Conseils pour contrer le phishing et renforcer la cybersÃ©curitÃ©
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 10/11/2023 14:00:00

A l'approche des fÃªtes de fin d'annÃ©e, une augmentation significative des dÃ©penses en ligne se profile Ã l'horizon. Cette augmentation des transactions numÃ©riques crÃ©e une opportunitÃ© idÃ©ale pour les cybercriminels, qui en profitent pour lancer des campagnes de phishing visant Ã dÃ©rober les informations bancaires de leurs cibles.

Selon une rÃ©cente Ã©tude de la FÃ©dÃ©ration Bancaire franÃ§aise, prÃ¨s de 9 FranÃ§ais sur 10 estiment que leurs donnÃ©es bancaires sont sensibles, mais ils semblent malgrÃ© tout nÃ©gliger les mesures de prÃ©caution face aux risques en ligne. Or, plus de la moitiÃ© des FranÃ§ais dÃ©clarent avoir dÃ©jÃ Ã©tÃ© confrontÃ©s Ã des tentatives d'arnaque visant leurs donnÃ©es financiÃ¨res.

Selon Fabrice de VÃ©sian, Sales Manager chez Yubico, bien que les consommateurs soient conscients des cyber-risques, cela ne les dissuade pas pour autant de partager leurs donnÃ©es sensibles ou dâ□□enregistrer leurs identifiants en ligne. Toutefois, il est impÃ©ratif qu'ils adaptent leur comportement en matiÃ¨re de cybersÃ©curitÃ© pour contrer lâ□□Ã©volution croissante des attaques en ligne, et notamment celles de phishing :

Â« Bien qu'il soit techniquement facile pour les sites de vente en ligne de mettre en Å□uvre une authentification de base par nom d'utilisateur et mot de passe pour leurs clients, ces types d'identifiants seuls sont faciles Ã contourner pour les cybercriminels. En effet, ils ouvrent la porte Ã un accÃ¨s non autorisÃ© aux comptes internet.

Pendant les mois de forte activitÃ© des achats en ligne, les consommateurs peuvent Ãªtre tentÃ©s d'adopter des habitudes risquÃ©es, telles que la rÃ©utilisation des mots de passe entre les services ou le fait de cliquer sur des liens d'information sur les commandes qui semblent lÃ©gitimes.

Dans ce sens, nos recherches rÃ©vÃ¨lent que prÃ¨s de 40 % dâ□□entre eux utilisent le mÃªme mot de passe pour plusieurs comptes, ce qui permet aux cybercriminels de s'y infiltrer plus facilement. Ces pratiques exposent dÃ¨s lors les consommateurs Ã un risque plus Ã©levÃ© de compromission de leurs comptes.

Pour garantir leur sÃ©curitÃ© en ligne, il est essentiel que les consommateurs adoptent des pratiques concrÃ¨tes plus sÃ©curisÃ©es, telles que lâ□□authentification multi-facteur (MFA) rÃ©sistante au phishing, et quâ□□ils arrÃªtent les mots de passe simples et identiques dâ□□un site Ã lâ□□autre.

Cependant, nos recherches rÃ©vÃ¨lent qu'actuellement, environ une personne sur deux ne sait pas si elle a activÃ© la MFA pour ses comptes en ligne actifs. Il y a donc une prise de conscience des cybermenaces, mais une mÃ©connaissance des moyens disponibles et trÃ¨s facilement accessibles Ã tous pour sâ□□en prÃ©munir.

Une grande partie des transactions en ligne repose par ailleurs sur la croyance que le site internet qui propose des produits ou des services Ã la vente est vÃ©ritablement ce qu'il prÃ©tend Ãªtre et qu'il garantit la protection adÃ©quate des donnÃ©es personnelles et bancaires de ses clients.

Bien que les consommateurs nourrissent des rÃ©serves Ã l'Ã©gard des opÃ©rations en ligne, ils continuent de partager et de conserver leurs informations sensibles sur ces sites. Selon nos recherches, il est prÃ©occupant de constater que prÃ¨s d'un tiers des personnes interrogÃ©es (32 %) ne se sentent pas en mesure d'identifier un site d'e-commerce frauduleux.

La majoritÃ© des FranÃ§ais prÃ©voient certainement de faire des achats en ligne entre novembre et dÃ©cembre, ce qui en fait le moment idÃ©al pour revoir leurs habitudes en matiÃ¨re de sÃ©curitÃ© en ligne. Bien que des progrÃ¨s restent Ã accomplir pour renforcer la sÃ©curitÃ© en ligne, la premiÃ¨re mesure Ã prendre consiste Ã revoir les mÃ©thodes de connexion existantes.

Cela implique la crÃ©ation d'identifiants uniques stockÃ©s dans un gestionnaire de mots de passe fiable et l'activation de l'authentification multi-facteur pour protÃ©ger leur compte.

La mise Ã jour de leurs mÃ©thodes de connexion pour intÃ©grer des solutions d'authentification multi-facteur robustes et rÃ©sistantes au phishing, comme l'utilisation d'une clÃ© de sÃ©curitÃ©, doit Ã©galement Ãªtre considÃ©rÃ©e, car elle constitue un vÃ©ritable rempart face aux cybermenaces. En suivant ces Ã©tapes, les consommateurs pourront efficacement se protÃ©ger efficacement contre toute tentative de fraude en ligne, assurant ainsi une expÃ©rience plus sÃ©curisÃ©e et sereine lors de leurs achats et transactions sur Internet. Â»