Over the past 5 years a scam known as electronic funds transfers at the point of sale (EFTPOS) skimming. People commonly swipe both credit and debit cards through the in-store machines to pay for goods and services and hackers have figured out how to skim customer cards.

BankInfoSecurity reports “The news is just one in a growing line of POS skimming fraud schemes. From the Michaels POS PIN pad swapping scam, which hit in May, to the Save Mart Supermarkets self-checkout breach announced in the last two weeks, merchant-level card security is garnering new attention.”

In Australia, Fast-food, convenience and specialist clothing stores are bearing the brunt of the crime. McDonald’s is among the outlets whose EFTPOS machines have been targeted for card skimming.

Officials say the problem is so bad they urged people to change credit and debit card pin numbers weekly to avoid the possibility of having their account balances wiped out, as it was likely more cases would be identified.

In the United States a similar card skimming scam was pulled off at the Stop and Shop Supermarket chain.

Anyone with inside knowledge of payments can easily hack a POS system. “Then they simply use tools to crack a Windows remote desktop – defaults at port 3389 – program’s password, and they are in.”

Here’s an abridged version of the protection tips against POS skimming fraud offered by BankInfoSecurity

#1 Never affiliate the business name with the name of the Wi-Fi network.

#2 Upgrade POS equipment and software regularly, and continually change device passwords. ”

#3 Ensure payments systems comply with Payment Card Industry Data Security Standard from end to end.

#4 Monitor network traffic.

Robert Siciliano personal and small business security specialist to ADT Small Business Security.