

The Internet of Threats

The lines between home and work continue to blur

Trend Micro's Head in the Clouds research shows that smart home devices and their associated apps could represent a weak link in the chain of cybersecurity



13,000remote workers27countries

The expanding home network



52%

of remote workers have IoT devices such as smart lights, plugs and door locks connected to their home network



10%

of these workers use IoT devices from lesser-known brands, which unfortunately often have well documented weaknesses such as an inability to update firmware or insecure log-ins

This could compromise a home network and open the door to a corporate one

A route in for hackers



70%

of remote workers connect corporate laptops to their home network, with 56% of them downloading a non-work application to their device



57%

of these workers have downloaded an application which directly controls their smart home

by linking work devices to potentially unsafe IoT equipment either directly or via their home network

Remote workers are putting corporate data at risk

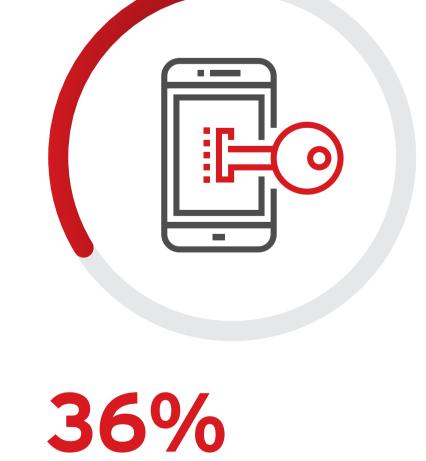
Bad habits continue with personal devices



of remote workers are likely

policy, by accessing business data from a personal device is could create another eas

break corporate security



or over one third,

don't even have basic password protection on all personal devices

This could create another easy route into the corporate network by potential bad actors

Remote workers need to be aware of how their home network setup may put corporate cybersecurity at risk. But not everyone sees

risk the same. Organisations need to move from generic education and training towards a more tailored IT security strategy that accounts for a range of cybersecurity personas.





To find out how, visit **trendmicro.com**