Achats en ligne : renforcer sa sÃ©curitÃ© pour les fÃªtes de fin dâannÃ©e
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 25/11/2022 13:00:00

Les fÃªtes de fin dâannÃ©e approchent, offrant aux cybercriminels lâoccasion rÃªvÃ©e pour rÃ©aliser des tentatives de fraudes. En effet, les pÃ©riodes de pic dâachats et de promotions, telles que Black Friday et Cyber Monday, entraÃ®nent une augmentation du nombre de transactions en ligne, et les hackers guettent les clients imprudents.

Selon une rÃ©cente Ã©tude menÃ©e par Toluna Harris Interactive, en partenariat avec la Fevad, 70 % des cyberacheteurs franÃ§ais prÃ©voient de participer au Black Friday cette annÃ©e.

Selon Fabrice De Vesian, Channel Manager chez Yubico, la sÃ©curisation des comptes doit rester une prioritÃ© lors des achats en ligne. Pour y parvenir, les utilisateurs doivent miser sur quelques bonnes pratiques en matiÃ¨re de cybersÃ©curitÃ© qui permettent de contrecarrer toute activitÃ© malveillante.

Â« A lâoccasion du Black Friday et du Cyber Monday, les consommateurs doivent redoubler de vigilance afin de protÃ©ger leurs informations personnelles.

Les cybercriminels, Ã lâaffÃ»t de la moindre faille, profitent en effet de ces Ã©vÃ¨nements trÃ¨s attendus pour mener Ã bien leurs attaques, en particulier par phishing, cette technique visant Ã rÃ©cupÃ©rer les donnÃ©es personnelles et bancaires de leurs victimes.

Les attaquants contactent gÃ©nÃ©ralement leur cible par email ou SMS, avec des offres dÃ©fiant toute concurrence, puis ils la redirigent vers un site malveillant dont l'apparence correspond Ã celle du site lÃ©gitime, afin quâelle y saisisse ses donnÃ©es personnelles.

Dans ce contexte de cybermenace omniprÃ©sente, il est donc primordial de se mÃ©fier pour ne pas tomber dans le piÃ¨ge, mais aussi de sÃ©curiser au maximum les accÃ¨s Ã ses comptes en ligne. Pour y parvenir, il existe une mesure trÃ¨s simple qui consiste Ã adopter lâauthentification forte.

Les moyens de connexion simples, utilisant un mot de passe, ne constituent en effet plus un mode de dÃ©fense efficace contre les cyberattaques. Quelle que soit leur complexitÃ©, ils restent vulnÃ©rables et ne rÃ©sistent pas aux efforts de hackers motivÃ©s.

Pour aller plus loin, et assurer sa sÃ©curitÃ© en ligne, la mise en place dâune authentification Ã deux facteurs (2FA) est donc fortement recommandÃ©e. Elle implique une deuxiÃ¨me vÃ©rification, au-delÃ de la simple combinaison mot de passe/nom dâutilisateur, et constitue ainsi un barrage supplÃ©mentaire pour le cybercriminel.

Toutefois, toutes les mÃ©thodes dâauthentification multifacteur ne se valent pas et câest important de le savoir. En effet, certaines sont plus faciles Ã dÃ©tourner par les hackers qui mettent sans cesse au point de nouvelles techniques.

Les codes envoyÃ©s par SMS ou les applications d'authentification mobile notamment, ne sont pas toujours Ã la hauteur pour contrer des attaques telles que le phishing ou le SIM-Swapping. Cette technique, qui prend de lâampleur, consiste, Ã usurper le numÃ©ro de tÃ©lÃ©phone de la victime en rÃ©cupÃ©rant une nouvelle carte SIM.

En gÃ©nÃ©ral, le cybercriminel contacte lâ□□opÃ©rateur et demande une nouvelle carte en se faisant passer pour sa cible, aprÃ¨s avoir rÃ©cupÃ©rÃ© des informations personnelles ; qui peuvent Ãªtre trouvÃ©es facilement sur Internet et les rÃ©seaux, afin dâ□□usurper son identitÃ©.

Tandis que les mÃ©thodes dâ□□attaques des hackers deviennent toujours plus sophistiquÃ©es, un niveau de sÃ©curitÃ© supÃ©rieur est requis, et il peut Ãªtre franchi avec une clÃ© de sÃ©curitÃ© physique. Une fois connectÃ©e Ã un ordinateur via un port USB, elle sÃ©curise l'accÃ¨s aux comptes en ligne. Ce facteur dâ□□authentification a lâ□□intÃ©rÃªt de la possession, car il est impossible pour les cybercriminels dâ□□accÃ©der aux comptes en ligne sâ□□ils ne possÃ¨dent pas la clÃ© en main propre.

A lâ□□approche des fÃªtes, les cybercriminels redoublent dâ□□efforts pour profiter des erreurs commises par les consommateurs, et voler des informations critiques.

Afin de dÃ©jouer toute tentative de fraude, il est essentiel de rester sur la dÃ©fensive, de ne pas tomber dans le piÃ¨ge dâ□□une offre qui semblerait trop belle et de renforcer sa cybersÃ©curitÃ© par le biais de lâ□□authentification forte.

La couche de dÃ©fense supplÃ©mentaire confÃ©rÃ©e par celle-ci, permet de bloquer lâ□□accÃ¨s non autorisÃ© aux comptes, et par extension aux donnÃ©es sensibles. Par ailleurs, une authentification multifacteur physique, telle quâ□□une clÃ© de sÃ©curitÃ©, assure une sÃ©curitÃ© additionnelle, car elle ne peut Ãªtre contournÃ©e.

Ces bonnes pratiques, ainsi quâ□□une prise de conscience accrue des cyber-risques, sont essentielles pour sÃ©curiser ses achats en ligne tout au long de lâ□□annÃ©e. Â»