# Des Suisses trop naïfs face aux cyber-arnaques

**TECHNOLOGIE** Les annonces de cyberincidents affectant des particuliers, mais aussi de cyberattaques paralysant des entreprises, se maintiennent à un niveau très élevé, selon les chiffres officiels. Si les pirates usent d'artifices ingénieux, les victimes sont souvent trop crédules

Au premier semestre 2025, 35 727 cyberincidents ont été communiqués à l'Office fédéral de la cybersécurité, dont 58% concernaient des tentatives d'escroquerie. *(GETTY IMAGES)*

ANOUCH SEYDTAGHIA

Ouvrez votre téléphone et parcourez quelques applications. Les SMS, d'abord. «Bonjour maman, mon téléphone est cassé. J'ai perdu toutes mes données. Tu peux m'envoyer un message sur WhatsApp? C'est mon nouveau numéro», dit le message, affichant un numéro commençant par + 41 77. Ouvrez ensuite Telegram. Vous verrez que vous avez été ajouté au groupe «Global Wealth Hub», une certaine Emma Rose Williams livrant ses conseils d'investissements. Dans votre messagerie, les e-mails d'apparence légitime d'Infomaniak, Assura ou La Poste s'empilent. Et ne parlons même pas des appels reçus – comme ces enregistrements en anglais censés provenir des autorités –, mais parfois beaucoup plus subtils.

Nous sommes harcelés par les cyberarnaques. Certaines débutent de manière anodine et se poursuivent avec des niveaux de sophistication impressionnants. Et le phénomène ne faiblit pas, les criminels exploitant la naïveté toujours tenace de leurs victimes. Mardi, l'Office fédéral de la cybersécurité (OFCS) a publié des chiffres qui donnent un aperçu glaçant du phénomène. Lors du premier semestre 2025, pas moins de 35 727 cyberincidents lui ont été communiqués, un chiffre «stable, à un niveau élevé», selon l'OFCS, qui note que 58% concernaient des tentatives d'escroquerie (le solde étant des piratages, fuites de données ou encore des maliciels). Si les alertes liées à des appels frauduleux ont baissé, à 10 578 cas, les tentatives d'escroqueries à l'investissement en ligne via des publicités ont explosé, avec une multiplication par cinq des cas à 3485 annonces.

Ces chiffres ne représentent qu'une toute petite pointe du gigantesque iceberg des cyberarnaques. Il s'agit d'annonces volontaires de citoyens. Et l'OFCS ne sait rien des sommes perdues par les victimes: des centaines, et parfois des dizaines de milliers de francs, les médias relatant sans cesse des histoires dramatiques.

L'OFCS donne plusieurs exemples édifiants, ciblant notamment Twint ou des services d'e-banking. Les escrocs repèrent leurs victimes, qui vendent un objet sur des sites de petites annonces, et les appellent par téléphone. «Grâce à des contacts personnels établis parfois sur plusieurs jours, ils paraissent crédibles, veillant notamment à rassurer leurs victimes au cas où elles deviendraient méfiantes», écrit l'OFCS, qui déplore que les cibles donnent petit à petit toutes les informations sensibles.

### Pistes brouillées

Autre arnaque: les pirates créent de faux sites web de banques, payent pour qu'ils soient mieux référencés que les sites légitimes sur Google et parviennent ainsi à aspirer progressivement toutes les informations de connexion à leurs cibles, avant de «piller le compte e-banking de leurs victimes», dit l'OFCS. Les pirates parviennent aussi régulièrement à prendre le contrôle de comptes Twint, grâce à de l'ingénierie sociale et en endormant la méfiance des internautes, avec, in fine, «des transactions irrévocables». «Souvent, les cybercriminels ont le temps de faire plusieurs opérations avant que la fraude ne soit découverte par la banque. Ils veillent d'ailleurs à brouiller les pistes en transférant de l'argent sur plusieurs comptes, dont certains piratés», détaille la Confédération.

> «Les fraudes sont de mieux en mieux conçues, ce qui rend leur identification complexe, même pour les utilisateurs expérimentés»
>
> YAN BORBOËN, ASSOCIÉ CHARGÉ DES SERVICES DE CYBERSÉCURITÉ CHEZ PWC

L'hameçonnage (ou *phishing* en anglais) continue ainsi de faire des ravages. «Malgré l'augmentation de la sensibilisation, les internautes restent vulnérables au *phishing*, car l'évolution rapide et la sophistication des attaques, notamment via l'intelligence artificielle, rendent leur détection plus difficile. Les efforts de formation, même s'ils progressent, peinent à suivre le rythme de l'innovation criminelle», analyse Yan Borboën, associé chargé des services de cybersécurité chez PwC.

Il faut aussi parler des arnaques à l'investissement. Ouvrez Instagram ou Facebook, ou alors consultez des sites de médias légitimes: vous y trouverez très souvent des interviews chocs de personnalités de la RTS, de Karin Keller-Sutter, de Roger Federer ou de DJ Bobo, permettant, prétendument, de tout savoir sur leur stratégie de placement. Les pirates demandent un apport de 250 francs au début, puis de beaucoup plus, avant que la victime – qui parfois reçoit un peu d'argent – finisse par perdre des sommes colossales. Et il y a plus pervers encore. «Les escrocs prennent contact avec les victimes de fraude à l'investissement, en affirmant pouvoir les aider à récupérer l'argent volé, à la condition, naturellement, que de nouveaux paiements soient effectués en avance, en échange de ce prétendu service», détaille l'OFCS.

Les victimes sont-elles beaucoup trop crédules? «Expliquer le problème des escroqueries à l'investissement en ligne uniquement par la naïveté des internautes ne reflète pas toute la réalité, car ces fraudes sont de mieux en mieux conçues, ce qui rend leur identification complexe, même pour les utilisateurs expérimentés», estime Yan Borboën. Et les autorités ne devraient-elles pas agir à la racine? «Concernant le laxisme perçu de l'Etat, il s'explique par la difficulté des institutions à suivre l'évolution rapide des attaques alimentées par l'IA et à adapter leurs réponses, plutôt que par un manque d'implication», affirme l'expert.

### Rançongiciel sur demande

Il y a enfin le point des attaques par rançongiciel (ou *ransomware*), qui paralysent les systèmes informatiques des entreprises et volent des données, les pirates exigeant ensuite une rançon pour que la victime les récupère – les menaçant dans le cas contraire de les publier. De 44, le nombre d'annonces est passé à 57 cette année, avec à la clé des dizaines de millions de francs perdus par les entreprises. Et le récent piratage de Logitech indique que le phénomène se poursuit. Les groupes de rançongiciel parviennent ainsi à modifier, voire à désactiver les produits de sécurité en place, afin d'éviter toute détection précoce, note l'OFCS.

Une tendance inquiétante se dessine. Les développeurs proposent, sur des plateformes prêtes à l'emploi, les instruments nécessaires aux différentes étapes d'une attaque par rançongiciel (p. ex. exfiltration des données, chiffrement, communication et paiement), détaille l'OFCS, permettant à n'importe qui de lancer des attaques. «Malgré le fait que les attaques par *ransomware* soient connues, 20% des organisations mondiales les considèrent encore comme l'une des menaces les moins maîtrisées, notamment à cause de l'élargissement de la surface d'attaque lié à la multiplication des objets connectés. Les entreprises doivent ainsi sécuriser un environnement toujours plus vaste face à des attaques complexes, ce qui demande plus de ressources», avertit Yan Borboën. Et même si, d'après l'étude «PwC Global Digital Trust Insights Survey 2026», 78% des organisations suisses prévoient d'augmenter leur budget dans ce domaine d'ici à 2026, le niveau de vulnérabilité des PME reste très élevé. ▬

### MAIS ENCORE

**L'«arnaque au président» toujours en vogue**
Selon l'OFCS, l'essor du phénomène de l'arnaque au président constaté l'année dernière s'est poursuivi. Les 605 tentatives d'arnaque au président signalées durant le premier semestre ont été presque aussi nombreuses que toutes les annonces de 2024. Les communes, les écoles et les églises en ont à nouveau fait les frais. (LT)

## Comment déceler en un éclair les messages suspects

**OUTILS Le site Flairsafe.ch permet d'analyser rapidement le contenu de SMS et d'e-mails douteux. Il faut en parallèle faire preuve de prudence en permanence**

Détecter des fautes d'orthographe, observer les images, les liens ou encore le ton du message: ce sont les principes de base lorsque l'on se trouve face à un message non sollicité, que ce soit un e-mail, un SMS, voire une notification reçue via WhatsApp ou Telegram. Depuis quelques jours, un nouveau site offre une analyse rapide et gratuite de tout contenu douteux, Flairsafe.ch.

Flair a été développé par Sandy Lavorel, spécialiste passionné de la lutte contre la fraude au sein de Vyntra, une société vaudoise active dans la détection des crimes financiers et basée à Yverdon. Il précise que la plateforme est une initiative strictement personnelle, créée en dehors de toute activité professionnelle et sans lien avec son employeur actuel. Le site permet de détecter les arnaques à partir de simples captures d'écran ou de messages reçus.

Pour utiliser l'outil, il faut soit effectuer un copier-coller du message douteux, soit charger une capture d'écran sur le site. Quelques secondes plus tard, le verdict apparaît, indiquant si le contenu est dangereux ou non. Nous l'avons par exemple testé avec un e-mail prétendument envoyé par les CFF, promettant un remboursement pour une facture payée à double. Résultat: le risque est jugé «élevé» par le site, car «ce message use de promesses de remboursement pour inciter à cliquer sur un lien suspect». Les signaux d'alerte principaux sont «l'usage d'un remboursement inattendu pour incitation au clic», «un lien raccourci ou non officiel (exemple: «swisspass.ch/erstattung» au lieu d'un sous-domaine officiel de Sbb.ch)» mais aussi l'«absence de destinataire personnalisé (e-mail générique, pas de nom mentionné)».

### Avec de l'IA générative

L'outil, encore en développement, ne garantit pas à 100% des résultats exacts. «Flair repose aujourd'hui principalement sur de l'IA générative, combinée à une approche d'analyse structurée des contenus suspects. L'outil a été optimisé avec de vrais exemples d'arnaques, récoltés, analysés et annotés par mes soins. J'ai également travaillé avec un groupe de testeurs qui ont évalué les premiers prototypes et permis d'améliorer l'ergonomie et la qualité des réponses. A ce jour, plus de 400 contenus suspects ont été analysés via Flair», détaille Sandy Lavorel.

Le spécialiste précise que «l'objectif n'est pas de fournir une vérité absolue, mais un diagnostic fiable et compréhensible, pour aider chacun à prendre une décision éclairée». Pour la suite, Sandy Lavorel songe à ouvrir son outil à d'autres canaux vecteurs d'arnaques (WhatsApp, Messenger, X, Instagram...), mais aussi à effectuer une connexion «avec les autorités et institutions pour faciliter le signalement sécurisé des arnaques».

### Innombrables conseils

De son côté, l'Office fédéral de la cybersécurité (OFCS) livre de nombreux conseils sur son site. Il faut par exemple activer autant que possible l'authentification multifactorielle (mot de passe puis code par SMS) pour renforcer la sécurité de vos comptes. «Cette méthode, qui réduit significativement le risque de violation de données, peut cependant tout de même être déjouée par des techniques d'ingénierie sociale», avertit aussi l'OFCS. Il faut aussi se méfier des demandes frauduleuses, transmises par courriel ou par SMS, invitant à confirmer des accès ou à divulguer votre code. Et il ne faut pas oublier qu'il est facile de falsifier une adresse électronique ou un numéro de téléphone afin de rendre un message plus crédible. Enfin, ne jamais inscrire de données de votre carte de crédit ou d'autres données sensibles sur une page ouverte à partir d'un lien reçu par courriel ou SMS. ▬ A. S.