des droits de celui qui le demande. Une faille IDOR est la négation de ce principe. L'authentification y fonctionne comme une porte unique, après laquelle plus rien n'est contrôlé.

Le critère de décision que suggère ce rapprochement n'est donc pas statutaire. Un compte qui peut lire un dossier n'appelle pas la même protection qu'un compte qui peut en extraire un million. Le praticien observe que les politiques d'habilitation classent les comptes par fonction, rarement par volume de données atteignable. **Un second facteur faible devant un accès de masse, ou une authentification forte devant une application qui ne contrôle plus rien ensuite, produisent le même résultat.** L'acceptabilité psychologique ne se négocie pas compte par compte. Elle se calibre selon ce que la compromission d'un seul compte rend possible.

Un second facteur qui se vole n'est pas un retard, c'est un choix d'architecture

Les chroniques précédentes de cette série avaient traité la réponse institutionnelle aux fuites, puis le compte usurpé sur la messagerie de l'État, puis la responsabilité du donneur d'ordre envers son prestataire. Les cas Vacaf et France Travail ajoutent un élément que ces lectures laissaient de côté : la nature du facteur exigé à l'entrée. Tant que le contrôle d'accès repose sur un secret que l'usager peut se faire dérober, qu'il s'agisse d'un mot de passe ou d'un code recopié, l'accès volé reste indiscernable de l'accès légitime. Ajouter un SMS ne change pas cette propriété, il en déplace le point de franchissement. Le principe d'acceptabilité psychologique de Saltzer et Schroeder permet de nommer ce que l'indicateur binaire masque. Un mécanisme facile n'est pas un mécanisme acceptable au sens de 1975 si sa facilité repose sur la vigilance de chacun. **La sécurité d'un second facteur est une propriété d'architecture, pas une consigne adressée aux agents.**

L'hypothèse qui en découle est vérifiable. Si l'État traite le sujet comme un retard de déploiement, ses bilans continueront de compter la présence d'une authentification multifacteur, et des comptes protégés par SMS continueront d'apparaître parmi les modes opératoires décrits. S'il le traite comme une question d'architecture, un indicateur distinct apparaîtra. Le premier signe observable sera la présence, dans un point de situation REACTIV ou dans un document de pilotage publié par l'ANSSI ou les services du Premier ministre, d'une mesure séparée de la part des comptes d'agents et de partenaires protégés par un facteur résistant à l'hameçonnage. Le second sera la traduction de la recommandation R8 en exigence datée et opposable pour les accès privilégiés ou de masse aux données personnelles. L'horizon de vérification est fixé au 31 décembre 2027. À cette date, l'absence des deux signaux indiquerait que la doctrine de 2021 est restée une qualification sans échéance, ce que le secteur bancaire avait évité en trois ans.

Note méthodologique

L'analyse s'appuie principalement sur le deuxième point de situation REACTIV du CERT-FR (12 novembre 2026), son retour d'expérience du 20 octobre 2026 et le guide ANSSI-PG-078 de 2021. Les volumes de Vacaf divergent selon les sources publiques : le CERT-FR compte près de 1,2 million de dossiers, la Cnaf 1 619 893 allocataires concernés. Les deux unités n'étant pas identiques, les deux chiffres sont rapportés sans être réconciliés. Le constat selon lequel l'indicateur de progrès ne distingue pas la nature du second facteur est borné au bulletin du 12 novembre 2026, consulté le 21 novembre 2026. Le choix du principe d'acceptabilité psychologique comme cadre central, de la médiation complète comme appui secondaire et de la migration bancaire de 2019 à 2021 comme parallèle relève de l'auteur. Recherche de sources, croisement des données et structuration du raisonnement s'appuient sur une assistance par intelligence artificielle. Le choix de l'angle et du cadre théorique, la vérification des sources, les arbitrages et l'établissement du texte final relèvent de l'auteur.

Sources

Sources primaires institutionnelles

CERT-FR, Agence nationale de la sécurité des systèmes d'information, « REACTIV. Point de situation », deuxième point de situation de l'opération, référence CERTFR-2026-CTI-010, 12 novembre 2026. Page du rapport et document PDF.

CERT-FR, Agence nationale de la sécurité des systèmes d'information, « RETEX du CERT-FR sur les violations de données applicatives », référence CERTFR-2026-CTI-008, version 1.01, 20 octobre 2026. Document PDF.

Agence nationale de la sécurité des systèmes d'information, « Recommandations relatives à l'authentification multifacteur et aux mots de passe », guide ANSSI-PG-078, version 2.0, 8 octobre 2021. Page du guide.

Caisse nationale des allocations familiales, communiqué de presse « Incident de cybersécurité concernant Vacaf : la Cnaf présente les conclusions de ses investigations et les mesures engagées », 2 novembre 2026. Communiqué.

National Institute of Standards and Technology, Special Publication 800-63B-4, « Digital Identity Guidelines: Authentication and Authenticator Management », version en ligne consultée le 21 novembre 2026. Publication.

Cadre théorique

Jerome H. Saltzer et Michael D. Schroeder, « The Protection of Information in Computer Systems », *Proceedings of the IEEE*, vol. 63, n° 9, septembre 1975. Version mise en ligne par l'auteur au MIT, section « Basic Principles of Information Protection », consultée le 21 novembre 2026. Texte.

Parallèle historique

Ministère de l'Économie, des Finances et de la Relance, réponse à la question écrite n° 31658 de Valérie Beauvais, Journal officiel du 6 octobre 2020, page 6866. Question et réponse.

Observatoire de la sécurité des moyens de paiement, communiqué de presse, Paris, 6 juillet 2021. Communiqué.

Observatoire de la sécurité des moyens de paiement, « Rapport annuel de l'Observatoire de la sécurité des moyens de paiement 2020 », mis en ligne le 18 octobre 2021. Rapport.

Chroniques liées

« Cyberfuites : l'État déplace les organigrammes », 14 mai 2026. Chronique.

« Tchap, l'accident normal de la souveraineté », 2 juillet 2026. Chronique.

« Le fisc piraté par un « tiers habilité » : l'angle mort de l'identité déléguée », 11 septembre 2026. Chronique.

« 545 000 usagers : la région qui sous-traitait sa fuite », 12 octobre 2026. Chronique.