

UNISYS SECURITY INDEX™ 2021 AUSTRALIA



THE UNISYS SECURITY INDEX FOR AUSTRALIA IS AT A 15 YEAR HIGH: 159 OUT OF 300 POINTS

TOP SECURITY CONCERNS FOR AUSSIES

Despite COVID-19, in 2021 Aussies are more concerned about protecting our data and privacy than natural disasters such as pandemics.



Identity fraud



Hacking and viruses



Bankcard fraud



Online shopping



Natural disasters



Financial obligations



National security



Personal safety

UNPREPARED TO AVOID SECURITY THREATS WHEN WFH

While Aussies are concerned about data theft and hacking, they don't know what threats to look for or who to tell.



39%
4 in 10 click on suspicious links in emails



73%
3 in 4 don't know who to report a data breach to



55%
Half don't know about SMSing scams



79%
8 in 10 haven't heard of SIM jacking

AUSSIES PUSH BACK ON EMPLOYER MONITORING

While Australians enjoy the convenience of working from home, most don't support employer monitoring measures regardless of whether it is for productivity, security or IT support.

FOR SECURITY



82%
Reject facial recognition on webcams to authenticate user



81%
Believe monitoring their computer screen is off limits



85%
Don't want to share passwords



85%
Deny their organisation access to their microphone

FOR PRODUCTIVITY

62%

Aren't comfortable with login/logout monitoring



76%
Reject mandates to turn on video for meetings



81%
Disagree with keyboard activity level monitoring



81%
don't want their browser history on personal devices used for work checked

73%

Don't want software response times monitored



EMPLOYEE EXPERIENCE IMPACTS SECURITY

43% of Aussies admit they have downloaded unapproved apps or software on work devices, because...



43%
It is better than the tools my company provided



38%
Want to use the same software or apps used in their personal lives for work



36%
Confessed to downloading apps for entertainment or personal use

UNISYS RECOMMENDS FOUR SECURITY ESSENTIALS FOR ALL WORKPLACES



#1
Ensure ongoing & updated training in how to spot cybersecurity threats



#2
Also implement policies and technologies to make it extra hard for people to do the wrong thing



#3
Be transparent about how and why WFH monitoring takes place to create a culture of trust and understanding



#4
Review if traditional methods of productivity monitoring are still relevant ie. hours vs output