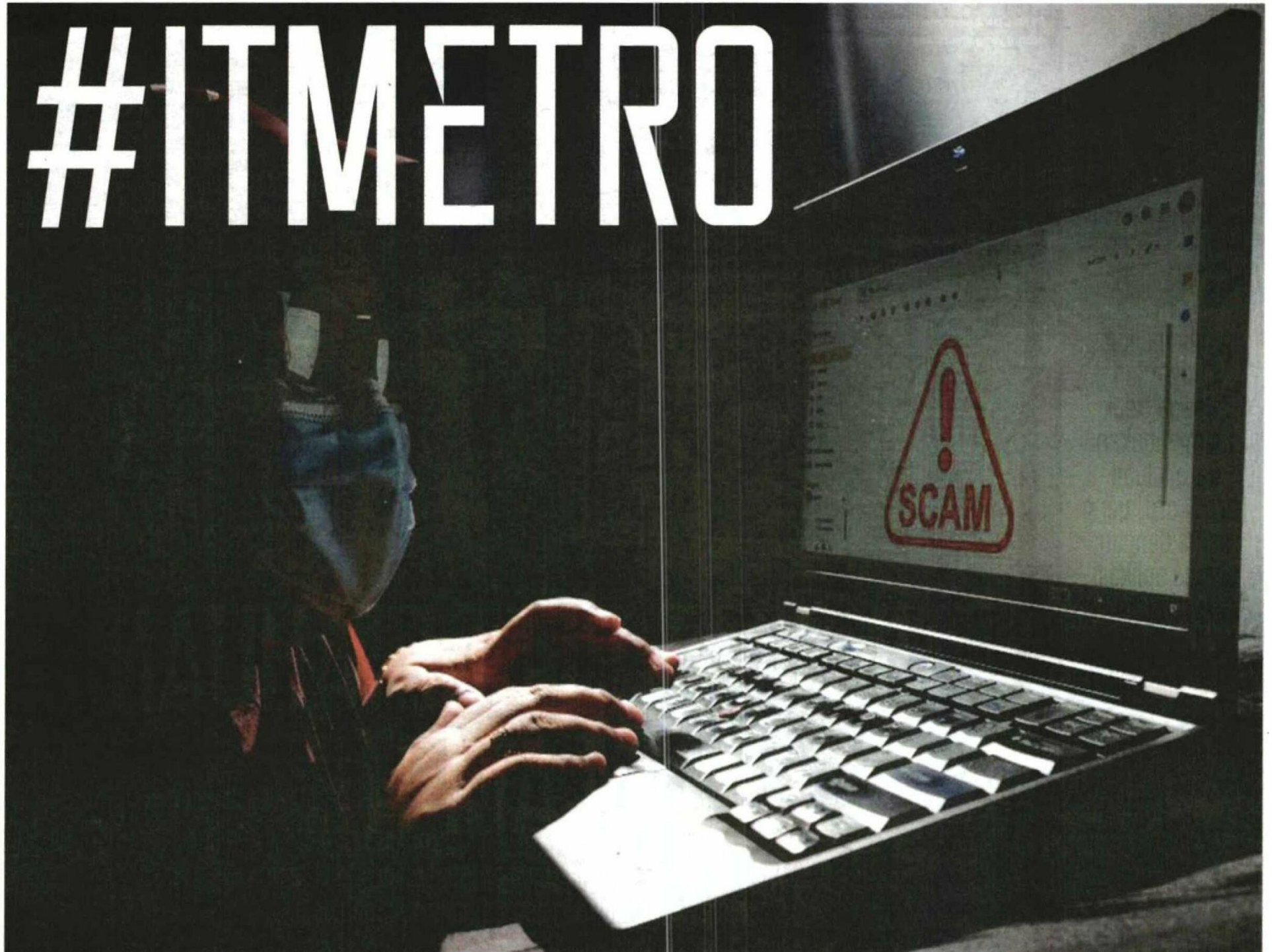




MEREKA PANTAU TELEFON KITA

Penggodam cipta perisian hasad memantau serta memancing mangsa, pengguna boleh guna antivirus berbayar pada gajet

FOKUS

Oleh Muhammad Saufi Hassan
saufi@mediaprima.com.my

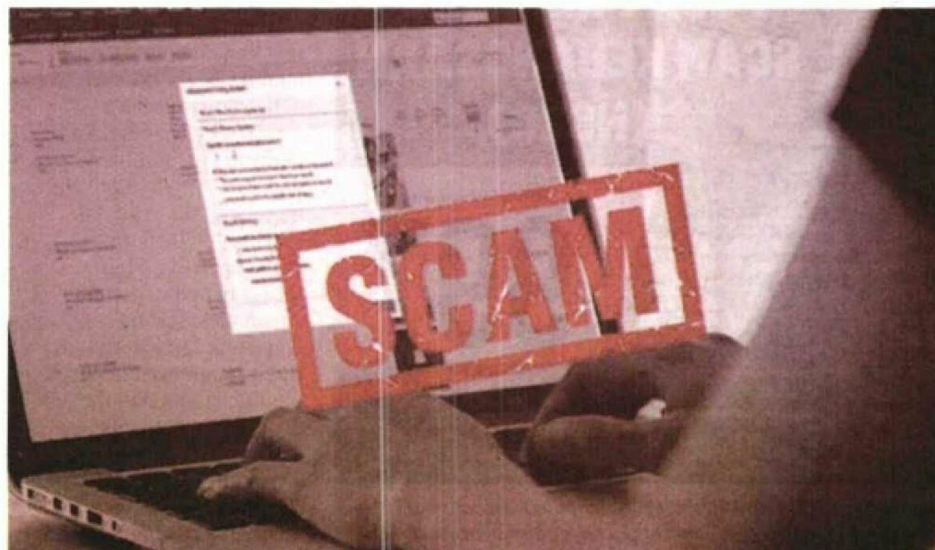
Beberapa tahun lalu, pengguna terpaksa berdepan dengan pelbagai birokrasi untuk melaporkan kes penipuan atas talian atau 'scam' ini.

Berdasarkan senario terdahulu, pengguna yang menyedari berlaku pengaliran wang keluar daripada akaunnya perlu melaporkan kepada institusi perbankan untuk menyekat akaun kemudian

melaporkan kepada pihak polis untuk tindakan susulan.

"Walaupun kita terpaksa membayar sedikit untuk antivirus berkenaan asalkan dapat menyelamatkan aktiviti transaksi kita daripada kerugian kelak—Siraj Jalil

Hasil daripada inisiatif kerajaan berjaya mewujudkan satu pusat khusus untuk menangani jenayah penipuan atas talian ini dengan kewujudan Pusat Respons Scam Kebangsaan (NSRC) dengan menghubungi talian 997 sebagai nombor kecemasan



baharu.

Presiden Persatuan Pengguna Siber Malaysia (MCCA) Siraj Jalil yang menyambut baik inisiatif berkenaan turut menyatakan bahawa pengguna perlu melaporkan menerusi panggilan kecemasan 997 berkenaan.

"Agensi ini akan membabitkan kerjasama dengan Polis Diraja Malaysia (PDRM), Suruhanjaya Komunikasi dan Multimedia (SKMM), Pusat Pencegahan Jenayah Kewangan Nasional (NFCC) serta Bank Negara Malaysia (BNM) berkaitan isu kewangan.



pengguna juga diingatkan supaya tidak menggunakan kata laluan (password) yang sama dengan semua aplikasi kerana itu tindakan yang paling bahaya

SIRAJ JALIL

DARI MUKA 35

"Bagi mendepani isu scam ini, tidak cukup dengan agensi penguatkuasaan saja sebaliknya perlu juga kepekaan dan keprihatian pengguna itu sendiri," katanya.

Berdasarkan rekod, Siraj berkata, sebanyak 51,632 kes penipuan atas talian dilaporkan membabitkan jumlah kerugian lebih RM1.61 bilion daripada 2019 hingga 2021.

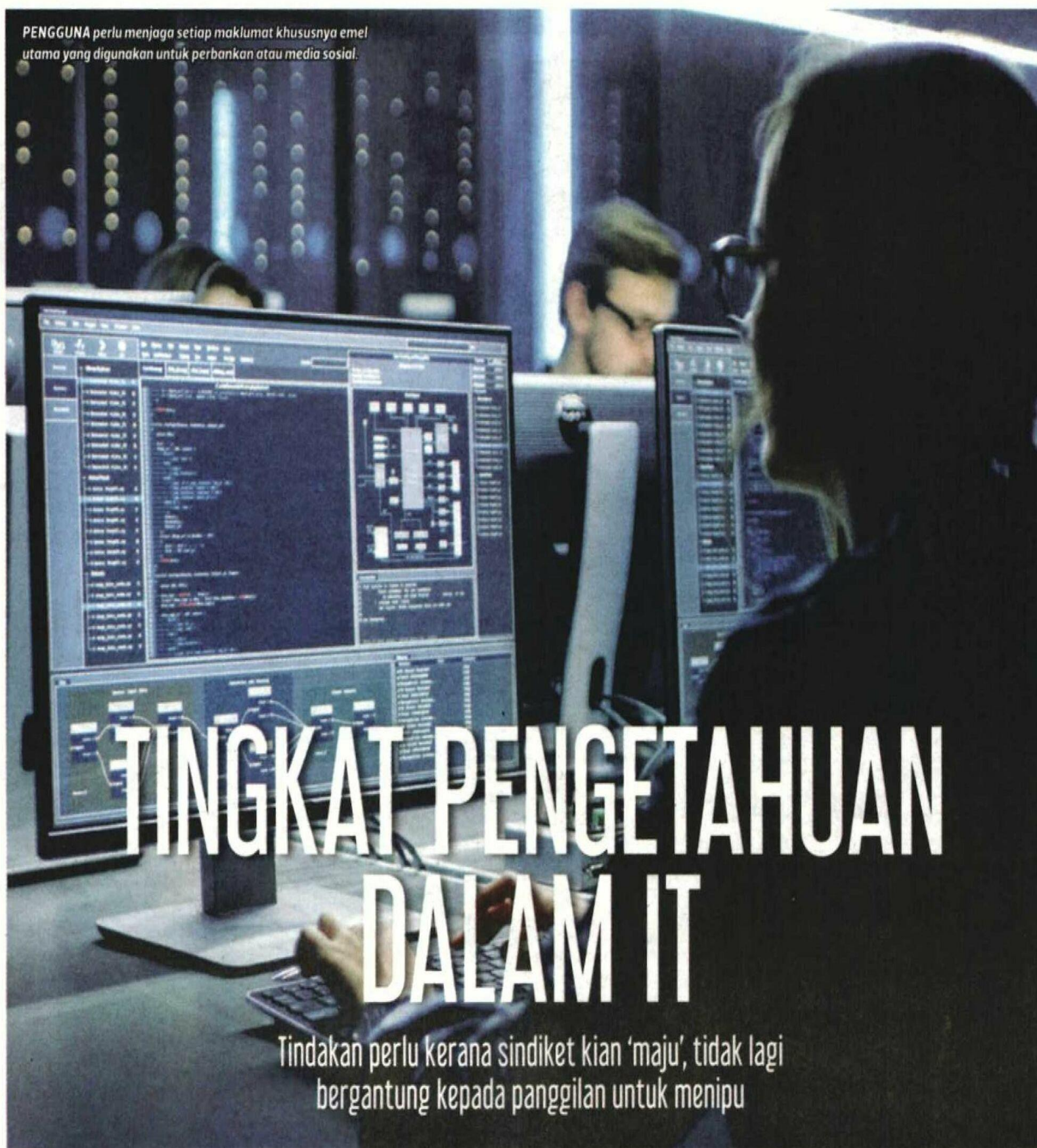
Beliau pada masa sama turut berkongsi empat tips keselamatan siber khusus untuk perhatian pengguna supaya dapat dipraktikkan dan mengurangkan risiko menjadi mangsa penipuan siber.

"Tips yang pertama adalah memasang antivirus berbayar di dalam telefon pintar atau laptop kegunaan harian untuk memastikan sebarang bentuk perisian hasad atau 'spyware' dapat dicegah diperingkat awal.

"Penggodam pada masa kini tidak hanya bergantung kepada panggilan telefon semata-mata malah sindiket penipuan ini sudah maju dengan mencipta perisian hasad untuk memantau sebarang aktiviti kita di telefon pintar.

"Walaupun kita

PENGUNA perlu menjaga setiap maklumat khususnya emel utama yang digunakan untuk perbankan atau media sosial.



TINGKAT PENGETAHUAN DALAM IT

Tindakan perlu kerana sindiket kian 'maju', tidak lagi bergantung kepada panggilan untuk menipu

terpaksa membayar sedikit untuk antivirus berkenaan asalkan dapat menyelamatkan aktiviti transaksi kita daripada kerugian kelak," katanya.

Beliau berkata, pengguna juga diingatkan supaya tidak menggunakan kata

laluan (password) yang sama dengan semua aplikasi kerana itu tindakan yang paling bahaya.

Menurutnya, jika penggodam dapat mengetahui kata laluan satu akaun media sosial dan kata laluan sama digunakan

untuk semua aplikasi termasuk perbankan Internet, ia memberi kesan paling buruk kepada pengguna.

"Selain itu, tips seterusnya adalah emel utama (primary email) pengguna khususnya untuk perbankan, kata laluan emel berkenaan perlu sukar untuk diteka oleh pihak ketiga.

"Psikologi manusia ini akan mencipta kata laluan yang berkaitan dengan dirinya iaitu tarikh lahir, nombor kad pengenalan, nombor kereta dan sebagainya sekali gus memberi laluan mudah kepada penggodam.

"Penggodam hari ini sangat licik dan mereka sudah melakukan 'kejuruteraan sosial' atau 'social engineering' untuk melihat latar belakang pengguna sekali gus dapat meneka kata laluan seseorang," katanya.

Siraj berkata, jika pengguna mempunyai

PENGODAM pada hari ini licik dengan mencipta perisian hasad dan spyware untuk memantau aktiviti pengguna di telefon pintar.



keupayaan serta kemampuan, langkah terbaik adalah mengasingkan nombor telefon khusus untuk tujuan 'One Time Password' (OTP) atau TAC, manakala nombor telefon lain digunakan untuk tujuan harian.

Katanya, pengguna juga jangan terlalu mendedahkan diri di laman sosial seperti melakukan rutin harian.

"Contohnya, rutin harian setiap pagi minum di kedai A dan setiap kali minum pagi kita kemaskini status di laman sosial, ini tidak bagus dan mendedahkan keselamatan kita.

"Lebih baik jangan berkongsi atau kurangkan berkongsi perkara-perkara peribadi yang membabitkan kehidupan harian," katanya.



PUSAT RESPONS SCAM KEBANGSAAN (NSRC)

Hubungi talian :

997

Waktu Operasi :
8.00 pagi - 8.00 malam
Setiap hari

Anda mangsa penipuan siber?
Hubungi bank anda atau NSRC dengan segera bagi menyekat pengeluaran wang anda.

Pastikan anda memberikan maklumat berikut ketika menghubungi NSRC :

- Insiden penipuan.
- Maklumat komunikasi dengan suspek.
- Maklumat transaksi yang berlaku.

KEWUJUDAN NSRC adalah inisiatif baik daripada kerajaan untuk mewujudkan satu tempat laporan bagi jenayah penipuan atas talian.