ARNAQUES EN LIGNE
Beaucoup plus de victimes recensées en 2019

Chantage à la webcam, piratage de compte et *phishing* sont les attaques sur Internet les plus fréquentes de l'année dernière, selon le rapport d'activité du site Cybermalveillance.

— Par **MARIE BOURDELLÈS**

Un « score » de 28 855 en 2018 puis de 90 604 en 2019 : en un an, les demandes d'assistance ont bondi de 214 % sur la plateforme Cybermalveillance.gouv.fr, dédiée aux victimes de cyberattaques, des particuliers dans 90 % des cas. Si une telle hausse signifie que le dispositif a gagné en visibilité auprès de la population, elle témoigne aussi de l'ampleur d'un nouveau type de menace numérique qui a explosé en 2019 : le chantage à la webcam. Particulièrement important en début d'année (*QC* n° 579), ce phénomène représente, à lui seul, 38 % des tentatives d'arnaques recensées par le site. Le piratage de compte et le *phishing* (hameçonnage), eux, continuent de faire des ravages. Autant de modes opératoires pour aboutir à un objectif unique : extorquer aux internautes leurs données personnelles et/ou bancaires ou de l'argent.

Des escrocs organisés en réseaux

Comme *Que Choisir* l'a révélé tout au long de l'année dernière, les escrocs rivalisent d'imagination et s'organisent en réseaux internationaux, afin de piéger les internautes par e-mail, sur les réseaux sociaux ou encore via de faux sites. En ce début 2020, rançongiciels (demandes de rançon à la suite d'un vol de données) et faux supports techniques, notamment, ne cessent de progresser. La prudence reste donc de mise. Surtout lorsque l'on sait que 9 Français sur 10 ont déjà été confrontés à de la cybermalveillance[1]. Cédric O, secrétaire d'État chargé du Numérique, a annoncé, lors du Forum international de la cybersécurité (FIC) 2020, qui s'est tenu fin janvier, le lancement du Campus Cyber, à Paris, d'ici au premier semestre 2021. L'ambition ? Réunir pouvoirs publics et structures privées en un même lieu afin de renforcer la sécurité numérique en France mais également en Europe. Si l'alliance public-privé est le nouveau mot d'ordre gouvernemental pour combattre les cyberattaques, celui des consommateurs demeure, pour l'instant, inchangé : vigilance ! ◆

9 Français sur 10 déjà confrontés à la cybermalveillance

(1) Source : étude menée en juin 2019 par Cybermalveillance et l'Institut national de la consommation.

CYBERMALVEILLANCE.GOUV.FR
Le site national fait peau neuve

Cybermalveillance.gouv.fr est né, en 2017, d'une volonté gouvernementale. Cette plateforme assiste les victimes de cyberattaques, mène des actions de prévention et fournit des éléments statistiques. L'UFC-Que Choisir fait partie des 40 partenaires du dispositif. Une version revue et corrigée du site a été lancée le 4 février. Grande nouveauté : la mise en relation avec l'un des spécialistes en sécurité informatique référencés se fait désormais par son intermédiaire. Il s'agit, pour la plupart, de petites structures, dotées de diverses compétences (applications Web, objets connectés…). Une fois que le consommateur a trouvé l'entreprise ou l'association idoine, il traite en direct avec cet interlocuteur, qui peut lui proposer une solution et lui envoyer un devis (pour désinfecter, réinstaller des logiciels…). Ce service est en phase d'expérimentation. Il reste à parier sur la réactivité des prestataires pour qu'il se pérennise.