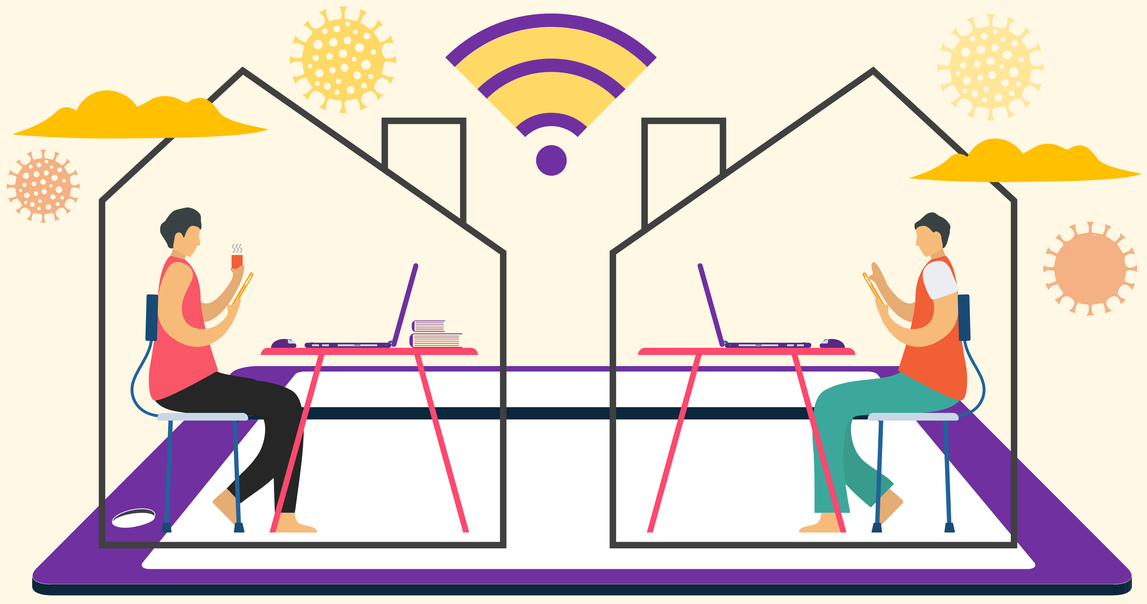
anunta®

SECURING THE NEW NORMAL



SECURITY RISKS IN REMOTE WORK

COVID-19 has accelerated the transition of traditional workplace towards remote working model. The IT and security teams are under pressure to respond quickly to the new normal, resulting in cybersecurity gaps and vulnerabilities.

In one of the reports published, nearly **25%** of employees using personal devices for remote work claim that they are unaware of the security protocols on their device and more than **1-in-4** have recurring issues with spotty Wi-Fi, limiting the antivirus' functions.

Source: *Morphisec's WFH Employee Cybersecurity Threat Index.*

1 GROWING MALWARE ATTACKS

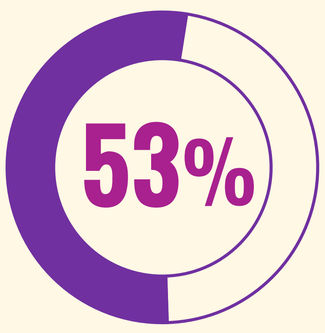
Google tallied more than **18 Mn** malware and phishing emails related to the novel coronavirus on its service each day in April.

Source: *Mckinsey*

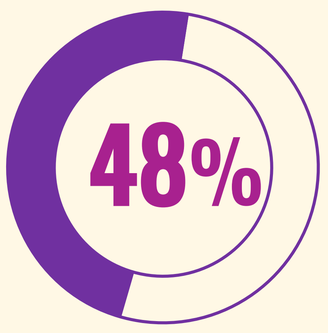
It also reported identifying more than a dozen government-backed groups using COVID-19 themes for these attempts.

The most common tip employees receive from IT in transitioning to WFH was being cautious of

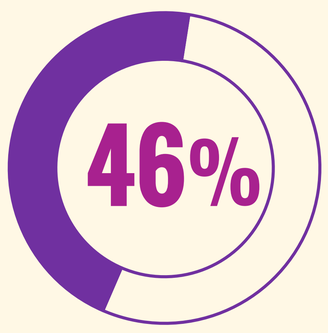
Suspicious emails, attachments, or pop-ups



This was followed by ensuring antivirus software was active



and updating software frequently



Source: *Morphisec's WFH Employee Cybersecurity Threat Index*

2 LACK OF IT CONTROL

of respondents who are newly working from home said none of the personal devices they use for work are administered by their employer.

Source: *IBM Security Work From Home Study*

3 HANDLING USER SENSITIVE DATA

4 out of 10

of respondents who are newly working from home said they handle Personal Identifiable Information (PII) including Social Security Number, financial information, and personal medical information in their job.

Source: *IBM Security Work From Home Study*

Adopt Cloud Desktops for Secure Remote Work

Eliminate data storage at the local endpoints of the remote workforce and secure the desktop infrastructure through increased adoption of Cloud Desktop. It delivers:

Zero Trust Environment
Provides access at the application layer

Multi-Factor Authentication
Protects access to enterprise data and application

HIPPA & PCI Compliance
Compliant with security protocols for handling sensitive data

Centralized Desktop Management
Regular security and patch update ensuring complete IT control

Single Sign-On
Provides user with secure access to external resources