thestar.com

Mock email scam at Justice Canada snares hundreds of bureaucrats

An internal security exercise in the Justice Department shows almost 2,000 staff members were conned into clicking a phoney phishing link.

Dean Beeby, The Canadian Press, June 21, 2014

OTTAWA—Many of the Justice Department's finest legal minds are falling prey to a garden-variety Internet scam.

An internal survey shows almost 2,000 staff were conned into clicking on a phoney "phishing" link in their email, raising questions about the security of sensitive information.

The department launched the mock scam in December as a security exercise, sending emails to 5,000 employees to test their ability to recognize cyber fraud.

The emails looked like genuine communications from government or financial institutions, and contained a link to a fake website that was also made to look like the real thing.

Across the globe, an estimated 156 million of these so-called "phishing" emails are sent daily, and anyone duped into clicking on the embedded link risks transferring confidential information — such as online banking passwords — to criminals.

The Justice Department's mock exercise caught 1,850 people clicking on the phoney embedded links, or 37 per cent of everyone who received the emails.

That's a much higher rate than for the general population, which a federal website says is only about five per cent.

The exercise did not put any confidential information at risk, but the poor results raise red flags about public servants being caught by actual phishing emails.

A spokeswoman says "no privacy breaches have been reported" from any real phishing scams at Justice Canada.

Carole Saindon also said that two more waves of mock emails in February and April show improved results, with clicking rates falling by half.

“This is an awareness campaign designed to inform and educate employees on issues surrounding cyber security to protect the integrity of the department’s information systems and in turn better protect Canadians,” she said in an email.

“In this case, this exercise specifically dealt with the threat from phishing, which is increasingly being used as an attack vehicle of choice by cyber criminals.”

“As this project progresses, we are pleased that the effectiveness of this campaign is showing significant improvement.”

A February briefing note on the exercise was obtained by The Canadian Press under the Access to Information Act.

The document indicates there are more such exercises planned — in June, August and October — and that the simulations will be “graduating in levels of sophistication.”

Those caught by the simulation are notified by a pop-up window, giving them tips on spotting malicious messages.

The federal government’s Get Cyber Safe website says about 10 per cent of the 156 million phishing emails globally make it through spam filters each day.

Of those, some eight million are actually opened by the recipient, but only 800,000 click on the links — or about five per cent of those who received the emails.

About 10 per cent of those opening the link are fooled into providing confidential information, which represents a worldwide haul of 80,000 credit-card numbers, bank accounts, passwords and other confidential information every day.

“Don’t get phished!,” says the federal website, “Phishing emails often look like real emails from a trusted source such as your bank or an online retailer, right down to logos and graphics.”

The site says more than one million Canadians have entered personal banking details on a site they don’t know, based on surveys.

In late 2012, Justice Canada was embroiled in a major privacy breach when one of its lawyers working at Human Resources and Skills Development Canada was involved in the loss of a USB key.

The key contained unencrypted confidential information — including medical conditions and SIN numbers — of about 5,045 Canadians who had appealed disability rulings under the Canada Pension Plan. The privacy commissioner is still investigating the breach.

The department has some 5,000 employees and about half of them lawyers.

leSoleil
Actualités Affaires Alimentation Arts et spectacles

2000 fonctionnaires tombent dans le piège d'un courriel malveillant

La Presse Canadienne, le 22 juin 2014

Bon nombre d'employés du ministère fédéral de la Justice sont tombés dans le piège d'un courriel malveillant des plus courants.

Un sondage interne démontre qu'environ 2000 membres du personnel ont cliqué sur un faux lien d'hameçonnage reçu par courriel, soulevant des questions sur la sécurité des informations confidentielles du ministère.

C'est le ministère lui-même qui a lancé le faux pourriel, en décembre, en guise d'exercice de sécurité. Il a envoyé le courriel à 5000 employés afin de tester leur habileté à reconnaître la cyberfraude.

Les courriels ressemblaient aux communications d'institutions financières ou gouvernementales et contenaient un lien vers un faux site Web, également crédible.

Environ 156 millions de courriels frauduleux sont envoyés chaque jour partout dans le monde. Celui qui clique par inadvertance sur un lien qu'il contient risque de partager à des destinataires douteux des informations sensibles, telles que des mots de passe pour des comptes bancaires en ligne, par exemple.

L'exercice du ministère de la Justice a piégé 1850 personnes, soit 37% des adresses visées. Ce taux est beaucoup plus élevé que celui de la population générale, qui est de 5%, selon un site du gouvernement fédéral.

Heureusement, aucune information sensible n'a été compromise, mais les résultats soulèvent des inquiétudes quant à la vigilance des fonctionnaires face aux courriels d'hameçonnage.

Une porte-parole, Carole Saindon, affirme que le ministère de la Justice n'a repéré aucune atteinte à la confidentialité dans les vrais courriels d'hameçonnage reçus au département, en soulignant que le personnel avait obtenu de meilleurs résultats lors de deux autres vagues de faux courriels frauduleux, en février et en avril.

«C'est une campagne de sensibilisation conçue pour informer et éduquer les employés sur les enjeux de la cybersécurité, dans le but de protéger l'intégrité des systèmes d'information du ministère et en bout de ligne, de mieux protéger les Canadiens», a-t-elle expliqué par courriel.

«Dans ce cas-ci, l'exercice portait spécifiquement sur la menace de l'hameçonnage, qui devient de plus en plus la méthode de prédilection des cybercriminels.»

Une note d'information datée de février, obtenue par La Presse Canadienne, indique que d'autres exercices semblables sont prévus en juin, en août et en octobre, et que leur «degré de sophistication» augmentera.

Ceux qui se font prendre par la simulation en sont informés par une fenêtre contextuelle (ou «pop-up») qui donne des conseils pour reconnaître les messages malveillants.

Selon le site «Pensez cybersécurité» du gouvernement, environ 10% des 156 millions de courriels d'hameçonnage envoyés chaque jour réussissent à traverser les filtres antipourriels. De ceux-là, quelque huit millions sont ouverts par le destinataire, mais seulement 800 000 personnes cliquent sur le lien. Environ 10% de ceux qui cliquent se font prendre à donner des informations confidentielles, ce qui représente environ 80 000 numéros de cartes de crédit, de comptes bancaires, de mots de passe et autres informations.