Dear NOVA IT Department and Office of Student Affairs,

It has come to my attention for that I need to write an expression of concern that's been growing for a long time and affecting thousands of college students across NOVA & campus nationwide. Due to the currently increasing amount of risk amongst cybersecurity attacks, specifically targeting students who not only lack the proper knowledge but also the training and simple habits for protecting themselves online. As today's technology is advancing at a rapid pace, our academic, financial, and personal information continues to shift towards the digital world. Nowadays, students are more vulnerable than ever to phishing attempt attacks, identity theft, and even security data breaches. In order to reduce these vulnerabilities and risks and in order to create a safer campus environment digitally, NOVA should implement a requirement of cybersecurity awareness training, as well as implementing protective digital measures for all NOVA enrolled students. As each year progresses, cyber threats continue to escalate. I believe that this issue must meet the demanded attention immediately and that NOVA is in the perfect position to strengthen cybersecurity awareness in higher education.

Today, many students are really unaware of even the basic fundamentals of practicing cybersecurity; as a result of this, they’re constantly at risk and very vulnerable, whether or not they even realize it, and are self aware. Research highlights that a vast majority of college students typically use weak passwords, the same login credentials for every account, and even connecting to public Wi-Fi networks that are unsecured without understanding the dangerous risks involved in doing these routinely actions. Cybersecurity studies done by a numerous amount of universities have stated that a lot of students “believe” that they are very knowledgeable about technology; however, they still fail to recognize simple phishing emails, identifying fake and suspicious links, or even understanding the concept of how their sensitive personal information can easily be exposed (Hobbs 161). Due to this false confidence in being knowledgeable about technology, this results in students making marked as the prime victims for cybercriminals to target for identity theft, credential theft, and financial scams.

Due to these consequences still being vulnerable as they are today, the results of these consequences are extremely serious, especially for students. A single attack can affect a student's banking and credit information, academic accounts, personal identity, and even financial aid, such as FAFSA or IRS documents. If supposedly, any of that information manages to fall into the wrong hands of cybercriminals, it can lead to open fraudulent credit lines, they're able to take out loans and access accounts, and even damage a student's financial aid, financial information, and academic future for a numerous amount of years. The most concerning part is that most students aren't even aware and don't notice identity theft until it's too late, after the damage has already been done. The National Cybersecurity Alliance explains that college students are the most targeted group since they frequently create factors that are perfect opportunities for cybercriminals, such as handling sensitive information online, relying heavily on multiple amount of devices, and even always moving in between networks that are constantly unsecured (Cybersecurity Tips for College Students)

Although NOVA offers the basic IT guidelines as well as occasional security alerts through email and sms, the reality of the matter is that the current efforts aren't near enough of protecting students from the growth of cyberattacks. Having optional workshops, email and sms lerts, or even short warnings posted and sent on the website isn't nearly enough in creating a long term lasting awareness or teaches students the basic daily habits to follow, required to stay safe online. According to Armas et al., a lot of colleges that have been able to successfully reduce cyber incidents are the types of institutions that are working towards building a cybersecurity culture that focuses on early education, actual training thats contionius, and campus awareness instead of relying on the IT department (Armas et al). Colleges, including NOVA, continue to have the belief that anything cybersecurity related, mainly responsiblities, belongs to the IT department. This mindset ends up causing damage to students as they're left unprepared and unaware of the real dangers they face daily. The issue isn't that they lack the understanding of cybersecurity, but really how they haven't been provided the required resources or taught to make cybersecurity, no matter what field they're in.

In order to solve this ongoing problem today, NOVA should implement two solutions that are not only impactful but also immediately strengthen student online safety on campus. The first solution NOVA should implement is a required cybersecurity awareness course for all first year students within their first semester, much like SDV100. The required course should include on focusing on the essential cybersecurity skills, such as recognizng the patterns of phishing attempts, creating stronger and unique passwords for each account, understanding the uses of multi factor authentication, updating all devices to the latest security updates regularly, and knowing how to protect personal information whenever students connect to different networks, the majority being networks from public libraries and cafes. Research shows that the students who are able to gain early cybersecurity skills and training are able to learn better habits and encounter fewer cyber incidents throughout college (Armas et al). No matter the amount of required training a student gains, it can drastically reduce the number of vulnerabilities on campus.

The second solution includes having an enhanced outreach of ongoing cybersecurity awareness initiatives, such as monthly newsletters, immediate alerts of any trending scams, security update reminders, and hands-on interactive workshops throughout the semesters. These implementations not only keep the students alerted and informed about the evolving cybersecurity world, but also helps in giving simple reminders to students by advising them to avoid vulnerabilities such as suspicious links, not updating their passwords, and ignoring alerts of any phishing scams. These implementations are essential, as according to the National Cybersecurity Alliance, regular security updates are one of the strongest tools when it comes to preventing attacks before they even occur and develop (Cybersecurity Tips for College Students).

The two solutions listed are not only both realistic, but also really attainable with the current resources that NOVA currently holds. Since the IT Department of NOVA already has the responsibility of handiling a lot of the overall cybersecutiyt infrastructures, they also already have the knowledge as well as the experience that are necessary in order to help the students understanding on how to build safer habits online. Having the IT department expand their role of increasing cybersecurity in a student focused area would be very beneficial in landing higher roles in their IT and Cybersecurtity careers, especially

students who have volunteered in working with the IT department. Since the NOVA systems, such as Canvas, SMS alerts, and email, they can easily adapt to these new implementations with minimal structural changes.

NOVA would be taking a big leap forward towards creating a protective student environment, not only academically but also personally and financially. Regardless of every student's major and field, each of them relies on online platforms for important uses such as financial aid, assignments, and banking information. Learning cybersecurity isn't just an academic improvement but something that will benefit them as a long term investment. Students are able to form stronger habits from the implementations of training, support, and awareness that will have an impact in their academic and professional careers. Knowledge and cybersecurity education must evolve as technology continues to evolve as well, and having students start developing these foundational skills and knowledge is a key factor for their long term success.

As Cyber threats are increasing as the years go by, students remain the target audience that's the most vulnerable when it comes to cyber attacks due to the fact that their lack of knowledge as well as experience when it comes to identifying vulnerabilities and threats. For these reasons mentioned, I encourage NOVA to take a step forward towards immediate action as I strongly recommend implementing a required cybersecurity course for all first year students as well as continuous cybersecurity initiatives throughout the semesters. From taking these steps mentioned, NOVA can drastically strengthen not only the safety and awareness of every student on campus, but also their digital security and protection too. Thank you for time and consideration in this message, as a student myself, I truly hope you take action towards this concurrent problem in creating a safer and secure environment for all students of NOVA.

Respectfully,

Haytham Abouelfaid

Armas, R., et al. “Building a Cybersecurity Culture in Higher Education.” Information, vol. 16, no. 5, 2025, pp. 1–15. MDPI, https://www.mdpi.com/2078-2489/16/5/336

Hobbs, James. “Cybersecurity Awareness in Higher Education: Understanding Student Knowledge Gaps.” Issues in Information Systems, vol. 24, no. 1, 2023, pp. 159–169. IACIS, https://iacis.org/iis/2023/1_iis_2023_159-169.pdf

“Cybersecurity Tips for College Students.” National Cybersecurity Alliance, 18 Aug. 2025, https://staysafeonline.org/articles/cybersecurity-tips-for-college-students