**Malware Attack User Manual**

**Table of Contents**

1. Introduction
2. Game Overview
3. System Requirements
4. Game Structure
5. Game Mechanics
6. Level Guide
7. Educational Content
8. Troubleshooting
9. FAQ

**Introduction**

This Malware Attack game are separately from the Cyber Security previous stage which is in Stage 4 and focused to entertain and educated user about how to defending and protecting server system to get infected with many kind virus and learn about antivirus too.

**Purpose of the Game**

Malware Attack is an educational game designed to teach players how to identify, prevent, and respond to malware attacks. Through engaging space shooter gameplay and interactive drag-and-drop antivirus tools, users will learn how different types of malware operate and how cybersecurity tools can neutralize them effectively.

**Target Audience**

This game is designed for a **general audience**, including students, adults, and especially **parents** who want to understand digital threats and protect their home networks. No prior technical knowledge is required.

**How to Use This Manual**

This manual guides you through understanding the game structure, controls, educational value, and troubleshooting steps. Navigate through each section using the table of contents to find relevant information quickly.

**Game Overview**

**Game Description**

Malware Attack puts the player in charge of defending a virtual computer server from waves of malware including viruses, worms, trojans, and ransomware. Players use a mix of space shooter mechanics to eliminate threats and drag-and-drop antivirus tools to analyze and clean infected files.

**Key Features**

• Interactive malware identification system  
• Drag-and-drop antivirus lab simulation  
• Fast-paced space shooter gameplay mechanics  
• Real-time feedback and learning tips  
• Multiple levels with increasing difficulty

**Educational Benefits**

* Teaches users to recognize different types of malware
* Demonstrates how antivirus software identifies and removes threats
* Reinforces the importance of real-time protection and data hygiene
* Provides real-world strategies for safe computing

**System Requirements**

**Minimum Requirements**

• Operating System: Windows 10 / macOS Catalina or higher  
• Browser: Chrome, Firefox, Edge (latest versions)  
• Memory: 4 GB RAM  
• Internet Connection: Required for updates and leaderboard access  
• Screen Resolution: 1920x1080

**Recommended Requirements**

• Operating System: Windows 11 / macOS Ventura or higher  
• Browser: Chrome or Edge (latest versions)  
• Memory: 8 GB RAM  
• Graphics: Integrated GPU (Intel HD 620 or above)  
• Screen Resolution: 1920x1080

**Game Structure**

**Main Components**

* **Main Menu**: Access levels, settings, and tutorial
* **Antivirus Lab**: Drag-and-drop interface to scan and clean files
* **Simulation Arena**: Real-time virus elimination gameplay
* **Learning Hub**: Recap of lessons and malware facts after each level

**Navigation**

Players can navigate using mouse clicks. Use the top menu to switch between modes and progress through the levels.

**User Interface**

* **Server**: Shows the computer server to protect
* **Toolbox**: Contains antivirus tools (scanner, quarantine, firewall)

**Game Mechanics**

**How to Play**

* Use your antivirus tools by dragging them onto computer servers.
* Switch between modes as needed to protect your server.
* Learn about each malware after defeating it.

**Controls**

Use mouse to drag the antivirus to protect the server from virus appeared randomly

**Scoring System**

* +5 points: Successfully cleaning tutorial
* +10 points: Successfully level 1
* +15 points: Successfully level 2
* +20 points: Successfully level 3
* +25 points: Successfully level 4

**Level Guide**

**Level 1: Virus vs Antivirus**

* **Objective: Protect the server from basic viruses using antivirus software through drag-and-drop.**
* **Skills Taught: Virus identification, basic signature-based antivirus use.**
* **Malware Type: Virus**
* **Protection Tool: Antivirus**
* **Spawn Rate: 10 viruses**
* **Completion Criteria: Prevent the server from being compromised by all virus attacks.**
* **Tips: Viruses often target document files. Drag the antivirus tool onto the server to activate a shield. Each shield can block up to 5 virus hits.**

**Level 2: Trojan vs Firewall**

* **Objective: Defend the server from trojans pretending to be legitimate files by applying firewall protection.**
* **Skills Taught: Firewall basics, monitoring suspicious application behavior.**
* **Malware Type: Trojan**
* **Protection Tool: Firewall**
* **Spawn Rate: 15 trojans**
* **Completion Criteria: Successfully block all trojan threats before they breach the server.**
* **Tips: Trojans often mimic trusted applications. Drop the firewall onto the server to grant it a temporary shield capable of blocking up to 5 threats.**

**Level 3: DDoS vs Anti DDoS**

* **Objective: Stop waves of Distributed Denial-of-Service (DDoS) attacks using anti-DDoS protection.**
* **Skills Taught: Network defense, traffic filtering.**
* **Malware Type: DDoS Attack**
* **Protection Tool: Anti-DDoS**
* **Spawn Rate: 20 DDoS bots**
* **Completion Criteria: Ensure the server remains stable and does not crash under attack.**
* **Tips: DDoS attacks come rapidly and in large numbers. Apply the anti-DDoS shield early to maximize protection each shield absorbs 5 attacks.**

**Level 4: Ransomware vs Data Recovery**

* **Objective: Protect the server from ransomware attacks by deploying data recovery systems.**
* **Skills Taught: Backup strategies, ransomware awareness.**
* **Malware Type: Ransomware**
* **Protection Tool: Data Recovery System**
* **Spawn Rate: 25 ransomware files**
* **Completion Criteria: Prevent data encryption and restore compromised files before permanent damage occurs.**
* **Tips: Ransomware targets critical data. Quickly drag and drop the data recovery tool to restore lost files — each shield can handle 5 encryption attempts.**

**Educational Content**

**Real-World Applications**

The game simulates real cybersecurity scenarios that users may encounter, such as phishing emails, disguised trojans, or ransomware attacks. The learned strategies help users:

* Protect personal computers
* Recognize suspicious behavior
* Choose effective antivirus software
* Back up important files

**Learning Assessments**

Each level ends with a short quiz and a malware identification challenge to assess understanding and reinforce learning.

**Troubleshooting**

**Common Issues**

* **Game not loading**: Ensure browser is updated; clear cache
* **Lag or delay**: Lower graphics settings or close background apps
* **Drag-and-drop not working**: Try a different browser or device

**Technical Support**

Visit our support site at (website icon+) or email us at (email icon+)

**FAQ**

**Q: Do I need technical knowledge to play this game?**  
A: No, the game is designed for all users, including parents and beginners.

**Q: Is the game safe for children?**  
A: Yes, it is educational and family-friendly.

**Q: Does it require an internet connection?**  
A: Only for leaderboard access and updates; offline play is available.

**Q: Can I replay previous levels?**  
A: Yes, all completed levels can be replayed for practice.

**Supported by Icon+ and President University**

**Troubleshooting**

* Restart your browser or device
* Ensure JavaScript is enabled
* Make sure you meet the minimum system requirements

© 2025 Icon+. All Rights Reserved.