If the conflict in the Middle East causes the "not a fuel crisis" to eventuate, are you ready to pivot to working from home again?

Are your security systems in place? Do you have some control over the devices that will be connecting to your IT? Do you have a way to keep security in the fore of people's mind?

The last time we were all told to work from home, cyber criminal activity spiked to its highest levels, resulting in the greatest ever monetary loss recorded by Australian businesses.

Technological advancements such as AI being expertly adopted by cyber criminals are changing the playing field. It is increasingly difficult to spot bad content in emails and web sites.

Savvy businesses are deploying security systems and processes to protect their computer fleet and, importantly, to protect their people's privately-owned computers that access the business' systems.

Savvy businesses have centrally managed protection against:

- anti-virus and anti-malware
- phishing and business email compromise
- web sites that are compromised or intentionally serving bad content

Businesses that do not have these protections in place on all computers that interact with their systems are taking a big risk, particularly at a time when it may become challenging for IT support to rapidly get on-site to overcome security breaches.

Remex can deal with this for you from less than $7 per computer per month.

These are protections that you should have anyway, but the potential of having your people working from home again raises the urgency to get things in place because we know, from experience, cyber criminals will increase their activity while they believe people are more susceptible to exploitation.

It is reported that approximately 90% of Australian business respondents faced phishing, business email compromise and/or email-based ransomware attacks during the Covid-19 pandemic “shut down” of 2021.

AI enables targeted and very sophisticated attacks to be created and deployed in minutes rather than days.

AI-generated phishing campaigns are reportedly four times more likely to get someone to take the bait, compared to human-generated attacks.

Gen Z is the generation currently most susceptible to phishing attacks. They’re also the generation most likely to mix personal and work devices. If you want to check this, just Google: “Which generation is most susceptible to phishing”

Information published by the ACCC shows the highest volume of losses through scams in Australia occurred in 2022 ($3.15 billion).

According to the Commonwealth Bank, your business’ best defence includes:

- ensuring your IT security is up to date
- run antivirus software
- have a good firewall
  and
- maintain staff awareness.

This is exactly where Remex can help you.

remex.com.au/prepare.html