Geeksquad Internship

Kayla Thompson

Supervisor Brandy Austin

Best Buy

Department of Cybersecurity

CYSE 368

Professor Duvall / TA Russell

April 19, 2026

Table of Contents:

Geeksquad Internship

Introduction

My internship with Geek Squad at Best Buy served as a bridge between my academic training in cybersecurity and network engineering and the real-world technical environments where these skills are applied. As a senior cybersecurity student preparing for both U.S. and international cyber roles, I entered this internship intending to strengthen my technical confidence, improve my customer-facing communication, and gain hands-on experience with device diagnostics, troubleshooting, and secure data handling. This internship provided a unique opportunity to work directly with customers, analyze a wide range of technical issues, and apply cybersecurity principles in a fast-paced, high-volume environment.

Throughout the internship, I was exposed to a variety of devices, operating systems, and user behaviors that broadened my understanding of both technical and human factors in cybersecurity. I learned how to diagnose hardware and software issues, perform system repairs, communicate technical information clearly, and maintain professionalism. This paper provides an overview of my experience, including the organization's structure, my responsibilities, the technical skills I developed, the challenges I encountered, and how this internship contributed to my academic and professional growth. I truly look forward to spending the rest of my summer working for them and building upon my skills. My co-workers and supervisors always encourage us to be better and have fun doing it, which has made the experience even more rewarding.

Organization Overview

Geek Squad is the technical support and repair department of Best Buy, one of the largest consumer electronics retailers in the United States. The organization provides a wide range of services, including device diagnostics, hardware repair, software troubleshooting, data recovery, network setup, and cybersecurity-related support. Geek Squad operates within a hybrid environment that combines customer service, technical expertise, and operational efficiency.

The culture at Geek Squad emphasizes teamwork, adaptability, and problem-solving. Agents must balance technical accuracy with customer communication, ensuring that customers who may have little technical knowledge understand the issues affecting their devices. This environment requires patience, clarity, and the ability to translate complex technical concepts into accessible explanations. We tend to have to reduce the complexity of concepts to better fit the understanding of our customers, like relating them to sports or soap operas. Being able to relate these issues to their interests creates a bond between agents and customers, increasing the likelihood of customers coming back for more services.

From a cybersecurity perspective, Geek Squad plays an important role in educating customers about safe digital practices. Many customers arrive with malware infections, compromised accounts, or unsafe device configurations. As a result, Geek Squad agents must be aware of privacy protocols, secure data procedures, and best practices for preventing unauthorized access. This aligns closely with the principles taught in cybersecurity coursework, making the internship a valuable extension of academic learning. Internet safety awareness is a key component in our role; customers may have little technical knowledge, and they become prime targets for phishing scams. My ability to convey these important messages to customers

has developed my speaking and technical skills tremendously, because I know that skill will be pivotal in future employment.

Roles and responsibilities

My role as a Geek Squad intern involved a combination of technical diagnostics, customer interaction, and operational support. Everyone depending on when you came in had different roles to do when they came in. Morning shifts would have to do appointment confirmations and call customers for further details regarding devices, check the queue of the devices being worked on, and fix any devices that are left to be worked on. Midshift would have to take walk-in clients and gather any supplies that the morning crew may have run out of. The closing team will clean all workstations and clear the queue of devices that need to be fixed. Depending on who the team is that day, tasks may be distributed differently. Usually, when I work, I am forward-facing, taking clients, while my other co-workers will be doing back-of-the-house tasks like opening mail and receiving products. Each day presents a new set of challenges, requiring me to apply both technical knowledge and interpersonal skills. My responsibilities included:

Device Intake

I evaluated incoming devices, documented customer concerns, and performed initial assessments to determine whether issues were hardware or software-related. This required attention to detail and the ability to ask clarifying questions to understand the customer's experience. Making sure to document specifications such as physical conditions at intake and asking questions to better understand the full situation and find the best solution.

Running Diagnostics

I used internal tools and Apple diagnostic systems to evaluate device health, battery performance, storage integrity, and potential malware infections. This process helped identify root causes and determine appropriate repair paths. This is our first step to any intake, to ensure the scope of work is what we can do, and we follow proper protocol to prevent further damage.

Explaining Technical Issues

One of the most important aspects of my role was communicating findings to customers in a clear and understandable way. Many customers were anxious or frustrated, and it was my responsibility to explain issues without overwhelming them with jargon they don't understand. I have gotten very good at this aspect by relating complex problems to personal interests; it is easier to digest in that manner.

Performing Repairs and System Restorations

I assisted with OS reinstallations, data backups, device resets, and hardware troubleshooting. These tasks required precision and adherence to secure data protocols. We had USB sticks that had the Windows operating system installed, which we used to repair corrupted systems.

Documentation and Workflow Management

I created and updated service tickets, tracked repair progress, and ensured accurate documentation for each case. This helped maintain transparency and consistency across the team.

Collaboration with Senior Agents

I frequently worked alongside experienced agents, learning advanced troubleshooting techniques and observing how they handled complex customer interactions. Shadowing was insanely crucial in the beginning; it helped me see how to apply Cybersecurity troubleshooting techniques that I had used in class to diagnose devices.

This role required adaptability, patience, and a willingness to learn quickly. Over time, I became more confident in my ability to diagnose issues, communicate effectively, and contribute to the team's daily goals.

Technical Skills Applied

My internship allowed me to apply and expand a wide range of technical skills, many of which were directly connected to my academic background in cybersecurity and network engineering experience. It was the first time I could see how the theories, protocols, and frameworks I had studied came alive through hands-on troubleshooting and customer interaction. Every task, from diagnosing hardware failures to performing secure data wipes, required a balance of technical precision, ethical responsibility, and clear communication. This environment pushed me to think critically, act decisively, and refine my technical instincts.

Apple Device Diagnostics

I performed battery health checks, storage evaluations, and system diagnostics using Apple's internal tools. This helped me understand common failure points and how to interpret diagnostic results. These assessments required precision and patience, as even minor inconsistencies could indicate deeper issues. I became proficient in evaluating system

performance metrics, understanding how firmware interacts with hardware, and recognizing patterns that signal potential component degradation.

Operating System Reinstallations

I assisted with macOS and Windows reinstallations, ensuring that customer data was backed up securely if possible. This required knowledge of file systems, boot processes, and partition management. I had prior knowledge from my Windows Management class that I had to remotely install Windows on different virtual machines, which made it so easy to implement.

Data Backup and Recovery

I helped customers recover lost files, transfer data between devices, and set up cloud storage solutions, like OneDrive. This reinforced my understanding of data integrity and redundancy.

Malware Detection and Removal

I encountered several devices with malware infections, unsafe browser extensions, or compromised accounts. I applied cybersecurity principles to identify threats, remove malicious software, and educate customers on prevention. This is a daily occurrence, which worries me about public internet safety. This hands-on experience complemented my academic understanding of intrusion detection and reinforced the importance of proactive defense measures. I also learned how to communicate cybersecurity risks to customers in an accessible language, bridging the gap between technical detail and user awareness.

Network Troubleshooting

I assisted customers with connectivity issues, router configurations, and device pairing problems. My academic training in DHCP, DNS, and network protocols helped me diagnose these issues efficiently. I applied these principles to real-world problems, such as diagnosing slow connections or resolving device pairing failures. This practical application of networking theory improved my ability to think critically and deliver efficient solutions.

Secure Data Handling

Geek Squad maintains strict privacy protocols. I learned how to handle customer data responsibly, prevent unauthorized access, and follow secure wipe procedures when devices were reset or recycled. We usually destroy hard drives, because that is the only way to get rid of data.

These technical experiences strengthened my confidence and prepared me for more advanced cybersecurity roles in my future career. I evolved from a student applying classroom concepts to a professional capable of diagnosing complex issues, safeguarding data, and communicating solutions effectively. The internship transformed my technical proficiency into professional readiness, preparing me to contribute meaningfully to the cybersecurity field.

Work Orders

During my internship, I worked on numerous devices throughout my day that challenged my technical and communication skills. Every device we would work on would have a work order attached to keep track of what is coming in and out. We use this work order to take detailed notes of customer concerns, device condition, procedures that need to be completed, and details

of what the technician did to the computer. I've worked on laptops, custom builds, PS5s, Meta Glasses, Smart appliances, and so much. Each case provided valuable insight into real-world troubleshooting and customer service within a cybersecurity environment. Below are examples that highlight the range of issues I encountered and the lessons learned from each of them.

Device 1: Apple Device Diagnostic and Battery Replacement

One of my earliest projects involved diagnosing a MacBook Air that was shutting down unexpectedly. Using Apple's diagnostic suite GSX, I discovered that the battery's cycle count exceeded Apple's recommended limit, and the voltage readings were unstable. I explained the issue to the customer, emphasizing how battery degradation affects system performance and power management. After having the customer sign the approval, I assisted the tech in replacing the battery and recalibrating the system. This case reinforced the importance of precise diagnostic interpretation and clear communication, especially when customers are unfamiliar with technical terminology.

Device 2: Malware Infection and Data Recovery

A customer brought in a Windows laptop that was running slowly and displaying pop-up ads. Upon inspection, I found multiple malicious browser extensions and a Trojan embedded in the startup registry. I used our antivirus and malware removal tool WSHTF, "When Shit Hit the Fan," to clean the system, then performed a full scan to ensure no residual threats remained. The customer had lost access to several files, so I guided them through data recovery using external storage and cloud backup. This experience deepened my understanding of malware behavior and the importance of user education in preventing more attacks.

Device 3: Network Connectivity Troubleshooting

Another project involved a customer who could not connect their smart devices to a home network. I analyzed the router configuration and discovered conflicting DHCP settings and outdated firmware that the customer was not aware of. After updating the router and reconfiguring IP assignments, I successfully restored connectivity. I explained how network protocols like DHCP and DNS interact, connecting this real-world scenario to my coursework in network engineering. This demonstrated how theoretical knowledge directly translates into practical solutions, it was a very textbook problem to me.

Device 4: Secure Data Wipe and Device Recycling

Geek Squad follows strict data destruction protocols when recycling devices. I assisted in securely wiping several hard drives using a hammer to ensure no recoverable data remained. This process involved verifying wipe completion logs and physically destroying drives when necessary. It was a hands-on application of cybersecurity principles, specifically confidentiality and data lifecycle management.

Device 5: Customer Education on Cyber Hygiene

One of the most rewarding experiences was helping a customer who had fallen victim to a phishing scam. I explained how to identify suspicious emails, verify sender authenticity, and use multi-factor authentication. I also helped them update their passwords and enable account recovery options. This case highlighted the human side of cybersecurity, how empathy and education can prevent future incidents. It reminded me that cybersecurity is not only about

technology but also about empowering and teaching users to protect themselves online. It is a scary world we live in, but knowing technical literacy can make a difference in sensitive information being stolen.

Cybersecurity Exposure & Lessons

Throughout my internship, I observed how cybersecurity principles apply even in everyday consumer interactions. Many customers unknowingly expose themselves to risks through weak passwords, outdated software, or unsafe browsing habits. I learned to identify these vulnerabilities and provide practical advice without overwhelming or confusing them.

I also gained insight into how data privacy regulations influence service operations. Geek Squad's procedures for handling customer data, such as secure storage, limited access, and verified destruction, reflect compliance with privacy standards. This exposure helped me understand how cybersecurity policies are implemented at the organizational level, reflecting my Information Assurance class, which directly talks about safeguarding consumer data. I learned to perform secure data wipes using industry-standard tools, verify deletion logs, and maintain chain-of-custody documentation for recycled hardware. These practices mirrored the compliance standards discussed in my coursework, such as those related to the NIST Cybersecurity Framework and GDPR principles. Seeing these standards applied operationally helped me appreciate the intersection between policy and practice.

Additionally, I saw how social engineering remains one of the most common threats. Customers often shared sensitive information too freely, showing the need for continuous internet awareness training. These experiences reinforced my belief that cybersecurity education

must be accessible and ongoing. I sympathize with older customers because they lived in a world where this was not a thing, and I know adjusting can be hard for them.

Customer Service & Professional Development

Working in a customer-facing role taught me the importance of communication, patience, and professionalism. Technical expertise alone is not enough; the ability to explain complex issues clearly and calmly is essential. I learned to adapt my language based on the customer's level of understanding, using analogies and visual examples when necessary. Using analogies is the best way to explain complex concepts and helps the customer understand and improve their internet literacy skills. I use this technique with myself when learning new concepts in class and not fully grasping what I'm being taught.

I also developed more emotional intelligence, recognizing when a customer was anxious, frustrated, or confused, and responding with empathy. This skill improved my interactions and helped build trust. Collaborating with my supervisor, Henry, and other team members taught me how to balance independence with teamwork. I observed how experienced agents managed time, prioritized tasks, and maintained composure under pressure. It has taught me what tasks need to be completed for the business operation to be successful daily.

The internship also exposed me to incident response principles on a much smaller scale. When devices showed signs of potential compromise, I followed structured steps: isolate the system (putting the device in airplane mode), identify the threat, remove malicious components, and verify recovery. This mirrored the containment and eradication phases of professional incident response frameworks. Although the scale was smaller than enterprise-level operations,

the logic and discipline were identical. It taught me that cybersecurity methodology is scalable from personal devices to corporate networks.

These interpersonal lessons are just as valuable as technical ones. They prepared me to communicate effectively in professional cybersecurity environments, where collaboration and clarity are critical. Miscommunications have to be resolved quickly because if we report the wrong information, we have to create escalation tickets that take weeks to resolve at times. It also helps us make sure we are giving customers their devices and the notes for said device correspond.

In summary, my exposure to cybersecurity during the internship transformed abstract concepts into experiences. I witnessed how vulnerabilities arise, how protective measures are enforced, and how education empowers users to safeguard themselves. These lessons strengthened my commitment to pursuing cybersecurity as a career focused on both technology and people. This closes the gap between digital defense and human understanding.

Academic Connections to Coursework

My coursework at Old Dominion University provided a strong foundation for this internship. Concepts from CS 462 (Cybersecurity Fundamentals) and CS 464 (Networking Systems) were directly applicable. For example, understanding network protocols helped me troubleshoot connectivity issues, while knowledge of encryption and authentication informed my approach to secure data handling.

Lessons from CS 420 (Machine Learning Applied in Cybersecurity) also influenced my thinking. Although I did not implement machine learning models during the internship, the analytical mindset, identifying patterns, and anomalies proved useful in diagnosing system behavior. Similarly, my experience with Windows administration and file system management supported tasks involving OS reinstalls and data recovery. It helped me understand Windows systems thoroughly and in greater detail. I was able to gain hands on experience from work and school, and I am basically a professional when it comes to Windows operating systems. This integration of theory and practice strengthened my confidence and demonstrated the relevance of academic learning in professional contexts.

Additionally, my coursework in Interdisciplinary Studies (IDS 300W) taught me to connect technical solutions to ethical and social contexts. This perspective helped me appreciate the human side of technology, how digital security affects everyday lives, and why clear communication matters. It reminded me that cybersecurity professionals must balance technical expertise with empathy and social awareness.

Through these academic connections, I realized that my education is a makeup bag for problem-solving. Each course contributed to my ability to think critically, act responsibly, and communicate effectively in a professional setting. The internship validated that academic learning, when applied thoughtfully, becomes the foundation for growth and career success.

Growth, Reflection, and Career Impact

By the end of the internship, I had grown both technically and personally. I became more confident in my ability to diagnose issues, communicate effectively, and manage customer

interactions. I also gained a deeper appreciation for cybersecurity's role in everyday technology use.

The experience clarified my career goals. I realized that I enjoy roles that combine technical analysis with human interaction, positions such as cybersecurity analyst, network engineer, or incident responder. The internship also motivated me to pursue additional certifications, such as CompTIA Security+ and Cisco CCNA, to strengthen my professional profile. I hope to get my CompTIA Security+ certification by the end of this summer to advance my career. I realized which aspects of cybersecurity I do and do NOT enjoy. Personally, I like the ethics aspect of cybersecurity and making sure that individuals are aware of the threats that could be on the Internet. I would love a job in cybersecurity that involves governance and implementing regulations for an organization. I am doing very well with technical writing and think I would flourish in the sector of cybersecurity. I do not enjoy Linux creation or Python coding whatsoever and hope to stay far from it; it is very boring to me and I have no interest in creating programs. I think this frustration appears because my CYSE250 class was Introduction to Basic Networking and Python programming; it was very hard for me to apply the concepts we were learning, and I would rather do something I enjoy. I hope that one day I can be a Chief Information Officer for a technology company. I've noticed I'm good at directing and leading compared to just innovating, and would love a leadership role in the near future.

Beyond technical growth, I developed patience, empathy, and professionalism, which are qualities that will serve me well in any career path I decide to pursue.

Future Goals

Looking ahead, I plan to graduate in December 2026 and pursue cybersecurity roles that allow me to apply both technical and communication skills. I aim to work in environments that emphasize proactive defense, secure network architecture, and user education. My long-term goals include earning advanced certifications, building an ePortfolio that showcases my projects, and eventually working internationally in cyber defense or network engineering. I would love to be able to travel and incorporate technology as well. I'm not sure exactly what, but I have so much time to decide. I am going to keep exploring everything in cybersecurity to find the exact occupation that sparks my interests.

Next, I plan on going to Costa Rica and doing an environmental project that works with finding sustainable resources for AI for my last semester of my bachelor's. That experience will be everything and more, and I cannot imagine what it will be like. I want to merge my two favorite interests, technology and environmental science. They coincide with each other now with AI, a rapid explosion in the industry, which is destroying our ecosystems. I would love to be a part of a project that finds sustainable ways to make AI efficient and doesn't kill our planet.

Outside of career ambitions, I also plan to continue developing personal goals supporting my disabled younger brother's transition to independence, maintaining financial stability, and investing in real estate for passive income. The discipline and focus I developed during this internship will help me achieve these milestones!

Conclusion

My internship at Geek Squad under the supervision of Brandy was a transformative experience. It allowed me to apply classroom knowledge in real-world scenarios, strengthen my technical and interpersonal skills, and gain a clearer vision of my future in cybersecurity. I learned that effective technical support requires not only expertise but also empathy, communication, and ethical responsibility.

This internship reaffirmed my commitment to cybersecurity as a career path. It taught me that every interaction, whether diagnosing a device or educating a customer, contributes to a safer digital environment. The lessons I learned will continue to guide me as I advance toward professional roles that protect systems, data, and people.

This experience taught me that effective technical support is not just about solving problems, it's about protecting people. Every diagnostic test, data recovery, or malware removal was an opportunity to safeguard someone's digital life. I learned that empathy and communication are as essential as technical skills. Customers often arrived frustrated or anxious, and my ability to explain issues clearly and calmly transformed those interactions into moments of reassurance and education. That balance between technical precision and human connection is what defines excellence in cybersecurity practice.

On a personal level, this internship strengthened my confidence and clarified my career direction. I discovered that I thrive in environments that combine technical analysis with interpersonal engagement. Whether diagnosing a network issue or explaining safe digital practices, I found fulfillment in helping others understand technology more deeply. This

realization has shaped my professional goals: to pursue cybersecurity positions that emphasize both technical defense and user education, bridging the gap between complex systems and everyday users.

Looking forward, I see this internship as the foundation for my next chapter. It prepared me for advanced certifications, graduate-level work, and potential international opportunities in cyber defense. More importantly, it drilled a mindset of continuous learning, a recognition that technology evolves rapidly, and staying effective means staying curious. The lessons I learned at Geek Squad will continue to influence how I approach challenges, communicate solutions, and uphold ethical standards in every professional setting.