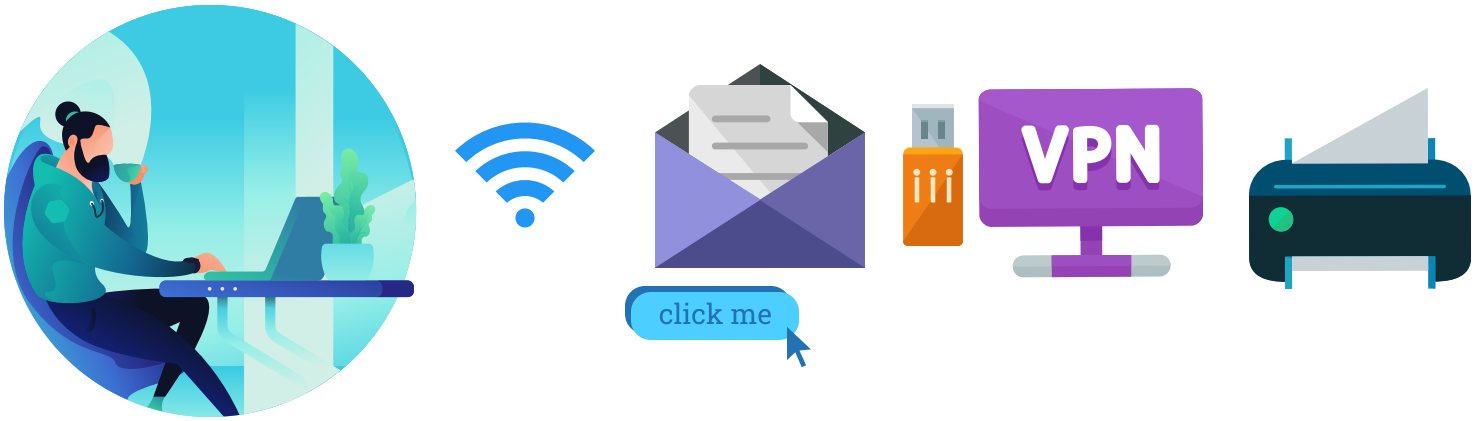
Security for Remote Staff



Most companies transitioned to a Work From Home (WFH) situation quickly, leaving little time to ensure that devices are properly secured. Companies will continue to support WFH going forward. Six areas of security to consider for remote workers regardless if using a company or personal device (not recommended):

1. Remote Access Controls

- VPN
- Multifactor Authentication
- Limit access to resources
- Secure printing

2. Data Access Oversight

- Monitor access to data
- Use data-loss-protection and behavioral analytics
- Secure removable media

3. Asset Management Controls

- Inventory devices with access to the network
- Regularly patch and update Antivirus
- Restrict network traffic by MAC address

4. Physical Security Controls

- Dedicated workspace
- Privacy screens
- Secure any sensitive paper documents
- Limit local printing
- Limit use of removable storage

5. Training and Awareness

- Business Email Compromise
- Malware awareness
- Clean Desk Policy
- Public Wi-Fi risks

6. Policy Review and Updates

- Remote Access Policy
- Work from Home Policy
- BYOD Policy
- Acceptible Use Policy
- HR Policy

LORICCA.COM

LORICCA