為什麼員工會掉進網路釣魚攻擊的陷阱

許多資料外洩或資安事件是源自網路釣魚攻擊，您可能認為難以置信，怎麼可能會有人對網路釣魚攻擊一無所知？

1. 對網路釣魚威脅缺乏警覺心

各大知名資安新聞網站不乏對網路釣魚攻擊這個話題的探討，甚至連許多主流新聞媒體也有所報導，不但有許多相關的研究和統計，也經常引發熱議。

相較於網路安全新聞和研究報告，社群媒體上的網路紅人和戲劇影片可能還比較能引起一般職員的興趣。即便你透過電子郵件向他們宣導資安方面的新聞和報告，他們也很可能不會去閱讀這些內容（或者只是概略看過而未詳讀）。

BSI 的合作夥伴之一 Wombat Security Technologies 在去年發表了 2017 網路釣魚報告（State of the Phish report 2017），該報告針對英美兩國各 1,000 名上班族對於網路釣魚攻擊的認知程度進行一項獨立調查。儘管有超過半數的員工確實知道什麼是網路釣魚 (大致瞭解)，但仍有 35% 美國受訪者以及 28% 英國受訪者對此完全不瞭解。

在今年最新的 2018 網路釣魚報告，除了美國與英國外，還增加了 1,000 名的德國受訪者，然而這三地仍有 39% 美國、27% 英國及 29% 德國的受訪者，顯示出民眾對於網路釣魚的認知與我們預期的程度差距相當大。

事實上，如果您沒有經常透過各種方式與職員溝通，並使用能讓他們產生共鳴的語言和素材，那麼您針對網路釣魚提出的警告大概也就不會引起任何迴響。

2. 對網路釣魚威脅有所認知，但不知如何應對

我們傾向使用「安全認知與教育訓練」這個詞，而不是「安全認知訓練」。原因很簡單：認知和訓練是兩碼子的事。

讓員工們意識到威脅存在，與教導他們在日常業務活動中遭遇安全威脅時該如何識別並加以回應，這是截然不同的兩件事。讓員工知道網路釣魚事件正在組織內肆虐，這固然算是小小的成就，但是要打贏這場戰爭，您需要透過反釣魚訓練工具，教育員工攻擊者會採用不同類型的社交工程手法來誘騙員工點選、下載，甚至送出敏感資料。

3. 人性就是如此

這或許不中聽，但是以零漏洞做為目標是不切實際的做法，因為我們不可能完全忽視人性的因素。人非聖賢，孰能無過。任何人都可能犯錯，您我也不例外。不過，我們絕無意要您打消念頭，徹底放棄安全認知和教育訓練。因為，正如同這條網路安全公式所說的：

認知能讓您的員工三思而行，而教育則讓他們獲得改變行為所需的知識。完全缺乏意識的員工很可能在點選連結時來者不拒，接受過訓練的員工會做出較為明智的決定，避免犯下錯誤，並且更有可能提醒您可疑的電子郵件，讓您的資安回應團隊能夠主動出擊，而非只是反應式的防禦。

既然您能容忍垃圾郵件篩選器、防毒軟體以及各種技術性的防護並非百分之百的安全，那麼您也要能理解組織成員對安全認知的知識可能不足。

減少漏洞的重點在於管理風險，而不是完全杜絕它

根據反釣魚工作小組（Anti-Phishing Working Group, APWG）2017 年上半年度的「網路釣魚活動趨勢報告」，發現網路釣魚攻擊的數量不僅年年升高，更有 640 家品牌商成為這類攻擊的固定目標，這些攻擊頻率從每隔幾周，甚至是每天都發生，且針對金融機構，物流和運輸以及雲端存儲公司的攻擊事件也有所增加。

面對驚人的攻擊數量與持續變化的攻擊趨勢，將「人」的因素加以管控，並結合對網路罪犯的專注力，才可能明顯降低網路安全風險。如果組織職員的風險管理目前不屬於您網路安全規劃的範圍...那麼，您還在等什麼？ 具體來說，安全認知和教育訓練計劃可以提供合乎經濟效益、著重結果的方式，給員工帶來即時影響，並能達到長期的改善的效果。

- 點此 下載 2018 網路釣魚報告（State of the Phish report 2018）
- BSI 訓練學苑協助各大企業組織進行員工網路安全意識訓練，根據當前網路風險趨勢、組織產業屬性及預算規劃包班課程，歡迎 洽詢 獲得更多資訊。