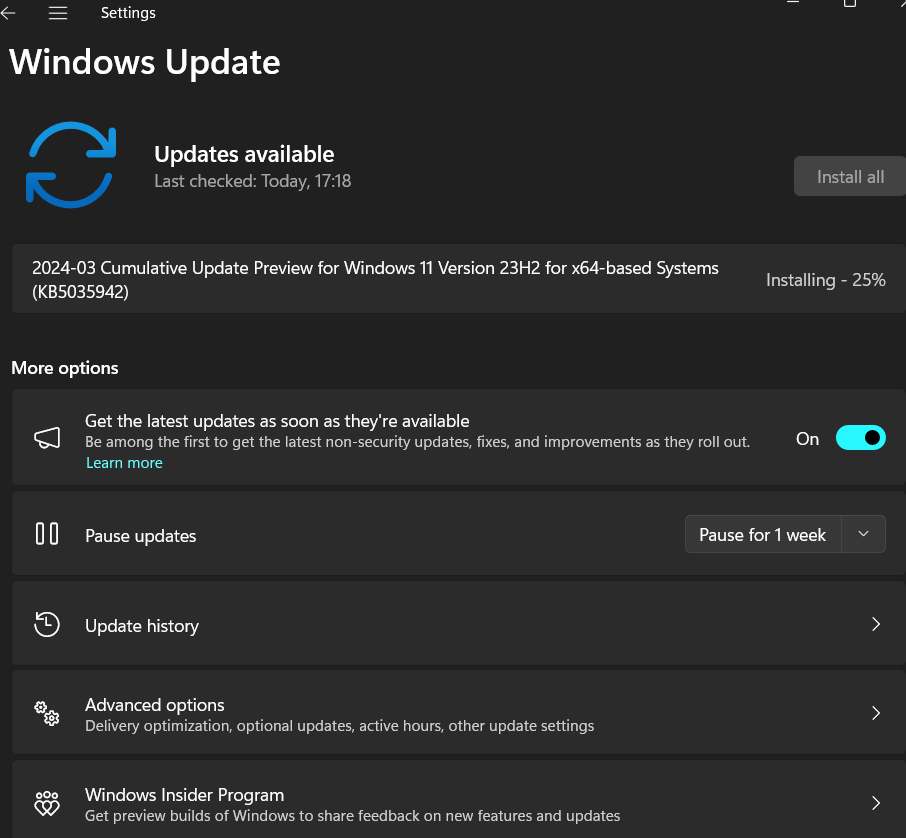
1. **DEVICE CONFIGURATION:**

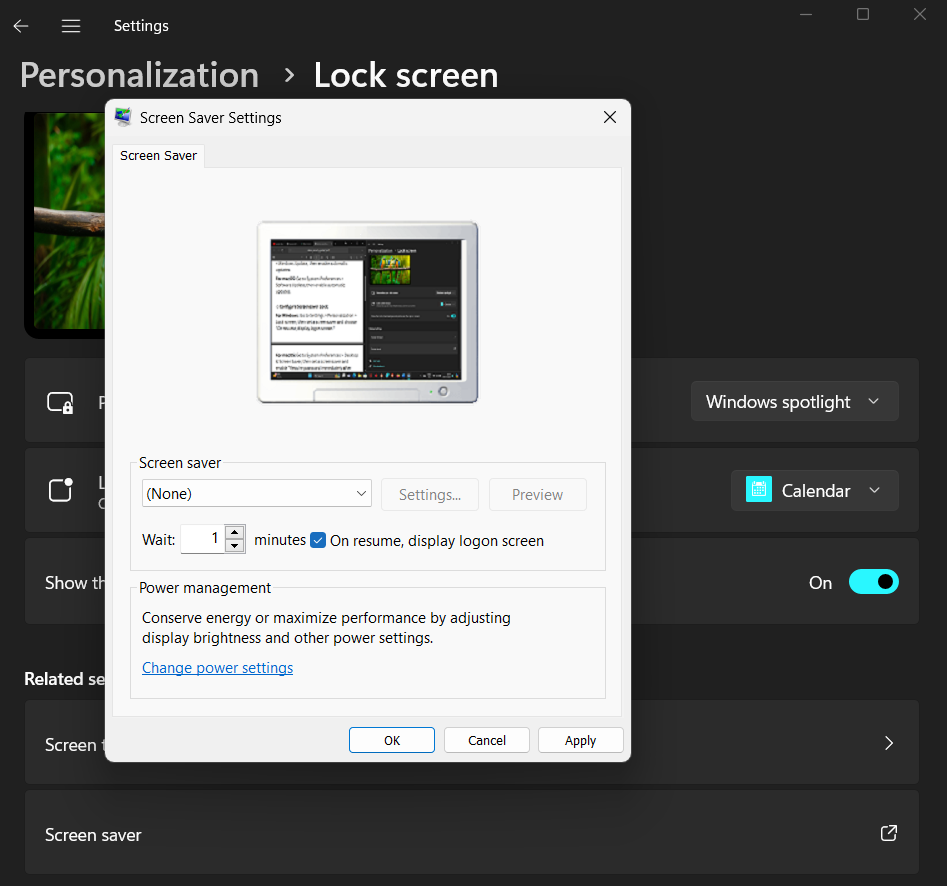
* **Enable Automatic Updates:**

**In windows:** : Go to Settings > Update & Security > Windows Update, then enable automatic updates.



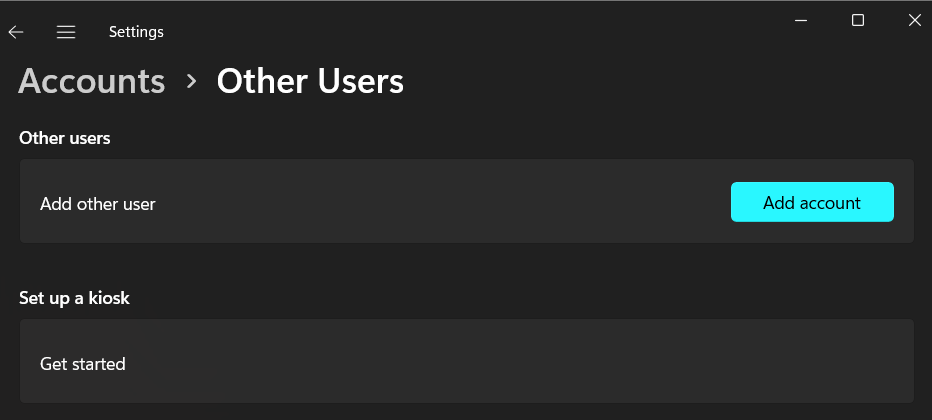
* **Screen Saver Lock:**

In windows:Go to Settings > Personalization > Lock screen, then set a screensaver and choose "On resume, display logon screen."



* **Set Up a Guest account:**

In Windows: Go to Settings > Accounts > Family & other users, then add a new user as a guest.



1. **Antivirus Software:**

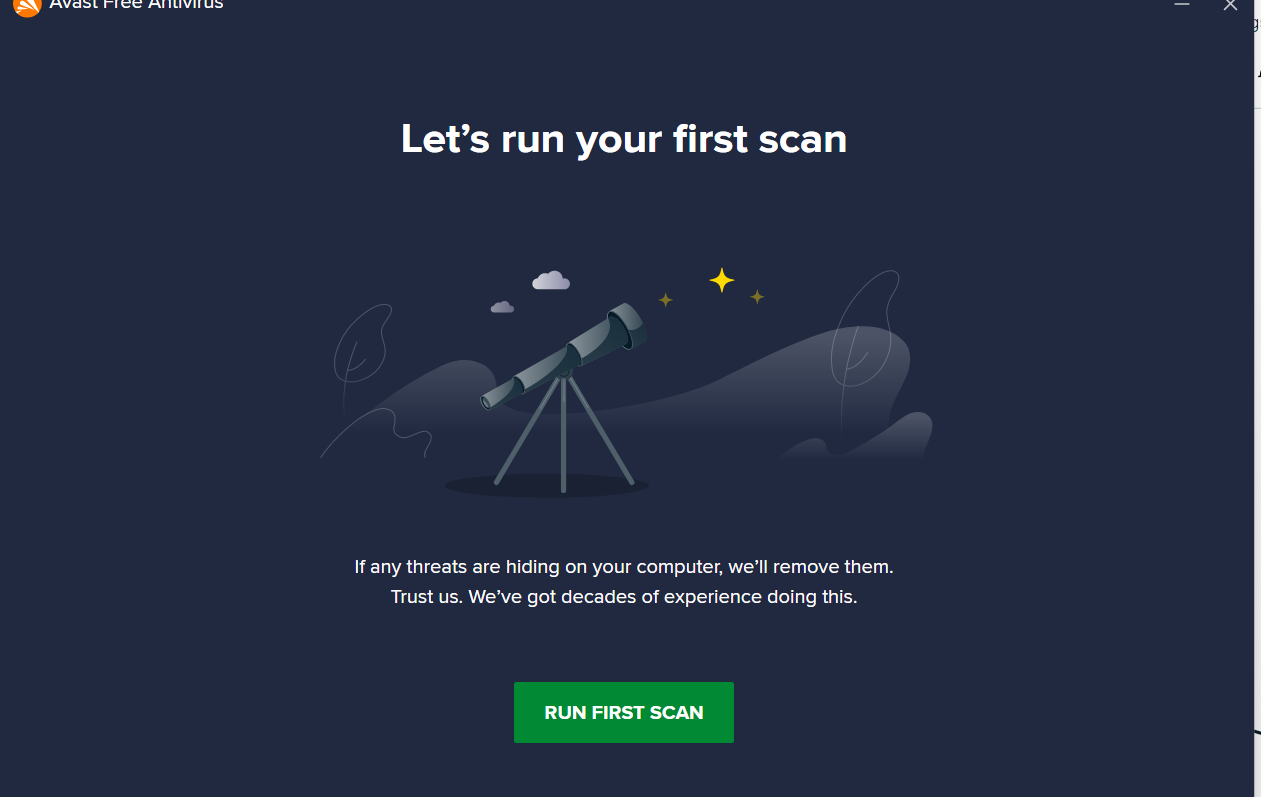
Use a Free Antivirus Software:

* First install a free antivirus software such as AVAST,AVG,BITDEFENDER,AVIRA,MICROSOFT DEFENDER.

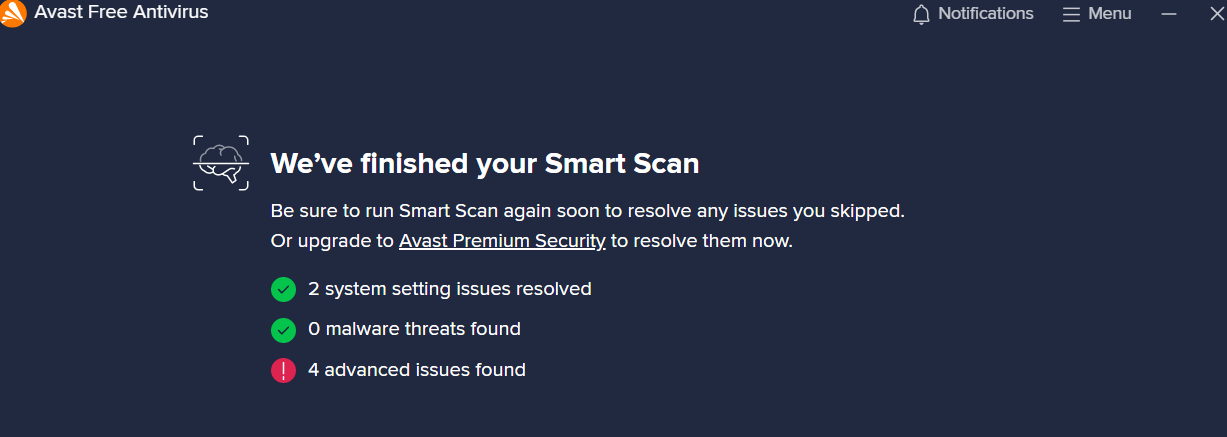


* **Run a Basic Scan**:

Open the antivirus software and initiate a basic scan to check for existing threats.



**Scan Result:**

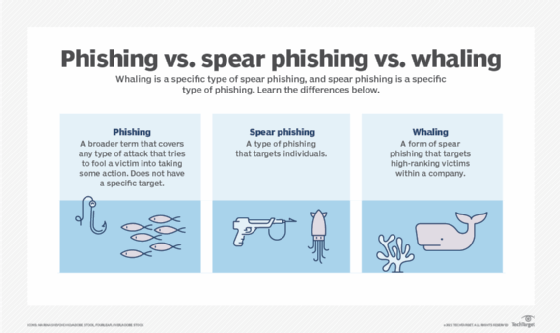
****

**User Awareness:**

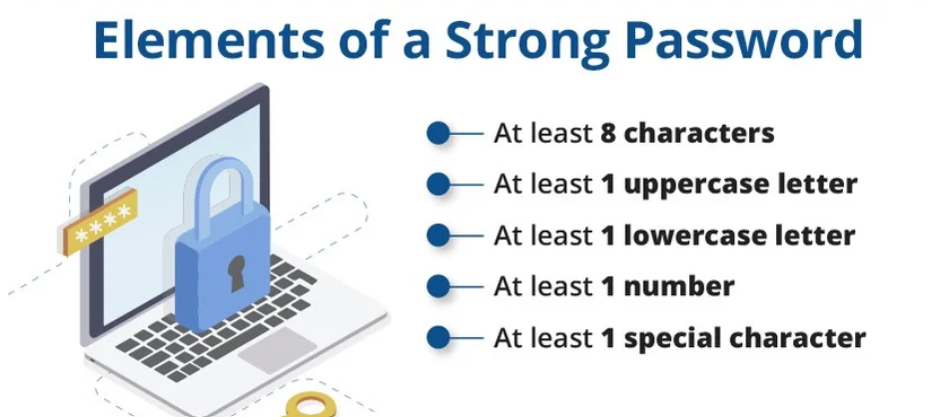
**A Basic Security Guide a For The New Employee**

**Phishing Emails: Phishing is a cyberthreat hackers use to trick individuals into revealing sensitive information, such as passwords and personally identifiable information.**

****

****

**Strong Passwords:** A strong password is one that is designed to be hard for a person or program to guess. Because the purpose of a password is to ensure that only authorized users can access resources, a [password](https://www.techtarget.com/searchsecurity/definition/password) that is easy to guess is a [cybersecurity](https://www.techtarget.com/searchsecurity/definition/cybersecurity) risk.



**Suspicious website:** Always visit https website do not visit http website because the connection is not encrypted.

