Après Hotmail, les attaques par phishing visent aussi Gmail, Yahoo et AOL

Microsoft n'est pas le seul à s'attirer l'attention des cybers-criminels avec Hotmail. **Yahoo et Google** viennent de reconnaître avoir eux aussi été victimes de campagnes d'attaques en règle.

Selon la *BBC*, **deux listes de comptes piratés** auraient été diffusés sur Internet. La première, de 10 000 comptes, se concentre sur le service Microsoft Hotmail. La seconde, de 20 000, touche cette fois les services Gmail, Yahoo Mail et AOL. Au total, 30 000 identifiants (nom et mot de passe) se baladent en ligne, notamment sur Pastebin.com, un site de partage de code dédié aux développeurs et où a été posté la première liste mais qui depuis l'a retiré de ses pages.

Google a ainsi reconnu que son service de webmail Gmail avait subi diverses attaques par phishing. Selon Mountain View, le problème concernerait **moins de 500 comptes de messagerie**. Mais Google déclare avoir eu accès à une troisième liste de comptes piratés et diffusée sur Internet dont il ne dévoile pas le nombre de cas concernés.

Pour mémoire, le phisihing est une arnaque qui consiste à pousser un internaute à dévoiler ses données personnelles (comptes de courriels, de banque en ligne, etc.) aux pirates qui les exploitent, ou non, ensuite à leurs comptes (revente des données, spam, *etc.*). L'attaque des comptes webmail s'appuie donc sur **une erreur humaine** et non pas sur une faille technique dans ces cas précis.

Face à ce fléau qui sait si bien exploiter la crédulité des internautes, les entreprises ne peuvent que renouveler leur conseils pour préserver l'intégralité des comptes. Google recommande, notamment pour les victimes, de **changer le mot de passe** de leur compte, mais aussi la question secrète (qui permet de retrouver ce mot de passe) et la seconde adresse e-mail qui sert généralement de roue de secours ainsi que d'utiliser un navigateur récent doté d'un filtre anti-phishing, activé bien sûr. Et, bien sûr, ne pas répondre instinctivement au premier courriel incitant à saisir ses identifiants sous n'importe quel prétexte…