

Sophos, firma specjalizująca się w technologiach ochrony informacji, radzi firmom, aby te przyjrzały się swoim praktykom bezpieczeństwa, po tym, jak Facebookowa strona fanowska muzeum Van Gogha w Amsterdamie znalazła się na celowniku scammerów.

Na zaatakowanej witrynie zostały umieszczone wiadomości i linki do generującego oszustom przychód scamu: "Byłem zalogowany XXXX godzin na Facebooku w 2010".

Muzeum Van Gogha umieściło aktualizację na swojej stronie, przeprasząc za wiadomości spam i pytając, w jaki sposób zapobiegać podobnym sytuacjom w przyszłości:

"Przepraszamy za wiadomości spam informujące, ile godzin byliśmy zalogowani na portalu, które automatycznie pojawiają się na naszej stronie. My ich nie umieszczamy! Czy ktoś wie, jak możemy zapobiec temu w przyszłości?"

W tym przypadku zamieszczone przez scammerów informacje spam znalazły się na na stronie fanowskiej muzeum Van Gogha za pośrednictwem 'Mobile Updates'.

Funkcja ta umożliwia użytkownikom Facebooka aktualizowanie statusu lub wysyłanie zdjęć i filmów prosto do swojego profilu. Do przesyłania służy unikatowy adres e-maila, przypisany tylko do konkretnego konta na Facebooku.

"Jeśli ktoś był w stanie rozszyfrować unikatowy adres email muzeum do wrzucania zdjęć, byłby też zdolny do umieszczania zdjęć oraz linków scam, z łatwością," powiedział Graham Cluley, starszy konsultant ds. technologii w Sophos. "Najwyższa pora, aby muzeum odświeżyło swój adres do mobilnych aktualizacji."

Firmom korzystającym z Facebooka zaleca się zaimplementowanie ostrych polityk bezpieczeństwa, aby zredukować szanse zostania ofiarą kampanii scam lub spam, które mogą dotknąć innych użytkowników.

"Administratorzy muzeum Van Gogha będą musieli upewnić się, czy wybrali trudne do złamania, unikatowe hasło i usunąć każdą podejrzaną aplikację, której mogli, przez przypadek, pozwolić na swobodny dostęp do profilu," dodał Cluley.

Sophos opublikował więcej informacji, wraz ze screenshotami, na blogu Naked Security pod adresem: <http://nakedsecurity.sophos.com/2011/02/10/van-gogh-museum-hit-by-facebook-scammers/>

Dołącz do grupy <http://www.facebook.com/SophosSecurity> i śledź na bieżąco informacje o zagrożeniach i jak ich unikać.

Sophos