Pourquoi nous nous faisons toujours piéger par de faux e-mails.

*Le phishing (ou hameçonnage) a connu une évolution impressionnante. Avant c’était la pratique d’envoyer des millions d’e-mails dans l’espoir qu’une nouvelle victime morde à l’hameçon. Tout comme d’autres formes de cybercriminalité, le phishing s’est fort développé (et demande donc une réponse subtile).*

Les chiffres de Sophos démontrent que les faux mails essaient de tromper des organisations jour et nuit. Ils constituent une attaque continue sur la vie d’entreprise : 41% des organisations reçoivent des faux mails quotidiennement (voire plusieurs fois par jour) et plus de deux tiers (77%) en reçoivent au moins un par mois. La nouvelle la plus inquiétante est que 30% de ces mails phishing soient ouverts. Malgré les campagnes de sensibilisation et les formations, les cybercriminels arrivent donc toujours à induire les gens en erreur.

Il est par conséquent extrêmement important d’avoir une bonne idée de leur façon d’agir. Sophos comprend quels mails atteignent leur but, qui est le plus souvent pris d’assaut, et quelles sont les (combinaisons de) technologies et formations qui permettent de sécuriser une organisation au maximum. Nous pouvons démontrer par exemple que la comptabilité et les finances sont les départements les plus visés. Toutefois, l’administration et le management suivent de près. Voilà pourquoi il est indispensable de combiner les technologies protectrices et les formations spécifiques et sur mesure, qui reflètent les rôles des individus.

Citons les propos de John Shier de Sophos :

*“Vu que la qualité des mails phishing s’est améliorée, il est important de retenir que certains destinataires sont induits en erreur. Les utilisateurs forment la première ligne de défense contre une attaque de hameçonnage. L’éducation est très importante pour garantir la sécurité d’une entreprise. Mais la possibilité pour un utilisateur de signaler un mail suspect l’est d’autant plus. Il faudrait que tout utilisateur puisse signaler une attaque de phishing de façon simple et sans qu’il y ait de conséquences, même s’il a été trompé. Le système d’une alerte précoce est crucial pour toute organisation qui veut réagir vite et avec fermeté contre une attaque de hameçonnage.”*

Vous trouverez le rapport des constats de Sophos ici. Si vous voulez discuter de ces informations, ou faire plus de recherches à propos de l’impact du phishing (ou savoir pourquoi et comment tant de personnes tombent toujours dans le piège), je peux vous mettre en contact avec les spécialistes de Sophos en Belgique ou à Londres. Nous disposons également d’une boîte à outils ‘anti-phishing’ et de notre whitepaper ‘Don’t take the bait’ (Ne mordez pas à l’hameçon) pour en écrire un article parlant et bien élaboré.