Working From Home Securely

Remote work offers flexibility but also creates new security challenges. Unlike office environments, home networks and personal setups often lack strong protections, making them easier targets for attackers. Employees must take extra care to safeguard company data when working outside the office.

Key Risks

Weaker Home Networks

Many home routers still use default or weak passwords, making them vulnerable to hacking. Once inside, attackers can monitor traffic or steal data.

Tip: *Set a strong, unique password on your WiFi router and keep its firmware updated.*

Shared Devices

Using family or personal devices for work increases the risk of data leaks, especially if those devices lack security controls.

Tip: *Keep work devices separate and never share them with family members.*

Unsecured Connections

Public or home networks without proper safeguards expose sensitive company information.

Tip: *Always use the company VPN when working remotely to secure your connection.*

Physical Security at Home

Even at home, leaving your screen unlocked can allow others to see confidential information.

Tip: *Lock your screen whenever you step away, just as you would in the office.*