06.05.2025

Rapport semestriel de l'Office fédéral de la cybersécurité (OFCS)

Avec un total de plus de 62 000 signalisations enregistrées au cours du deuxième semestre 2024, l'Office fédéral de la cybersécurité (OFCS) a enregistré une hausse significative des cyberincidents par rapport à la même époque de l'année dernière. En particulier, l'OFCS fait état d'une recrudescence des épisodes de phishing par téléphone ou phishing vocal (Voice Phishing ou «Vishing»).

Les statistiques de l'Office fédéral de la cybersécurité (OFCS) montrent que le phishing figure encore parmi les principaux défis auxquels sont confrontés l'économie et la population suisses. Avec 12 038 signalisations, l'hameçonnage représentait en 2024 le deuxième cyberincident le plus fréquemment signalé après les arnaques, soit une augmentation de 2 623 par rapport à l'année précédente. Au-delà des épisodes classiques d'hameçonnage, le phishing par téléphone a connu une forte augmentation au cours de l'année dernière. En particulier, les tentatives de phishing réalisées au nom de prestataires de services financiers sont très en vogue. En 2024, les escrocs ont principalement utilisé la méthode bien connue dans les années 2010 des appels provenant soi-disant d'instituts bancaires. Si le mode opératoire n'a effectivement pas changé, le prétexte invoqué par les malfaiteurs a été adapté.

Ces derniers se font en effet maintenant passer par exemple pour des collaborateurs du service de sécurité d'un établissement financier, en affirmant vouloir bloquer un paiement frauduleux. Or, pour ce faire, les escrocs ont réussi à usurper le numéro de l'institut financier en question (« spoofing »). Du coup, en voyant s'afficher le véritable numéro de téléphone de l'établissement financier, la victime ne se doute pas qu'il peut s'agir d'un appel frauduleux. Afin de bloquer le prélèvement présumé frauduleux, les criminels fournissent à la victime un faux numéro de téléphone censé les mettre en contact avec la police. Bien entendu, l'appel n'aboutit pas aux services de police mais de nouveau aux criminels, qui fournissent à la victime toute une série d'instructions et de liens piratés pour accéder à son compte bancaire et lui soutirer de l'argent.

Ce type d'attaque appelé phishing vocal (Voice-Phishing ou Vishing en anglais) permet aux escrocs d'agir pratiquement en temps réel, une condition absolument nécessaire pour permettre aux criminels d'accéder aux applications protégées par une authentification multifactorielle (MFA) (https://www.ebas.ch/fr/2024/12/authentification-multifacteur-et-passkeys/) , comme c'est le cas pour l'e-banking. Le MFA est un excellent rempart contre les attaques, mais il peut être contourné par des techniques d'ingénierie sociale.

Par conséquent, il convient là encore de faire preuve de scepticisme (https://www.ebas.ch/fr/5-faire-attention-et-etre-vigilant/) et de garder à l'esprit que les banques suisses ne vous demanderont jamais de fournir des informations aussi sensibles que votre mot de passe ou les codes fournis par les applications MFA.

Pour en savoir plus sur le facteur humain, cliquez ici (https://www.ebas.ch/fr/2025/04/le-facteur-humain-maillon-faible-ou-atout-pour-la-securite/) .

Pour consulter le rapport semestriel 2024/II (Juillet-Décembre) de l'OFCS, cliquez ici (https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/dokumentation/lageberichte/BACS-HJB-2024-2_FR.pdf.download.pdf/BACS-HJB-2024-2_FR.pdf) .