**Cyber Security Audit Report**

**Prepared by: Muhammad Talah Khan**

**Date: [04/03/2025]**

**System Audited:** [Acer Predator]

# 1. System Security Settings Review

* Windows Security Status: Enabled
* Firewall Status: Enabled
* Automatic Updates: Enabled
* User Account Control (UAC): Enabled

**Analysis:** All core security settings are enabled, which provides a strong defense against malware and unauthorized access. However, further verification of security patches and updates is recommended.

# 2. Antivirus and Malware Scan

* Antivirus Software: Windows Defender/Avast
* Last Scan Date: Yesterday
* Scan Type: Quick & Full Scan
* Detected Threats: Yes
* Action Taken: Deleted recommended files

**Analysis:** Regular malware scans are performed, and threats are being removed. However, enabling real-time protection and periodic full scans would further enhance security.

# 3. Browser Security Settings

* Browser Used: Chrome
* Security Protection Level: Not Enhanced
* Block Third-party Cookies: Maybe
* HTTPS-Only Mode: Disabled
* Extensions Installed: Avast Security

**Analysis:** The browser lacks enhanced security settings, which increases exposure to phishing and malicious websites. Enabling **Enhanced Protection**, blocking third-party cookies, and enabling HTTPS-Only mode are strongly recommended.

# 4. Password Management

* Password Manager Used: No
* Multi-Factor Authentication (MFA) Enabled: Yes
* Strong Password Usage: Yes
* Weak Passwords Identified: Maybe

**Analysis:** Although MFA is enabled and passwords are generally strong, the absence of a password manager poses a risk. Users may struggle to remember unique passwords, leading to potential reuse and weaker security.

# 5. Network Security

* Wi-Fi Encryption Type: WPA2
* Router Default Credentials Changed: No
* Devices Connected: PC, Phone, IoT Devices
* Unauthorized Devices Detected: No

**Analysis:** WPA2 encryption is enabled, which is good, but the **router’s default credentials are still unchanged**, making it vulnerable to attacks. It is highly recommended to change the default username and password.

# 6. Identified Vulnerabilities and Risks

1. **Browser Security Risks:** Lack of HTTPS-Only mode and enhanced protection increases the risk of phishing attacks.
2. **Weak Network Security:** The router still uses default credentials, making it vulnerable to unauthorized access.
3. **Potential Weak Passwords:** Without a password manager, weak or reused passwords may exist.
4. **Antivirus Limitations:** While threats are deleted, real-time protection should be enabled for continuous monitoring.

# 7. Recommendations for Improvement

* **Enhance Browser Security:** Enable Enhanced Protection, block third-party cookies, and enable HTTPS-Only mode.
* **Change Router Credentials:** Set a **strong and unique** admin password to prevent unauthorized access.
* **Use a Password Manager:** Helps manage strong and unique passwords across multiple accounts.
* **Enable Real-Time Protection in Antivirus:** Ensures ongoing monitoring of threats.
* **Regular Full-System Scans:** Conduct full scans at least **once a month** instead of relying only on quick scans.

# 8. Conclusion

The system is moderately secure, but improvements are needed in browser security, network security, and password management. Implementing the recommended measures will significantly reduce risks and strengthen the system’s cybersecurity posture.

**Signature:**  
Muhammad Talah Khan