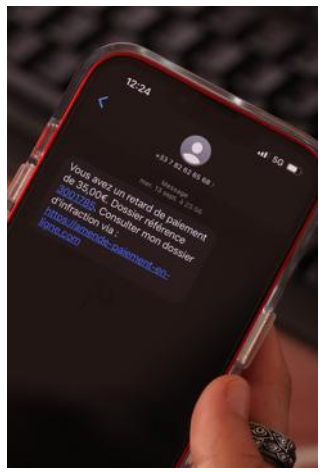
Jura

Ils se font passer pour votre banque, Amazon ou un commercial : gare aux arnaques

Les escrocs multiplient les stratagèmes pour soutirer de l'argent à leurs victimes. Depuis la rentrée, la police nationale constate, notamment sur le secteur dolois, une recrudescence des fraudes par SMS, par téléphone, voire en direct.

Ils se font passer pour la banque, le service client d'un site marchand ou la police et escroquent leurs victimes de plusieurs centaines, voire milliers d'euros. Dans le bassin dolois, la police nationale constate, depuis la rentrée, une recrudescence de ces fraudes, qui ciblent souvent des personnes âgées. Elle appelle à la plus grande prudence : il est préférable de contacter directement l'organisme concerné, avant de procéder à tout paiement, de cliquer sur un lien reçu ou de fournir des données personnelles.



Il ne faut jamais cliquer sur un lien reçu par SMS ou e-mail et invitant à régulariser une situation. Illustration Richard Mouillaud

Attention aux faux conseillers

Derniers exemples en date : une Doloise a reçu un e-mail lui indiquant que son abonnement Amazon Prime arrivait à échéance et qu'elle allait être débitée de 69 euros. N'ayant souscrit aucun abonnement de la sorte, elle a cliqué sur un lien avant d'être contactée par un faux conseiller. Elle a au final été escroquée de 3 000 euros.

À Choisey, un professionnel qui venait de réparer des fenêtres a reçu la visite d'un individu se présentant comme le commercial de la société de fenêtres. Il lui a indiqué que, pour le remercier de cette bonne publicité, il allait lui faire un virement de 160 euros. Il lui a alors tendu un terminal de paiement mais c'est finalement la victime qui s'est vue délester de cette somme.

Ne pas prêter son téléphone, activer le mode réparation

De même, il est recommandé de ne pas prêter son téléphone portable à un inconnu qui en fait la demande dans la rue, ni de laisser son appareil dans une boutique de réparation sans activer au préalable le mode réparation ou maintenance, lorsqu'il est disponible sur son appareil. À défaut, le contenu d'un téléphone peut être copié en quelques secondes.

● C.L.

Besançon

Le site commercial des Presses universitaires de Franche-Comté victime d'une cyberattaque

Une équipe d'intervention d'urgence du réseau Renater (sécurité numérique de la communauté éducation recherche) a détecté un script malveillant sur le site des Presses universitaires de Franche-Comté. Il s'agit d'un dispositif de « web skimming » capable d'aspirer les coordonnées bancaires des usagers d'un site lors d'un paiement en ligne. Selon le communiqué de l'Université Marie et Louis Pasteur, il semble que ce script était présent depuis 2023.

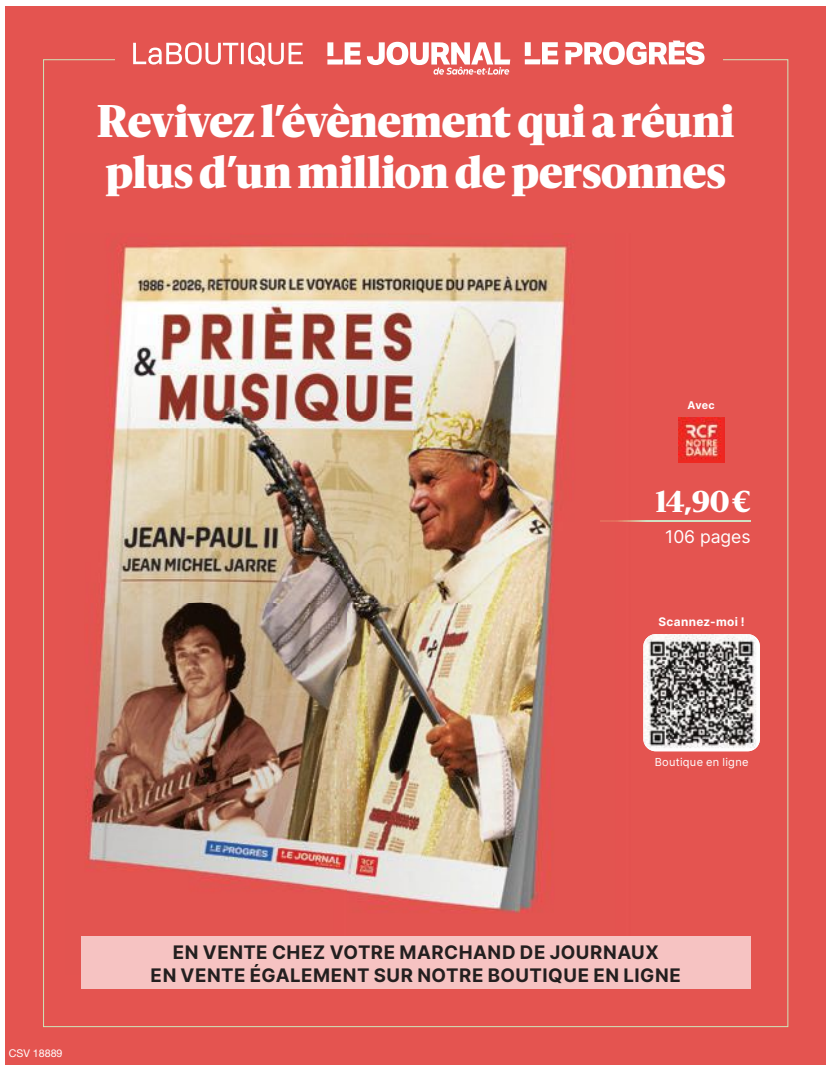
Le site a aussitôt été gelé avec interruption totale des accès publics afin de « neutraliser tout risque d'exfiltration des données ». Le protocole prévoit de saisir la Cnil (Commission nationale informatique et liberté) ainsi que l'Anssi (Agence nationale pour la sécurité des systèmes d'information). Une plainte est en cours de dépôt auprès du parquet de Besançon.

Un seul site concerné

Au sein de l'Université, une équipe de 10 personnes est sur les dents depuis la notification du réseau Renater, à commencer par Pascal Chatonnay, le responsable de la sécurité des systèmes d'information. « Nous avons informé les 1332 usagers du site. Nous attendons les retours pour savoir s'ils constatent des anomalies. Nous sommes très prudents, mais il est presque impossible que des grosses sommes aient été prélevées. Nous n'avons trouvé aucune trace ou signature malveillante sur les autres sites de l'université ».

Les usagers, qui ont effectué un achat depuis décembre 2023, sont ainsi invités à vérifier leurs comptes et, « au moindre doute, à se rapprocher de leur établissement bancaire pour solliciter le renouvellement de leur moyen de paiement ». L'UMLP dit regretter l'incident tout en mobilisant l'ensemble de ses moyens techniques et juridiques pour accompagner les usagers. « Nous prenons cette crise très au sérieux », admet Pascal Chatonnay.

● D.F.



512405100



513264300

JURB - V1