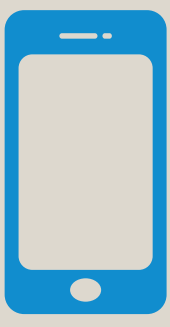
REMOTE WORK SECURITY THREATS

Let's talk about five common remote work security threats and potential solutions you can implement as an employee or business leader.

1 WIFI AND REMOTE ACCESS VULNERABILITIES

Employees: Change the default password and enable encryption on your router.

Businesses: Implement security awareness training and an Acceptable Use Policy, deploy a VPN if practical, require MFA, explore passwordless authentication options, and enforce Transport Layer Security (1.2 or higher).



2 PERSONAL DEVICE USAGE

Employees: Enable a passcode, encrypt the device, and keep the device updated and patched regularly.

Businesses: Develop and enforce a Mobile Device Management (MDM) strategy and Bring-Your-Own Device (BYOD) Policy. Require MFA on all remote applications.

3 UNSECURED VIDEO/ AUDIO CONFERENCING

Employees: Update your conferencing app regularly to ensure you have access to the latest security options. Generate a unique ID for your meeting instead of using a permanent access code. Add a password requirement when scheduling an audio/video meeting.

Businesses: Embrace one tool company wide, and educate employees on the above to make everyone's experience as secure as possible.

4 DATA SECURITY RISKS

Employees: Only input personal, company, and/or sensitive data into secure sites (look for HTTPS).

Businesses: Create and enforce an Acceptable Use Policy to set clear expectations for remote equipment and systems usage, and establish solid endpoint security solutions (i.e., screen locks, password authentication to machines).

5 ROGUE APPLICATION USAGE

Employees: Only use or access company information via approved tools, hardware, and software.

Businesses: Maintain a complete and accurate inventory of each and every outside application so you're aware of all the places your company information could be living. Consider a cloud access security broker (CASB) and ensure your security teams and tools are monitoring for abnormal system usage.

BARR ADVISORY