# Home Network Security

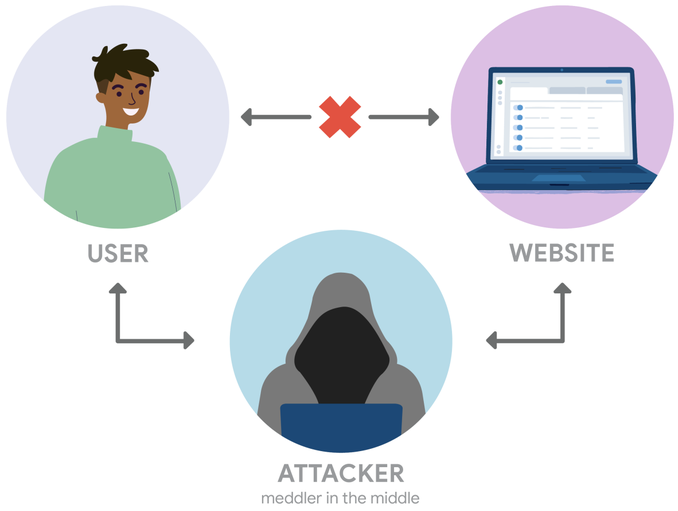
## Home Network Security

Employees who work from home use home networks to access company files and programs. Using home networks creates security challenges for companies. Companies can provide employees guidance for protecting their home networks from attacks. This reading will cover common attacks on home networks and steps to make home networks more secure.

## Common security vulnerabilities

Home networks have vulnerabilities to various types of attacks. The most common security attacks on home networks include:

- **Meddler in the middle attacks** allows a meddler to get between two communication devices or applications. The meddler then replies as the sender and receiver without either one knowing they are not communicating with the correct person, device, or application. These attacks allow the meddler to obtain login credentials and other sensitive information.




- **Data Theft** is when data within the network is stolen, copied, sent, or viewed by someone who should not have access.
- **Ransomware** uses malware to keep users from accessing important files on their network. Hackers grant access to the files after receiving a ransom payment.

## Keeping home networks secure

To protect company data, employees working from home need to take steps to improve the security of their home networks. Home networks can have added protection without expensive equipment or software.

Employees can take steps to keep home networks more secure:

- **Change the default name and password** using the same password guidelines as your company.
- **Limit access to the home network** by not sharing access credentials outside of trusted individuals.
- **Create a guest network** that allows guests to connect to the internet but not your other devices.
- **Turn on WiFi network encryption** requiring a password before a device can access the internet.
- **Turn on the router's firewall** to prevent unwanted traffic from entering or leaving your wireless network without your knowledge. Regularly update your router firmware.
- **Update to the newest WiFi standard** which is the most secure standard for home WiFi.

Another security measure that a company can take is for employees to work over a virtual private network, or VPN. Using a VPN creates an encrypted, secure internet connection through which employees can access company data.

## Key takeaways

Home network security is vital to protect a company's sensitive information when employees work from home.

- Data theft, ransomware, and meddler in the middle are common attacks on home networks.
- Employees working from home need to take steps to improve the security of their home networks.

**Mark as completed**