California Community Colleges | Information Security Center

WHITE PAPER: Reducing Fraudulent CCCApply Applications

A Guide for California Community Colleges | January 2020

CCCApply is the common application for admission to the California Community Colleges, and is used by almost every California community college district. Over the past few years, there has been a startlingly large increase in the number of fraudulent applications submitted through CCCApply. In a few cases, colleges reported receiving as many as 10,000 or more fake applications in a single day.

This application "spam" is more than just annoying. It can be dangerous – especially if it's part of a phishing scam in order to obtain passwords, social security numbers, and other personal information, or used to convince an end-user to reveal sensitive information about themselves or internal computer systems.

In addition to being a security risk, fraudulent applications can waste valuable business resources and server space storing and managing them until they are deleted.

A variety of efforts have sought to prevent this type of fraud, such as using machine learning algorithms within the CCCApply system to look for common signs that applications may be fraudulent. However, the highest degree of success at stemming abuse is achieved when colleges themselves take specific steps to remove incentives for creating fake applications.

Motivations Behind Email Fraud

In order to combat fraudulent applications, it is important to understand the motivation of the bad actors who submit them. Investigation has shown that most of these applicants are seeking to obtain an academic email address, otherwise known as a ".edu" email account, which may be used for financial gain or myriad other benefits, including:

- Sell to other bad actors
- Obtain free software licenses
- Get confirmations of residency
- Use residency to get California IDs
- Potential for serious security attacks

It is widely discussed on hacking forums that most California community colleges generate a .edu email address for a student minutes to hours within receipt of a completed application. Fraudulent applicants receive a fully functioning .edu email account without ever having to register for classes or even attend orientation.

While many fraudulent CCCApply applicants are using the academic accounts to obtain deeply discounted products and services such as Amazon Prime, unlimited cloud storage through Google Drive, and more, others are generating these accounts to sell on hacking forums for $8 to $20 per account. Efforts have been made to get these sales stopped but new sellers pop up faster than the old ones are blocked.

Combatting Email Fraud

To avoid becoming a conduit for online abuse, colleges are advised to adjust their email provisioning practices. There are multiple effective ways to accomplish this. One approach is to delay provisioning of student email accounts until a student has registered and paid for classes. The benefit of this is that it completely removes any incentive for fraudulent applicants. However, colleges may be resistant to this as it impacts automated business processes and impedes legitimate applicants from accessing onboarding resources essential to the enrollment process.

Rather than withhold a student email account, a recommended solution is to limit the use of these accounts to internal email communications until the student has registered and paid for classes. Colleges that have taken this step have seen an immediate, dramatic decrease in the number of fraudulent applications they receive. Evidence of this can be seen in hacking forums where criminals discuss which colleges still have working .edu email accounts.

A step-by-step tutorial describing three methods of restricting use of .edu accounts is available to California community colleges. To request a copy of the document, please contact Omer Usmani, ousmani@ccctechcenter.org, at the CCC Information Security Center.

###