Farah Alhamzawi

Mr. Green

Independent Study & Mentorship

10 November 2023

Analyzing Security Awareness of Students to Protect Their Data on Campus

Chinthada, Sarath. “Cybersecurity Awareness for Students: Protecting Personal Data on Campus.” Thetechhacker, 20 Nov. 2023, thetechhacker.com/2023/11/20/cybersecurity-awareness/. Accessed 28 Nov. 2023.

This article, “Cybersecurity Awareness for Students: Protecting Personal Data on Campus”, emphasizes the critical importance of cybersecurity awareness for students in the digital age, particularly when using online platforms for educational and personal purposes. It recognizes that students are constantly exposed to potential cyber threats, given the increasing prevalence of online resources and social interactions. The piece underscores the need for cybersecurity awareness to equip students with the knowledge and skills necessary to navigate the internet securely and protect their personal information from cybercriminals.

The article rightly points out that students often handle sensitive data, including personal identification details, educational records, and financial information, making them potential targets for hacking, phishing, and other cyberattacks. To mitigate these risks, the author suggests that students should understand basic cybersecurity principles such as secure password practices, recognizing phishing attempts, and adopting safe browsing habits.

Moreover, the article extends the significance of cybersecurity awareness beyond personal protection, highlighting its role in contributing to a safer digital environment for everyone. Educated students, it argues, can recognize and report potential threats, thereby preventing the spread of

malware or harmful content. The mention of early exposure to cybersecurity principles preparing students for responsible digital practices in their future careers adds a forward-looking perspective to the discussion.

The provided "10 Tips On Protecting Personal Data on Campus" further enrich the article by offering practical advice. These tips cover a range of cybersecurity measures, including the use of strong and unique passwords, caution regarding public Wi-Fi, regular device updates, awareness of phishing scams, installation of antivirus software, regular data backups, safe browsing practices, securing mobile devices, continuous education about cybersecurity, and prompt reporting of suspicious activities.

When it comes to cracking passwords, Malicious users can use many different types of brute force attacks, such as simple attacks, dictionary attacks, reverse attacks, and many more. A simple attack is when a malicious user attempts to guess a user's login by using any software. In these types of attacks, they would use information found on social media, such as Instagram, TikTok, and more, to figure out the combination. They would also be able to use common passwords such as password!, 123456, *name*1234, and more. When it comes to Dictionary attacks, malicious users use a combination of dictionary software and brute force attacks. The dictionary software can contain both lowercase and uppercase letters or one or the other. Lastly, Reverse attackers happen when malicious users have harsh passwords and try to guess the password based on the information found in the hash.

Moving on by updating your device regularly, making sure that the WIFI your going to connect to is always secure, brows safely, and by always being cautious, users will be able to protect themselves even more. With this information, I plan to create a section on my website that would summarize the information provided and give a more descriptive emphasis on each section.