CYBERSECURITY TIPS FOR INTERNATIONAL RESEARCH TRAVEL

KENNESAW STATE UNIVERSITY
UNIVERSITY INFORMATION TECHNOLOGY SERVICES

1 Secure Your Devices Before Departure

Update operating systems, apps, and antivirus software. Back up critical data.

2 Use Strong Authentication

Enable multi-factor authentication (MFA). Use unique, complex passwords.

3 Limit Sensitive Data

Carry only necessary data and devices. Remove confidential information before travel.

4 Protect Network Connections

Avoid public Wi-Fi; use a VPN for all internet activity. Disable auto-connect features including Wi-Fi.

5 Be Cautious with Physical Security

Keep devices with you at all times. Use privacy screens in public spaces.

6 Watch for Phishing

Be alert to phishing emails, suspicious links, and impersonation attempts. Verify identities before sharing info.

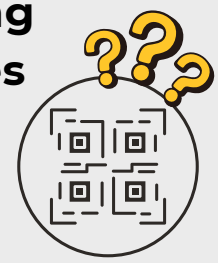
7 Use Secure Communication

Use MS Teams for secure communications. Avoid discussing sensitive research over unsecured channels.

8 Restart Devices

Power off all devices daily to limit unauthorized access and boost overall security.

9 Be Careful Scanning Unknown QR Codes



Unknown QR codes can lead to malicious sites—scan only from verified sources.

10 Report Issues Immediately

Contact the UITS Service Desk to report any suspicious activity.

470-578-6999 or service@kennesaw.edu