HUNAR INTERN
Forge your ambition

Internship Program
Cyber Security
ASSIGNMENT

Arpan Goswami

TASK 1 : Password Policy Review

- Imagine you are working as an IT intern in a small company. Your manager has asked you to review the existing password policy and suggest improvements to enhance the security of user accounts.

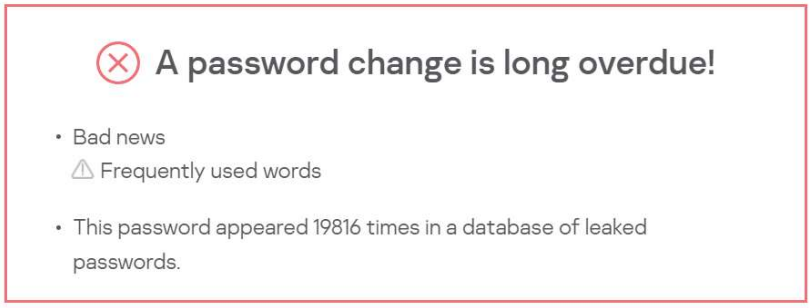
1. Current Password Policy:

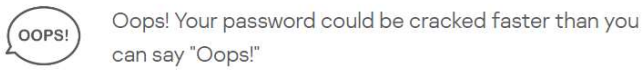
formal password policy

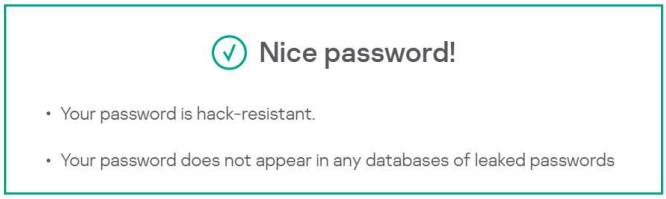
- Minimum Length: 12 characters.
- Complexity: Passwords must include at least one uppercase letter, one lowercase letter, one number, and one special character.
- Expiration: Passwords must be changed every 90 days.
- Password History: Users cannot reuse their last 5 passwords.
- Lockout Policy: Accounts are locked after 5 failed login attempts for 15 minutes.

2. Strength Assessment:

- Check the strength of password using Kaspersky Password Checker tool







Your password will be bruteforced with an average home computer in approximately...

3. Recommendation:

- Enhance Password Length: Recommend increasing the minimum password length if it's below 12 characters. Longer passwords are generally more secure.
- Increase Complexity: Suggest requiring a mix of characters (uppercase, lowercase, numbers, and symbols) if this isn't already enforced.
- Consider Multi-Factor Authentication (MFA): Recommend implementing MFA as an additional layer of security, requiring a second form of verification (e.g., a code sent to a mobile device).
- User Education: Propose regular training or reminders to educate users on creating strong passwords and recognizing phishing attempts.
- Review Expiration Period: If the expiration period is too short or too long, suggest adjusting it. A period of 60-90 days is often considered a good balance between security and usability.
- Enforce Password History: Ensure that users cannot reuse recent passwords to prevent the cycling of old, potentially compromised passwords.
- Strengthen Account Lockout Policies: Tighten the account lockout settings if necessary to protect against brute-force attacks, but ensure it doesn't lead to frequent lockouts for legitimate users.

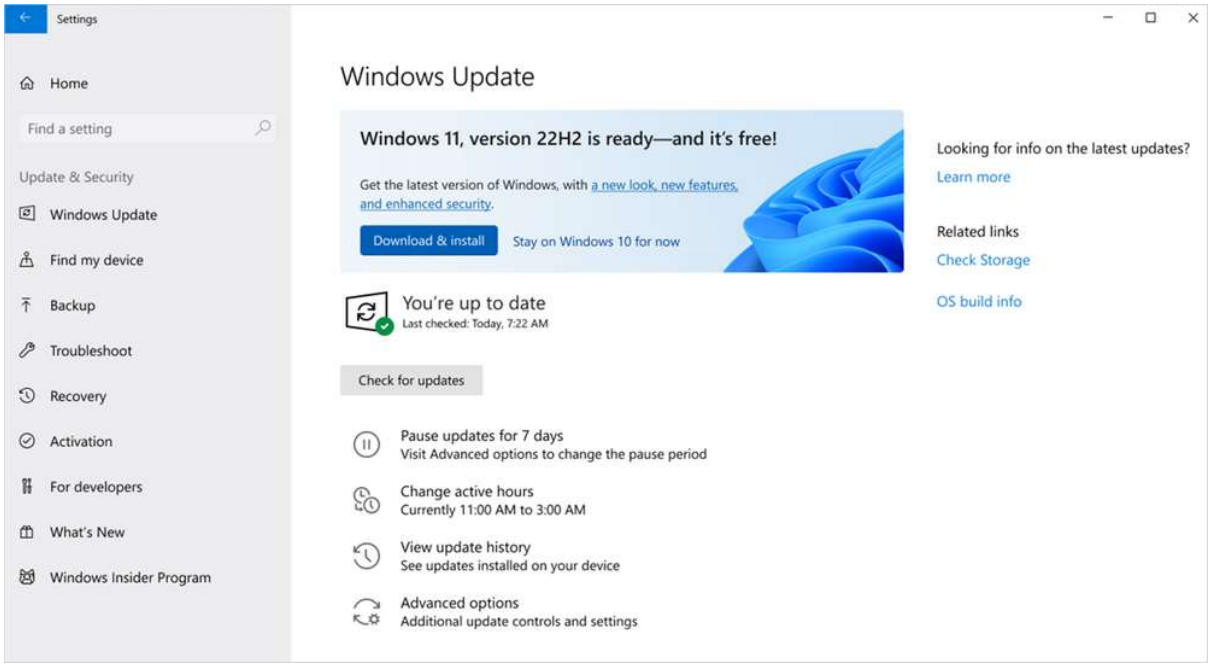
TASK 2 : Device Security Basics

- As part of your internship, you are assigned to set up a new employee's workstation. Your manager emphasizes the importance of securing the device against common threats.

1. Device Configuration:

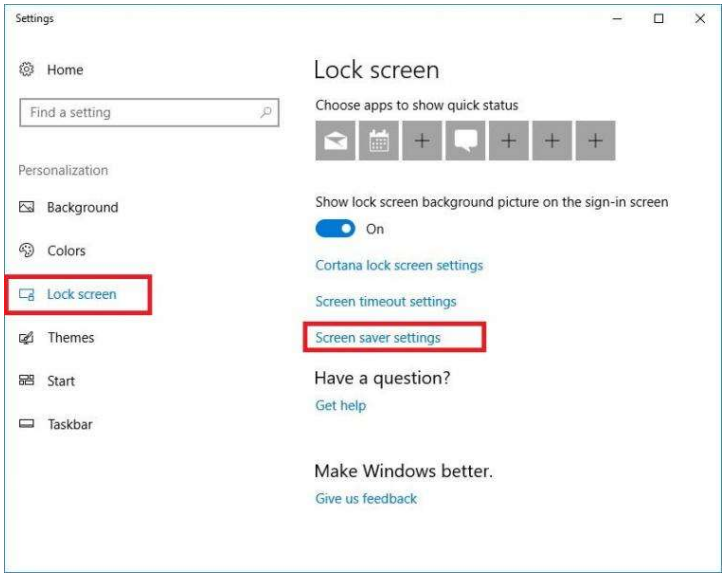
Enable Automatic Updates

- Open Windows Settings: Click on the Start menu and select the Settings gear icon.
- Go to Update & Security: In the Settings window, select Update & Security.
- Check for Updates: Click on Windows Update on the left pane, then click Check for updates to ensure the device is up to date.
- Turn on Automatic Updates: Ensure that Automatic updates are turned on. This will keep the system updated with the latest security patches.



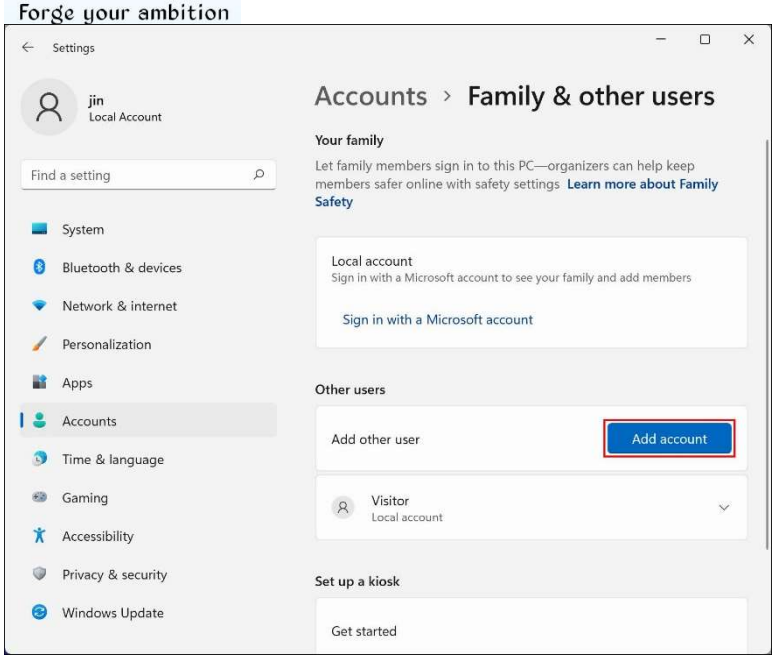
Configure a Screensaver Lock

- Open Screen Saver Settings: Go to Settings > Personalization > Lock screen > Screen saver settings.
- Set the Screensaver: Choose a screensaver from the dropdown menu and set a time after which the screensaver will activate.
- Require a Password: Check the box for On resume, display logon screen to ensure that the user must enter a password to unlock the screen.



Set Up a Guest Account

- Open User Accounts: Go to Settings > Accounts > Family & other users.
- Add a Guest Account: Click on Add someone else to this PC, and choose to add a guest account. Set permissions appropriately to limit access.



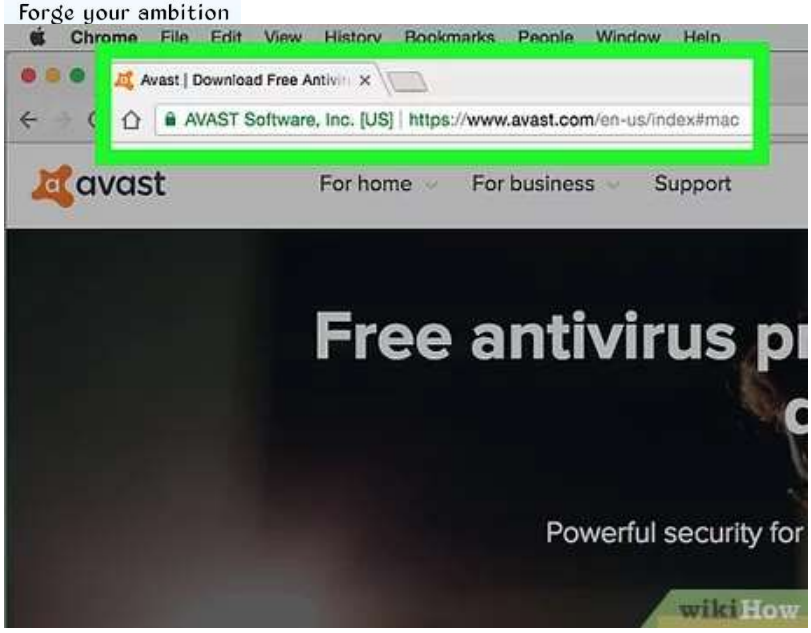
2. Antivirus Software:

Install Antivirus Software

- Choose an Antivirus Program

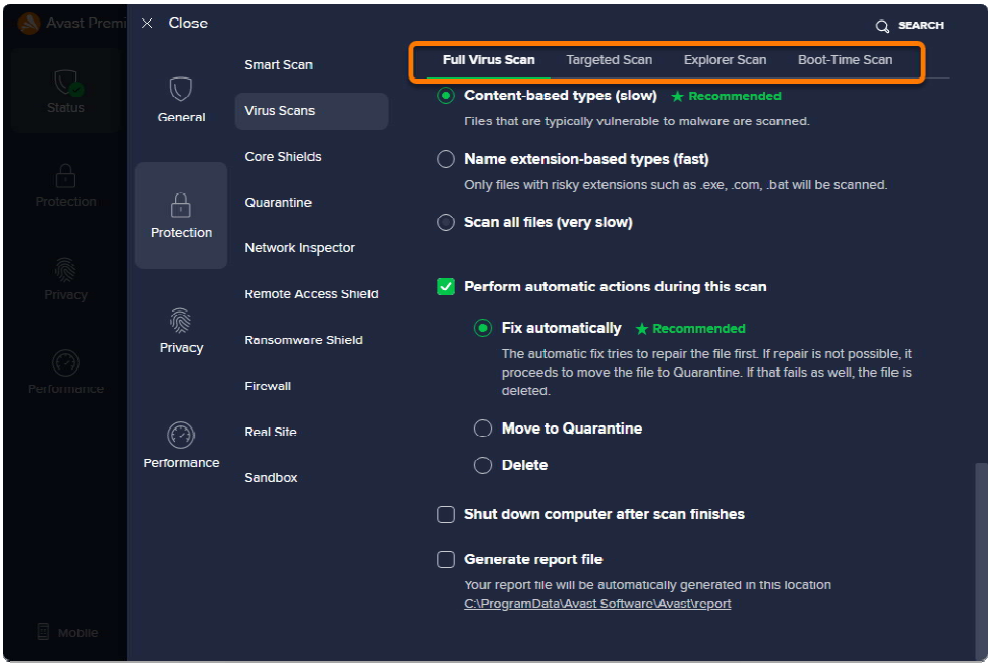
Download and Install:

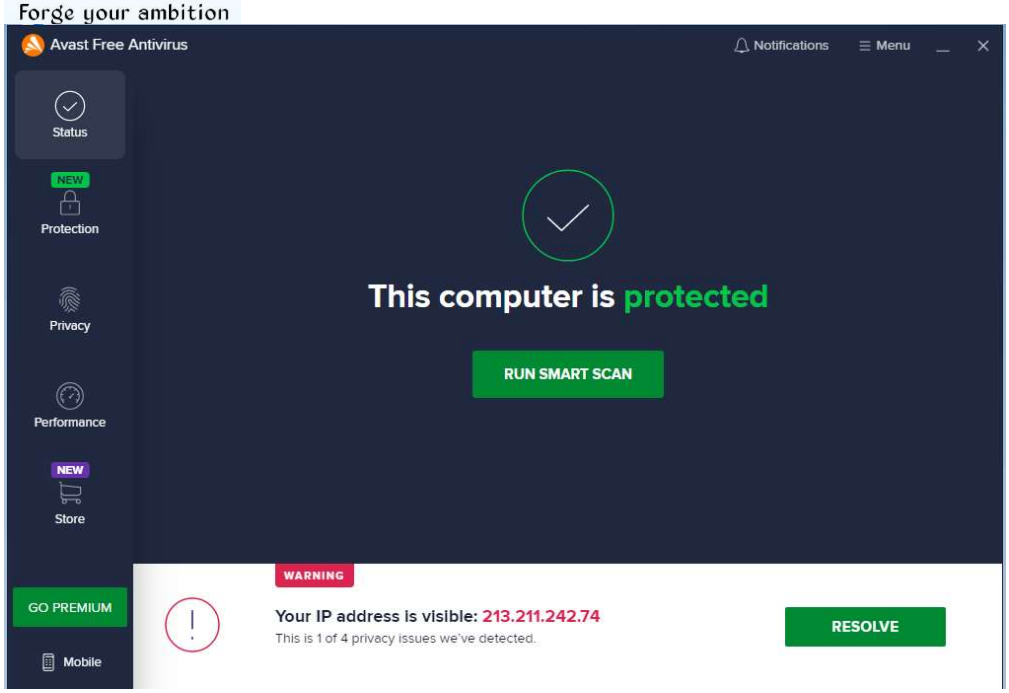
- Visit the official website of the chosen antivirus software.
- Download the installer file and run it.
- Follow the on-screen instructions to complete the installation.



Run a Basic Scan

- Once installed, launch the antivirus software.
- Look for options like Full Scan, Quick Scan, or Smart Scan.
- Select Full Scan to check the system for any threats.
- Once the scan is complete, review the results and take appropriate actions if any threats are found (e.g., quarantine or remove the threats).





3. User Awareness:
   - Prepare a Brief Guide

Recognizing Phishing Emails:

- Check the Sender: Encourage employees to always verify the sender's email address.
- Look for Red Flags: Highlight common signs of phishing emails, such as urgent requests, poor grammar, and suspicious links.
- Hover Over Links: Advise them to hover over links to see the actual URL before clicking.

Using Strong Passwords:

- Create Complex Passwords: Recommend passwords that are at least 12 characters long, with a mix of uppercase and lowercase letters, numbers, and special characters.
- Avoid Common Words: Suggest avoiding easily guessable information like names, birthdates, or common words.
- Use a Password Manager: Introduce password managers as a tool to generate and store complex passwords securely.

Avoiding Suspicious Websites:

- Check the URL: Ensure that the website starts with https:// and look for a padlock icon in the browser's address bar.

- Be Cautious of Pop-ups: Warn against interacting with suspicious pop-ups, especially those claiming to fix a problem or provide a reward.
- Install Ad Blockers: Suggest the use of ad blockers to reduce exposure to potentially malicious ads.

- Distribute the Guide
- Format the Guide: Create the guide as a PDF or Word document with clear headings and bullet points for easy reading.

Share with Employees:

- Send the guide via email to the new employee.