Soldes et rÃ©servations d'Ã©tÃ© : se protÃ©ger des attaques de phishing
Internet
PostÃ© par : JerryG
PubliÃ©e le : 24/7/2023 14:00:00

Alors que les soldes d'Ã©tÃ© s'intensifient et que les rÃ©servations de vacances de derniÃ¨re minute sâ□□accÃ©lÃ¨rent, les transactions en ligne connaissent une hausse importante. Les consommateurs Ã l'affÃ»t des meilleures offres entraÃ®nent une augmentation du trafic en ligne. Dans ce contexte, les pirates informatiques sont aux aguets, prÃªts Ã infiltrer des comptes peu sÃ©curisÃ©s en recourant Ã des attaques de phishing.

Pour Fabrice de VÃ©sian, Sales Manager France chez Yubico, les consommateurs doivent Ãªtre davantage sensibilisÃ©s aux cyber-risques afin de mieux se protÃ©ger lorsqu'ils surfent sur Internet :

Â« Dans le climat Ã©conomique actuel, les consommateurs sont plus soucieux de leur budget que jamais, et recherchent activement des bonnes affaires.

Â Cependant, cette chasse aux Ã©conomies donne potentiellement aux cybercriminels une occasion supplÃ©mentaire de dÃ©ployer des attaques par phishing. Les acheteurs qui ne se sont pas protÃ©gÃ©s par un systÃ¨me dâ□□authentification multifacteur (MFA) adÃ©quat, tel qu'une clÃ© matÃ©rielle sÃ©curisÃ©e, s'exposent Ã des cyberattaques. Celles-ci peuvent prendre la forme de SMS trompeurs dÃ©guisÃ©s en notifications de livraison de colis ou de liens malveillants demandant au client de donner suite Ã une commande.

Les cybercriminels se nourrissent Ã©galement du sentiment d'urgence et de peur pour manipuler leurs victimes, et les inciter Ã prendre des mesures immÃ©diates.

C'est pourquoi les consommateurs doivent rester prudents face aux emails faisant Ã©tat de stocks limitÃ©s, de demandes de paiement urgentes ou de menaces de suspension de compte. VÃ©rifier ces requÃªtes en contactant directement les canaux officiels dâ□□une entreprise est un excellent moyen de contrecarrer ces menaces.

Face Ã la multiplication des violations de donnÃ©es, l'adoption d'un deuxiÃ¨me facteur d'authentification n'est pas seulement conseillÃ©e, elle est indispensable.

L'activation de l'authentification Ã deux facteurs (2FA) permet de renforcer la sÃ©curitÃ© des comptes car elle exige une deuxiÃ¨me forme de vÃ©rification avant d'accorder l'accÃ¨s Ã un compte. Il peut s'agir d'un Ã©lÃ©ment biomÃ©trique ou d'un code PIN, ce qui complique la tÃ¢che des hackers souhaitant obtenir un accÃ¨s non autorisÃ©.

ParallÃ¨lement Ã ces mÃ©thodes, les utilisateurs doivent Ãªtre conscients des derniÃ¨res pratiques et tendances en matiÃ¨re de phishing et s'en tenir informÃ©s.

Aujourd'hui, alors que des technologies Ã©prouvÃ©es dans la rÃ©solution de problÃ¨mes de sÃ©curitÃ© informatique sont disponibles, la sensibilisation des consommateurs sur la protection en ligne est en effet essentielle. Les recherches montrent qu'environ 90 % de toutes les atteintes Ã la sÃ©curitÃ© impliquent une fuite de mot de passe ou une autre mÃ©thode d'authentification faible.

Cependant, la comprÃ©hension de base des diffÃ©rentes solutions d'authentification et d'autres

pratiques simples Ã suivre pour rÃ©duire 90 % des compromissions, n'a pas encore atteint le grand public. Dans ce sens, la sensibilisation aux signes d'alerte et Ã une meilleure cyber-hygiÃ¨ne favorise une culture de la prise de conscience qui, Ã terme, peut aider Ã lutter contre les tentatives de phishing.

Alors que les soldes d'Ã©tÃ© sont source de ferveur et d'offres allÃ©chantes, les consommateurs doivent donner la prioritÃ© Ã leur sÃ©curitÃ© en ligne, notamment contre les attaques de phishing, qui constituent une menace importante pendant cette pÃ©riode. En restant vigilants, en suivant les recommandations et en adoptant des mesures de sÃ©curitÃ© proactives, ils peuvent minimiser les risques et profiter d'une expÃ©rience d'e-shopping plus sÃ»re Â».