

Live phishing shows risk of personal info

November 9 2005

Despite all the warnings about giving out personal information, many people still freely give away seemingly innocuous details that can be used to crack their passwords, according to the results of a "live phishing" survey.

The 18-question survey, conducted by RSA Security in New York City, asked respondents for information such as birth date, mother's maiden name and pet's name. The survey was touted as being about tourism in New York.

It found that 70 percent of the 108 respondents gave their mother's maiden name, and 90 percent gave their date and place of birth, according to a news release from RSA.

Additionally, almost 85 percent of respondents provided their full name, street address and e-mail address.

"A lot of personal information actually functions like a password and, as such, needs to be robustly protected," said Chris Young, RSA's vice president of consumer authentication services.

According to the news release, the survey was deliberately designed to feel official and safe, to reflect how many phishing attacks use real corporate logos and industry terminology to appear legit.

More than half of respondents explained in the survey how they devise their online passwords. Even those who declined to, though, did give

personal information that can lead to figuring out their password, Young said.

"Many consumers have called their credit card company to check their account and be asked for their mother's maiden name as a personal identifier," said Young, noting one reason not to give out such personal information so freely.

"On top of this," Young said, "with a bit of sleuthing, motivated phishers can guess what a New Yorker's password is just by having his address and trying combinations that assume he's a fan of the Yankees or Knicks."

Federal Trade Commission research found that damage and loss resulting from identity theft and cyber-crime costs nearly \$50 billion annually.

Consumer concerns go beyond their own personal information to the security of companies that index personal data. A controversial bill pending in the House of Representatives called the Data Accountability and Trust Act includes a provision that states that companies whose data are compromised must notify each individual in writing, only if the company terms it a "significant risk."

ChoicePoint Inc. announced last February that thieves posing as small-business owners had gained access to the company's database the previous September. Authorities said that the compromise resulted in at least 750 cases of identity theft.

ChoicePoint only notified its affected customers months after the breach, when it publicly announced it, and some 17,000 customers only received a notice in writing in September 2005, a full year after the breach.

RSA offered several suggestions for people to avoid identify theft. Among them were not sharing your method for devising your password, not sharing any personal details with strangers and using a variety of different passwords.

"Our survey reminds us that we all need to be more aware of such vulnerabilities, and take appropriate precautions," Young said.

Copyright 2005 by United Press International

Citation: Live phishing shows risk of personal info (2005, November 9) retrieved 23 May 2024 from <https://phys.org/news/2005-11-phishing-personal-info.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.