**REPORT: Internship Scam Alert**

**Date**: June 18, 2023

**Subject**: Internship Scam Alert - Beware of Fraudulent Emails

**Introduction:**

On last Sunday dated June 11,2023 , an individual reported receiving an email regarding their selection for an internship they had previously applied for. This report aims to provide a detailed account of the incident and raise awareness about the ongoing scam that is affecting people worldwide.

**Description of the Incident:**

The individual received an email informing them that they had been selected for an internship. Without realizing it, they promptly sent their resume as requested. Subsequently, they received additional emails from different individuals, stating that they had been selected for various positions. Unfortunately, the individual did not notice these emails.

On June 13,2023, the individual received a call from a person claiming to be from Naukri, who raised concerns about their lack of response to companies and absence of a job ID. The caller alleged that legal action would be taken against the individual for not reading the terms and policies of Naukri.com. The caller further threatened to issue a challan of Rs. 48,000, potentially harming the individual's family reputation and imposing a seven-year ban on their documents.

**Resolution and Discovery of Fraud:**

Feeling alarmed by the caller's claims, the individual decided to investigate the matter further. Upon reviewing their emails, they noticed that all the selection emails came from an address named **sanjoli.raj@freshersindia.in.** Realizing the suspicious nature of the situation, the individual terminated the call and received a subsequent message discussing legal consequences.

In their quest for more information, the individual researched and discovered a website **(https://lnkd.in/gDSMDsWM)** confirming that they had indeed encountered a fraudulent scheme.

**Conclusion and Awareness:**

This incident serves as a warning to all individuals, especially students and job seekers, about the prevalence of scams targeting unsuspecting victims. The perpetrators of such scams often manipulate victims' desires for career opportunities and exploit their trust.

It is crucial to exercise caution and take proactive measures to verify the legitimacy of emails, websites, and job offers before sharing any personal information or documents. Here are some recommended steps to follow:

1. Be vigilant and skeptical: Scrutinize any emails, calls, or messages that demand immediate action or contain suspicious requests.

2. Verify the source: Confirm the legitimacy of the sender's email address, company name, and contact information. Cross-reference information with official websites or trusted sources.

3. Research the company or organization: Conduct a thorough investigation to ensure the existence and credibility of the company or organization offering the internship or job opportunity.

4. Check website security: Look for secure website connections (HTTPS) and authentic contact details. Be cautious of websites with irregular layouts or poorly written content.

5. Consult reliable sources: Seek advice from trusted mentors, career counselors, or professionals when in doubt about the authenticity of an opportunity.

By sharing this incident, the individual aims to raise awareness and prevent others from falling victim to similar scams. It is crucial to remain vigilant and adopt a proactive approach to protect personal information and financial security.

Please share this information with your peers, colleagues, and other individuals who may benefit from this warning.

Stay safe, informed, and secure.

**Aman Pandey(BCA)**

**Student of Trinity Institute of Professional studies, Dwarka**

**Executive head of Cyber Knight(Networking and Security club)**