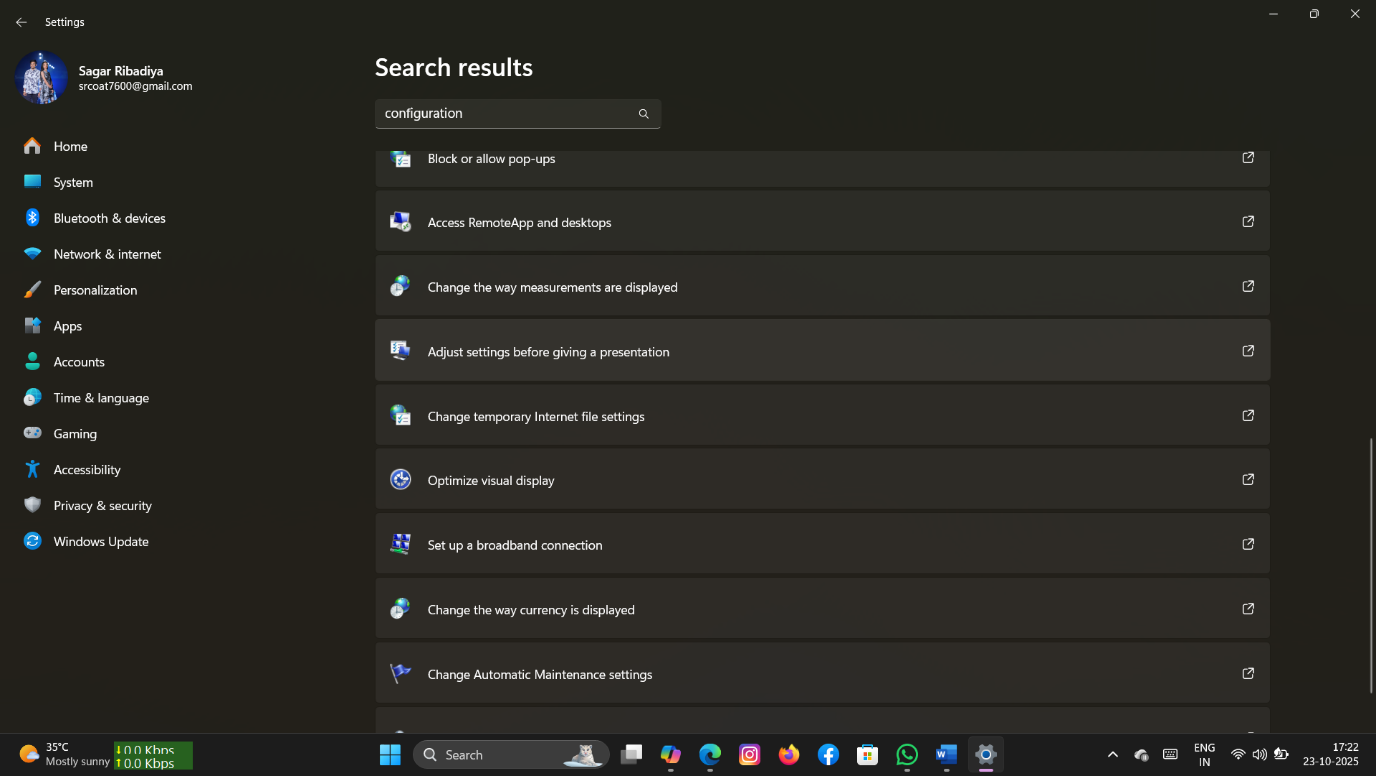
**Task-2 Devise Security Basics**

🔧 **1. Device Configuration**



Screenshot 1 ---- System Configuration



Screenshot 2 ---- windows Update

\* Purpose

To establish a secure, user-friendly environment that minimizes risk from day one.

\* Key Configuration Steps

1. Enable Automatic Updates

• Why: Keeps the operating system and software patched against known vulnerabilities.

• On Windows: Go to Settings → Windows Update → Enable automatic updates

• On macOS: System Preferences → Software Update → Automatically keep my Mac up to date

2. Set Strong Login Credentials

• Why: Prevents brute-force and unauthorized access.

• Minimum 12 characters

• Mix of uppercase, lowercase, numbers, symbols

• Avoid dictionary words or personal info

• Enable multi-factor authentication (MFA) if supported

3. Configure Screensaver Lock

• Why: Prevents unauthorized access when the user is away.

• Set timeout to 5–10 minutes

• Require password on wake

• Use biometric login (fingerprint/face) if available

4. Create a Guest Account (Limited Privileges)

• Why: Allows temporary access without compromising system integrity.

• Disable admin rights

• Restrict access to sensitive folders and settings

• Monitor usage logs if needed

5. Disable Unused Ports and Services

• Why: Reduces attack surface.

• Disable Bluetooth, USB access if not needed

• Turn off remote desktop unless explicitly required

6. Configure Firewall Settings

• Why: Blocks unauthorized inbound/outbound traffic.

• Use built-in OS firewall (Windows Defender Firewall, macOS Firewall)

• Set rules for allowed apps and services

**🛡️ 2. Antivirus Software**

**A screenshot of a computer

AI-generated content may be incorrect.**

\* Purpose

To detect, prevent, and remove malicious software that could compromise system integrity, data confidentiality, or network security.

\*\* Key Setup Steps

1. Choose a Trusted Antivirus Solution

• Free Options

• Windows Defender (built-in for Windows 10/11)

• Avast Free Antivirus

• Bitdefender Free Edition

• Paid Options (for business use)

• Kaspersky Endpoint Security – offers centralized management and strong malware protection

• Norton Business Antivirus – includes VPN, password manager, and identity theft monitoring

2. Install the Antivirus Software

• Download from the official website or trusted app store.

• Follow installation wizard and allow necessary permissions.

• Avoid installing multiple antivirus programs to prevent conflicts.

3. Run Initial Full System Scan

• Scan all drives and folders to detect pre-existing threats.

• Quarantine or delete any suspicious files found.

• Review scan logs for insights.

4. Enable Real-Time Protection

• Monitors system activity continuously.

• Blocks threats as they occur (e.g., during downloads or file access).

• Ensure this feature is turned on in settings.

5. Schedule Regular Scans

• Weekly full scans recommended.

• Daily quick scans for active threats.

• Set scan times during off-hours to avoid performance impact.

6. Update Virus Definitions Regularly

• Antivirus software relies on updated threat databases.

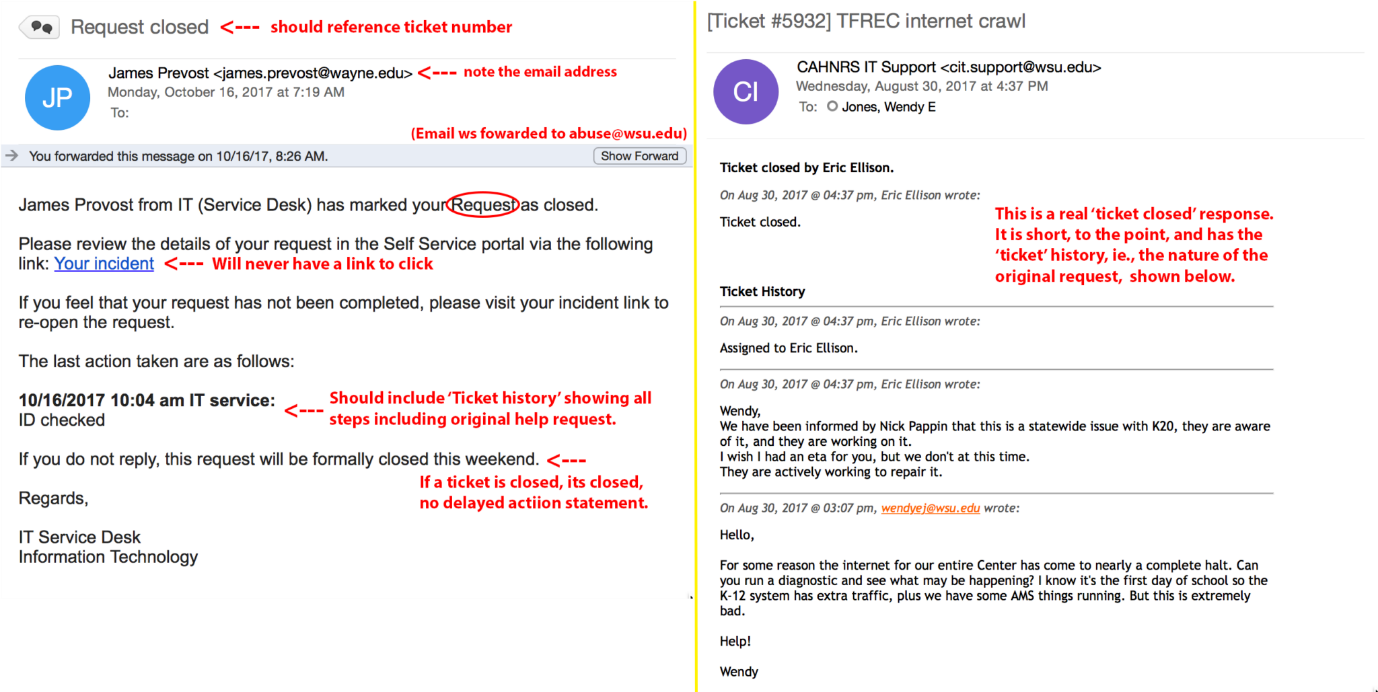
• Enable automatic updates to stay protected against new malware variants.

**3. User Awareness**

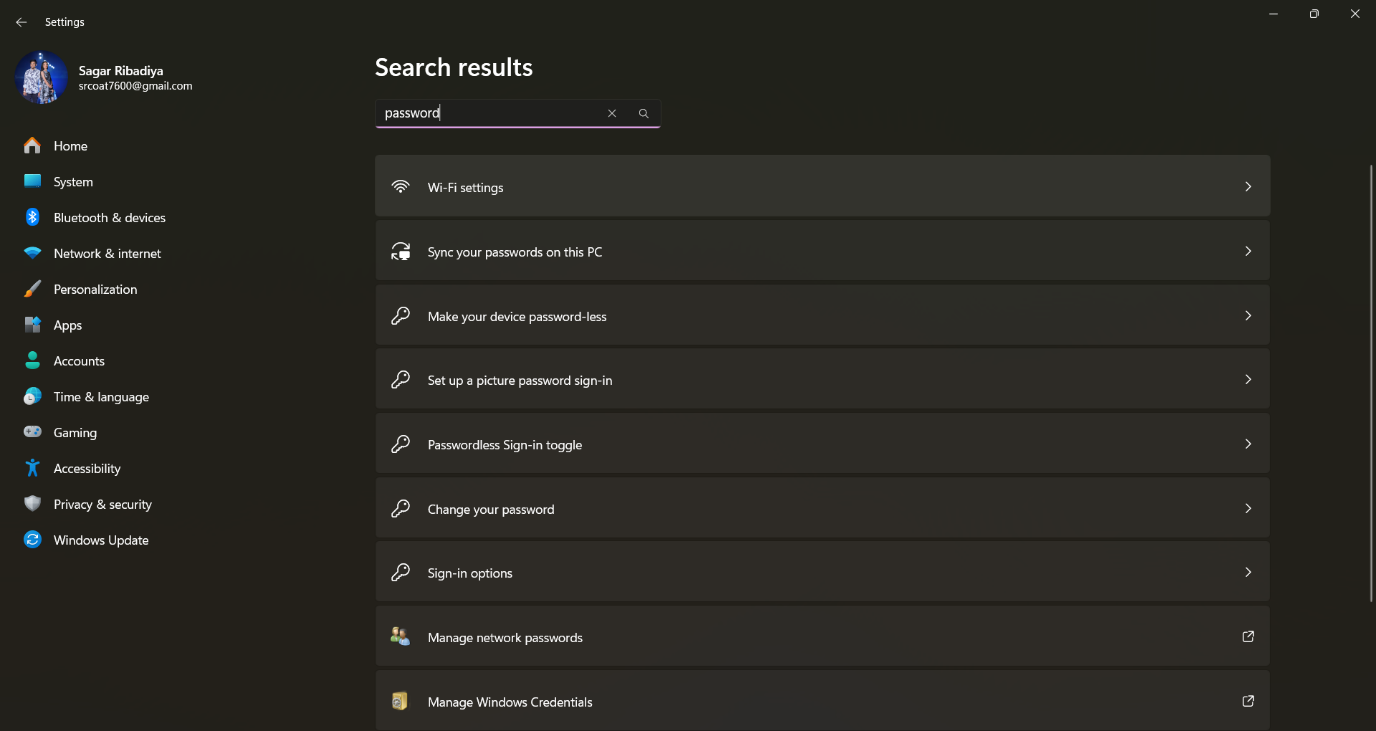
A yellow and black padlock with a exclamation mark

AI-generated content may be incorrect.

**Figure 1:** Example of a secure website (HTTPS padlock icon)



Screenshot 4 ---- phishing email with red flags highlighted



Screenshot 5 ---- Password manager interface

\*Purpose

To educate the new employee on basic cybersecurity hygiene so they can avoid falling victim to phishing, weak passwords, and unsafe browsing habits.

\*\* Core Topics to Cover

1. Phishing Awareness

• What it is: Fraudulent emails or messages that trick users into revealing sensitive information.

• How to recognize

• Suspicious sender addresses

• Urgent or threatening language

• Unexpected attachments or links

• Generic greetings like “Dear user”

• Best Practices

• Never click unknown links

• Verify sender identity

• Report suspicious emails to IT

2. Password Security

• Why it matters: Weak or reused passwords are a top cause of breaches.

• Best Practices

• Use long, complex passwords (12+ characters)

• Avoid using the same password across platforms

• Use a password manager (e.g., Bit warden, LastPass)

• Enable two-factor authentication (2FA) wherever possible

3. Safe Browsing Habits

• Risks: Visiting malicious websites can lead to malware infections or data theft.

• Best Practices:

• Only download software from trusted sources

• Avoid clicking pop-ups or ads

• Use secure (HTTPS) websites

• Keep browser and plugins updated

🧠 Training Suggestions

• Conduct a short onboarding session or share a PDF guide.

• Use real-world examples (e.g., phishing email screenshots).

• Include interactive elements like quizzes or simulations.

• Offer bilingual resources for better understanding.