Justin R. Lew

(718) 506-6340

justinlew1000@gmail.com

LinkedIn Profile - https://www.linkedin.com/in/justinrlew/

Personal Website - https://justinrlew.github.io/index/

I'm a highly motivated graduate who holds a Bachelor of Science degree in Cybersecurity and Information Assurance, and have earned certifications in CompTIA tracks such as PenTest+, CySA+, and Security+!

With experience in IT support, help desk troubleshooting, and web development, I am passionate about delivering effective solutions and providing excellent service. I pride myself on being highly disciplined, hard-working, and committed to being the best at what I do, always going the extra mile to make sure problems are resolved.

I’m adaptable, customer-focused, and dedicated to making sure that users have a smooth experience. With a commitment to continuous learning, I’m eager to contribute my skills to a dynamic team. If you're seeking someone who is dedicated, results-driven, and always focused on customer satisfaction, I’d love to connect and explore how I can support your organization’s success.

Bachelor of Science, Cybersecurity and Information Assurance
Western Governors University, Graduate

Experience

IT Support Specialist **Webster Bank** *(May 2024 – Nov 2024)*

- Provided courteous customer service by actively listening to user concerns.
- Offered reassurance through technical resolutions while maintaining a positive rapport.
- Responded to user inquiries via phone, email and ticketing system, diagnosing problems and offering solutions.
- Provided live chat, email, and phone support, ensuring fast and effective resolutions to user issues.
- Managed and prioritized helpdesk tickets to meet critical deadlines, reducing response times by 25%.
- Maintained a 95% user satisfaction score by proactively addressing customer pain points.

- Trained team members on best practices for **cybersecurity awareness** and system optimization.

Service Desk Analyst **Queens College, City University of New York** *(Jan 2024 – Apr 2024)*

- Provided attentive customer service by responding to technical issues with a friendly, patient attitude.
- Delivered technical solutions via live chat, achieving an average resolution time of 10 minutes per inquiry.
- Documented recurring technical issues and solutions to enhance team efficiency and knowledge sharing.
- Collaborated with Tier 2 support to escalate and resolve complex technical challenges.
- Answered user calls and emails, logging all issues into the ticketing system for tracking and resolution.
- Assisted with basic troubleshooting tasks, such as resetting passwords and helping users navigate software applications.

Technical Support Specialist ***Queens Library*** *(Sep 2023 – Dec 2023)*

- Delivered personalized customer service by explaining technical solutions in a straightforward and empathetic way.
- Provided real-time live chat support for over 30 user inquiries daily, earning a 95% CSAT rating.
- Diagnosed and resolved network, software, and hardware issues, ensuring optimal system performance.
- Improved customer confidence by simplifying technical concepts into clear, user-friendly explanations.
- Provided excellent customer service by explaining technical solutions in simple, user-friendly terms, achieving a 95% customer satisfaction rating.
- Responded to over 30 daily user inquiries via phone, email, and ticketing systems, delivering fast and efficient resolutions to technical issues.

Help Desk Technician Tier 1 **Queensborough Community College** *(May 2023 – Aug 2023)*

- Provided compassionate and patient customer service by delivering technical assistance to employees in an approachable manner.
- Offered compassionate and professional technical support across live chat, email, and phone channels.

- Assisted users in navigating software applications and resolving password-related issues.
- Supported onboarding processes, ensuring seamless access to company systems
- Answered user calls and emails, logging all issues into the ticketing system for tracking and resolution.
- Assisted with basic troubleshooting tasks, such as resetting passwords and helping users navigate software applications.
- Escalated more complex technical problems to senior team members or Tier 2 support.

Certifications

Certification	Date
CompTIA PenTest+	August 2024
ISC2 CCSP: Certified Cloud Security Professional	August 2024
CompTIA CySA+	June 2024
CompTIA Security+	October 2023
CompTIA Project+	April 2024
CompTIA Network+	September 2023
CompTIA A+	July 2023
ITIL 4 Foundation - IT Service Management (GR671577319JL)	October 2023
ISC2 SSCP: Systems Security Certified Practitioner	February 2024
LPI Linux Essentials	December 2023

Extracurricular Activities	Cyber Club Member: Actively participated in discussions and practiced hands-on cybersecurity concepts

Awards & Achievements	Excellence Award: Awarded for exemplary work in Managing Information Security coursework

Technical/Soft Skills

Programming Languages	Python, SQL, Bash, PowerShell, HTML, CSS, JavaScript
Customer Support & Ticketing Tools	Zendesk, ServiceNow, Jira Service Management
Productivity Tools	Microsoft Office
Customer Support Metrics	**Customer Satisfaction Score (CSAT):** ● Consistently maintained a CSAT rating of 90% through attentive and solution-oriented support. **First Response Time (FRT):** ● Achieved an average first response time of 3 minutes for live chat inquiries. **Resolution Time:** ● Resolved 80% of tickets within the same business day, improving overall user experience. **Ticket Volume Handled:** ● Managed 25+ live chat and email inquiries daily while maintaining service quality.

	Escalation Rate: ● Minimized ticket escalations to senior support to under 10% by providing accurate first-contact solutions. **Knowledge Base Contributions:** ● Created 5 knowledge base articles to address recurring issues, reducing related inquiries by 10%. **Accuracy in Resolutions:** ● Delivered correct solutions 95% of the time on the first response. **Feedback Implementation:** ● Collaborated with the team to incorporate user feedback, reducing recurring issues by 15%.

Tools/Technologies

User and Identity Management	Active Directory (AD), Okta, LDAP (Lightweight Directory Access Protocol), Duo Security
Ticketing and Helpdesk Systems	ServiceNow, Jira Service Management, Zendesk, Freshdesk, Spiceworks
Remote Access and Troubleshooting	TeamViewer, Microsoft Remote Desktop, Chrome Remote Desktop, LogMeIn, AnyDesk
Virtualization and Cloud Management	VMware vSphere, Hyper-V, AWS Management Console, Microsoft Azure Portal, Spiceworks

Endpoint and Device Management	Microsoft Intune, Jamf, PDQ Deploy

Network Monitoring & Analysis	Wireshark, Nmap
Firewall & Intrusion Detection	pfSense, Cowrie
Vulnerability Scanning & Exploitation	Metasploit, Nessus, OpenVAS
SIEM	Splunk
Password Cracking & Authentication	Hydra, John the Ripper, Hashcat
Phishing & Security Awareness	GoPhish, Have I Been Pwned

Projects

1. **ServiceNow Workflow Project**

This project uses ServiceNow to create workflows for an IT Help Desk environment. It showcases automated incident workflows, a self-service portal, email notifications, reporting dashboards, and incident assignment rules.

GitHub Repository - https://github.com/JustinRLew/ServiceNow-project

---

2. **Windows Active Directory Virtual Lab**

This project demonstrates the deployment and management of an Active Directory environment in a virtual lab. It includes setting up a domain controller, configuring DNS, managing users and groups, implementing Group Policy Objects, and integrating a client machine.

GitHub Repository - https://github.com/JustinRLew/Active-Directory-Virtual-Lab

---

3. **Remote Desktop Protocol (RDP) – Real-Time Walkthrough**

This project shows my ability to assist users in setting up and troubleshooting three popular remote desktop tools:

- Microsoft Remote Desktop Protocol

- Chrome Remote Desktop
- TeamViewer

GitHub Repository - https://github.com/JustinRLew/Remote-Desktop-Protocol-Project

---

4. **SIEM Monitoring with Splunk**

This project demonstrates the implementation of a Security Information and Event Management (SIEM) system using Splunk. The purpose of the project is to monitor a simulated network, detect security threats, and respond to incidents in real-time.

GitHub Repository - https://github.com/JustinRLew/SIEM-Monitoring-Splunk

---

5. **Phishing Simulation Tool**

This project involves building a phishing simulation tool using a custom HTML front-end interface, SendGrid, a Python Flask backend API, and Postman for testing API requests to demonstrate phishing attack methodologies.

GitHub Repository - https://github.com/JustinRLew/Phishing-Simulation-Tool

---

6. **Brute-Force Attack Simulation**

This project is a Python-based brute force attack simulation that demonstrates how brute force attacks work. The script attempts to guess passwords by hashing and comparing them to a stored hash.

GitHub Repository - https://github.com/JustinRLew/Brute-Force-Attack-Simulation

---

7. **Honey Pot – Creation & Deployment**

This project involves setting up a medium-interaction SSH honeypot using Cowrie to detect and analyze unauthorized login attempts (particularly brute-force attacks). The honeypot logs attacker behavior and provides insights into the threat landscape.

GitHub Repository - https://github.com/JustinRLew/Honey-Pot-Creation-and-Deployment

---

8. **Personal Firewall & Network Monitoring**

This project demonstrates how to configure a personal firewall and monitor network traffic on a Windows system. Windows Defender Firewall, PowerShell, Wireshark, and Nmap were used.

GitHub Repository - https://github.com/JustinRLew/Personal-Firewall-and-Network-Traffic-Monitoring

---

9. **Password Strength Checker**

Created a web-based password strength checker that evaluates passwords in real-time based on NIST guidelines. It provides visual feedback, displays password strength, and offers recommendations for improving password security.

GitHub Repository - https://github.com/JustinRLew/Password-Strength-CheckerPassword Strength Checker

Password Strength Checker App - https://justinrlew.github.io/Password-Strength-Checker/

---

10. **Founder and Blockchain Developer - CrustCoin (CRST)**

Founder and Creator of CrustCoin (CRST):

CrustCoin is an ERC-20 utility token developed as a blockchain-based solution for decentralized financial services. Designed to power Bank-as-a-Service (BaaS) platforms, CrustCoin integrates features like savings accounts, staking rewards, and community-driven governance. Its deflationary tokenomics and focus on scalability, security, and accessibility position it as a foundational layer for fintech innovation.

- **Key Features:** Blockchain-based savings, staking rewards, and governance mechanisms.
- **Tokenomics:** Deflationary model with a fixed supply of 1 billion tokens.

- **Built On:** Ethereum using OpenZeppelin libraries, with a React.js-based wallet interface.

Private GitHub Repository:

(Demonstration Video Available Upon Request)
This project demonstrates ability in Solidity, smart contract development, decentralized finance (DeFi), and blockchain integrations for fintech applications.

---

11. **Crypto Exchange Penetration Testing Toolkit**

The Crypto Exchange Penetration Testing Toolkit is designed to test and identify security vulnerabilities in cryptocurrency exchanges.

Targets common exploits:

1) API vulnerabilities (e.g., weak token validation, unauthorized access)
2) Improper input validation (e.g., SQL injection, XSS attacks)
3) Weakness reporting with severity rankings and recommendations.

Private GitHub Repository:

(Demonstration Video Available Upon Request)

Languages
English • Spanish • Chinese