Office of Research Security Newsletter

November 2019

Zynga data breach exposed 200 million Words with Friends players

By Irina Ivanova | October 2, 2019

More than 200 million players of the popular mobile games Words with Friends and Draw Something had their login information stolen.

Publisher Zynga announced there was a data breach of account login info for Draw Something and Words with Friends players on Sept. 12. Now, a hacker has claimed responsibility for the breach, CNET reports.

A hacker that goes by the name Gnosticplayers said they stole data from over 218 million Words with Friends player accounts, CNET wrote. The hacker accessed a database that included data from Android and iOS players who installed the game before Sept. 2, according to the report. Hacker News first reported the story.

The hack exposed users' names, email addresses, login IDs, some Facebook IDs, some phone numbers and Zynga account IDs, according to Hacker News. It did not include financial information, Zynga said, adding that it "has already taken steps to protect users' accounts from invalid logins" if the company believes their information was exposed. It noted that some users were required to change their passwords.

To read the full article – https://www.cbsnews.com/news/words-with-friends-hack-zynga-data-breach-exposes-200-million-users/

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

UPCOMING REFRESHER SECURITY TRAININGS:

- Thursday, Oct 24, BJA RSA – 11:30 am to 1:00 pm

November Movie Month

VBH, M50 - 1:00 pm to 3:30 pm

- Tuesday, November 5, 2019
- Tuesday, November 12, 2019
- Thursday, November 21, 2019
- Monday, November 25, 2019

Designed by Pngtree

Meet the Government's New Security Agency – DCSA Up and Running

Lindy Kyzer / Oct 2, 2019

A new government agency was born yesterday with the start of the fiscal year. The Defense Counterintelligence and Security Agency (DCSA) is now the organization responsible for the background investigations mission and government personnel security program.

The agency launched its new website last week, and the platform trades heavily on the types of questions we see frequently at ClearanceJobs, including how to find out the status of your background investigation, how to verify the identity of your background investigator, and how to fill out your security clearance application.

With the insider threat still one of the most significant challenges the personnel security program faces, and Security Executive Agent Directive (SEAD) 3 widening the reporting responsibilities for those privy to threat information, the newly launched DCSA website wisely provides information about how security clearance holders can self report potentially adverse information, and also how they should report information about others.

SEAD 3 was signed December 14, 2016, but ever since security representatives have speculated as to how the government planned to enforce the new directive. Previously, the security clearance process was dependent upon self reporting potentially adverse information, like new delinquent debt or a divorce. SEAD 3 broadened the scope for all individuals in sensitive positions to report any potentially adverse information they encounter – to include information about security clearance holders they may know, but who don't even work in the same company.

To read the full article –
https://news.clearancejobs.com/2019/10/02/the-governments-new-security-agency-dcsa-up-and-running/

OFFICE OF RESEARCH SECURITY STAFF

DENISE SPILLER, SECURITY ADMINISTRATOR
824-6444 / denise.spiller@uah.edu

JANINE WILISON
ASSOCIATE SECURITY ADMINISTRATOR
824-3025 / janine.wilson@uah.edu

APRIL MCMEANS
ASSISTANT SECURITY ADMINISTRATOR
824-6048 / april.mcmeans@uah.edu

CAITLYN SCHOENIG
SECURITY ASSITANT
824-4717/cns0017@uah.edu

MARIAH WILKINSON
STUDENT SPECIALIST II
824-4818/mw0077@uah.edu

RYAN WILKINSON
STUDENT SPECIALIST I

Pink Ladies of Office of Research Security

We will be out and about visiting your department soon…

Intellectual Property Awareness at Universities: Why Ignorance is Not Bliss

By: John Villasenor | Forbes | November 27, 2012

Recently, I conducted an informal survey of graduate engineering students at UCLA, where I teach, to assess intellectual property (IP) awareness. The results highlight the challenges of promoting and protecting IP in American universities and technology companies, and illustrate why universities need to increase their efforts to educate students on what IP is and why it matters.

First, the numbers: Of the approximately 60 graduate engineering students who completed the survey, 68% stated that they did not know enough to answer the question "what is a trade secret?" 21% stated that they did not know enough to answer the question "what is a patent?" The percentages of students unable to provide an answer to "what is copyright?" and "what is a trademark?" were 32% and 51% respectively.

This problem is even more pressing now that many cash-strapped universities are making IP a key focus of efforts to more effectively leverage their research output. By obtaining a greater number of patents and then licensing them to industry, universities hope to both boost revenues and speed the introduction of the results of their research into the market. In theory, this will benefit universities, companies, and the broader public. But the success of this endeavor relies on the ability of university researchers – who are very often graduate students – to recognize potentially patentable inventions and take the steps necessary to protect them by initiating and participating in the patent prosecution process. The survey results suggest that a key link in this chain may be broken.

To read the full article –
https://www.forbes.com/sites/johnvillasenor/2012/11/27/intellectual-property-awareness-at-universities-why-ignorance-is-not-bliss/#23b25d7613ce

THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE