SCAM ALERT

DISEDIAKAN OLEH :

JABATAN SIASATAN JENAYAH KOMERSIL
POLIS DIRAJA MALAYSIA
KONTINJEN PULAU PINANG

TAHUKAH ANDA ?

BAHAWA KAMI PIHAK POLIS DIRAJA MALAYSIA (PDRM), KHUSUSNYA DARI JABATAN SIASATAN JENAYAH KOMERSIL (JSJK) PULAU PINANG GIAT DALAM MEMERANGI JENAYAH SIBER!

TERUSKAN PEMBACAAN BAGI MENGETAHUI

INFO LEBIH LANJUT!

JENAYAH SIBER?!

DISINI KAMI KONGSIKAN JENIS-JENIS JENAYAH SIBER, TREND-TREND TERKINI DAN TIPS SERTA NASIHAT

01 TIPU MENYAMAR KENALAN

02 TIPU NOMBOR TAC

03 TIPU SMS

04 TIPU PEMBELIAN DALAM TALIAN

“Berdasarkan perangkaan yang diperoleh, kes jenayah komersial mencatatkan peningkatan. Usaha pencegahan perlu dilaksanakan dengan lebih komprehensif bagi memastikan maklumat berkaitan jenayah komersial dapat disampaikan kepada masyarakat.”

----DARIPADA PENGARAH JABATAN SIASATAN JENAYAH KOMERSIL (JSJK) BUKIT AMAN, DATUK MOHD KAMARUDIN MD DIN----

05 LOVE SCAM

06 PENYAMARAN TIPU PANGGILAN

07 PINJAMAN TIDAK WUJUD

08 TIPU PELABURAN

JENAYAH SIBER?!

DISINI KAMI KONGSIKAN JENIS-JENIS JENAYAH SIBER, TREND-TREND TERKINI DAN TIPS SERTA NASIHAT

“ Sikap tidak kisah dan tidak mahu ambil tahu akan memakan diri anda apabila anda menjadi mangsa sindiket penipuan ”

----DARIPADA KETUA JABATAN SIASATAN JENAYAH KOMERSIL (JSJK) KONTINJEN PULAU PINANG, MOHD ASMADI BIN YUSUFF

JENAYAH SIBER?!

DISINI KAMI KONGSIKAN JENIS-JENIS JENAYAH SIBER, TREND-TREND TERKINI DAN TIPS SERTA NASIHAT

09 PHISHING

10 KELDAI AKAUN

11 BUSINESS EMAIL COMPROMISE

JANGAN TAKUT

"Ketakutan membantu penjenayah. Sentiasa membuat semakan dengan pihak berkuasa atau ahli keluarga sekiranya anda tidak pasti"

01

TIPU MENYAMAR KENALAN

Satu penipuan yang menggunakan pelbagai media sosial seperti Facebook, Whatsapp, Telegram, dll, dimana saspek menyamar sebagai kenalan dan memohon bantuan dari mangsa.

INGAT! siapa-siapa boleh

MENYAMAR

dalam talian

"TIDAK KENAL JANGAN LAYAN"

JSJK PENANG

MODUS OPERANDI

Man, ingat lagi tak ? Azroy ni...
kawan sekolah kat kampung dulu.

Mak aku baru lepas operation, sekarang kat hospital ada masaalah sikit...
kekurangan duit nak bayar kos rawatan...

suspek menghubungi mangsa melalui telefon atau lain-lain media sosial

suspek menyamar sebagai kenalan (ahli keluarga/rakan lama)

suspek meminta untuk meminjam duit daripada mangsa dengan pelbagai alasan seperti berikut :-

- Untuk tujuan perniagaan
- Telah diragut dan memerlukan wang untuk perbelanjaan
- Membayar bil rawatan atau membeli barang keperluan

TIPS & NASIHAT

- JANGAN LAYAN nombor yang tidak dikenali.
- HUBUNGI rakan / ahli keluarga di nombor asal untuk pengesahan
- SEMAK nombor telefon dan akaun bank di SEMAKMULE sebelum membuat transaksi

02

TIPU NOMBOR TAC

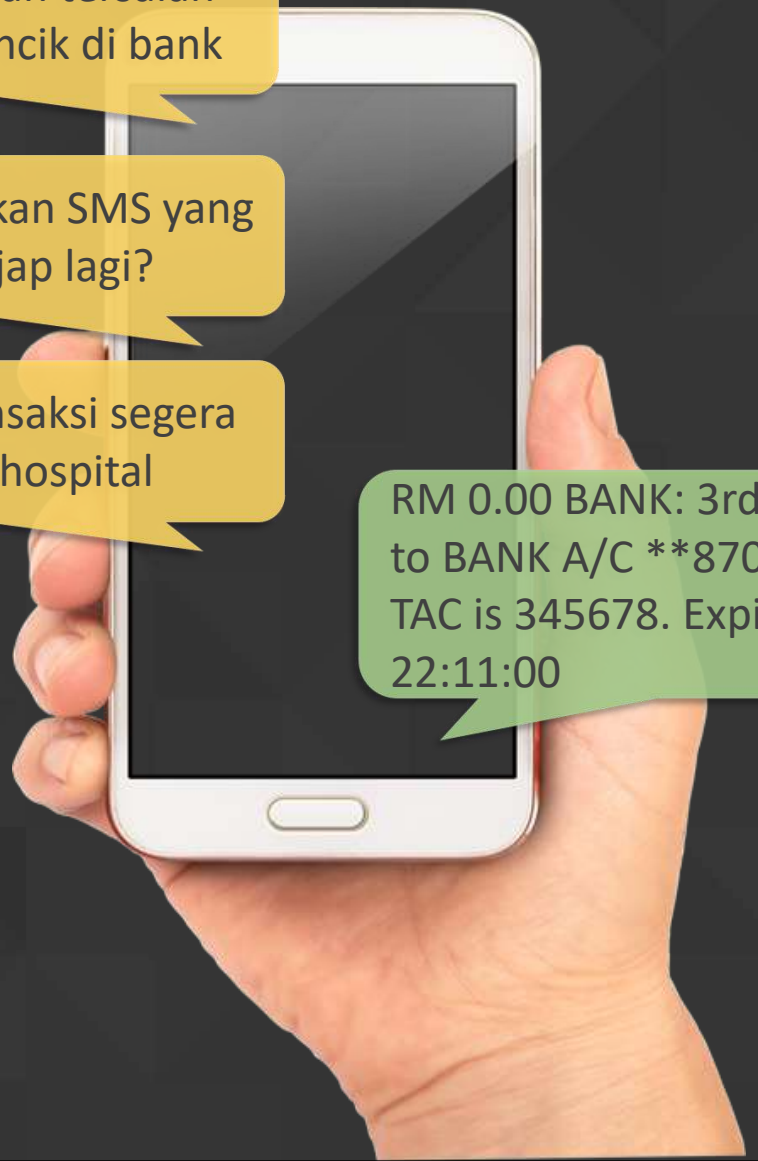
Satu jenis penipuan oleh saspek bagi mendapatkan nombor TAC daripada mangsa dengan pelbagai cara.

TIPS & NASIHAT

Maaf. Isteri saya telah tersalah daftar no. telefon encik di bank

Boleh encik forwardkan SMS yang encik terima kejap lagi?

Saya perlu buat transaksi segera untuk bayar bil hospital



JANGAN

Jangan kongsi nombor keselamatan bank / nombor TAC kepada mana-mana indvidu

ABAIKAN

Abaikan SMS atau Whatsapp dari orang yang tidak dikenali

HUBUNGI

Hubungi segera pihak bank untuk menyekat perbankan internet

03

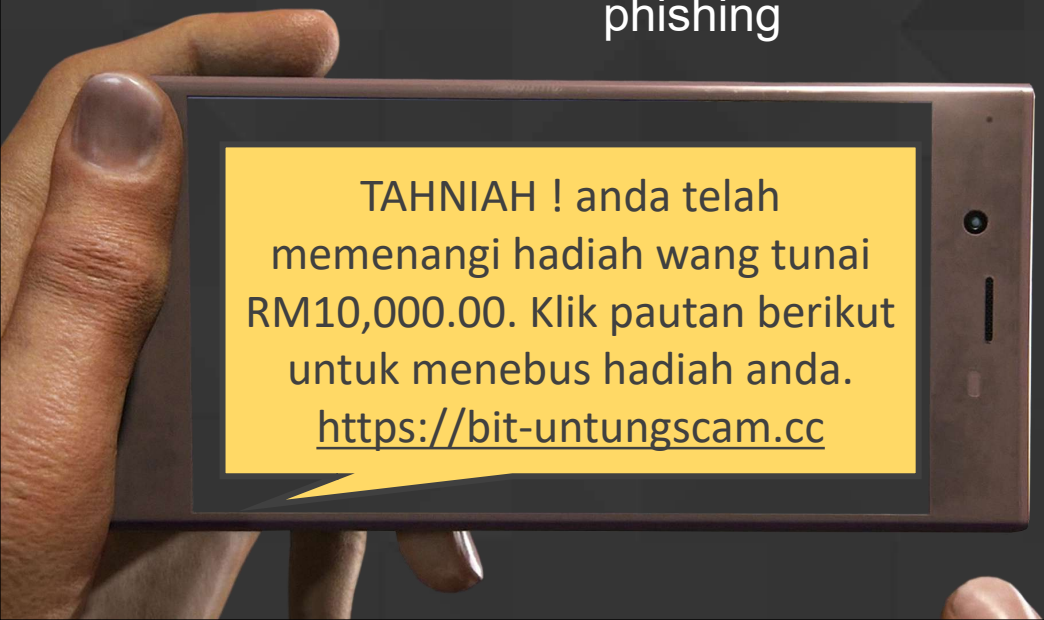
TIPU SMS

Penipuan dimana mangsa menerima SMS telah memenangi hadiah peraduan atau menerima SMS daripada mana-mana pihak yang akan membuatkan mangsa klik pautan web yang diberi.

MODUS OPERANDI

Menang Peraduan

- Mangsa menerima SMS telah memenangi hadiah peraduan.
- Mangsa diminta menekan pautan pada SMS dan mengisi maklumat perbankan yang sebenarnya merupakan laman web phishing



Penggunaan kad Kredit

- Mangsa menerima SMS tentang penggunaan kad kredit
- Mangsa telah menghubungi nombor telefon pada SMS tersebut dan telah memberikan maklumat perbankan kepada suspek

TIPS & NASIHAT

JANGAN TEKAN

Jangan tekan pautan pada SMS dari pihak yang tidak dikenali.

SEMAK

Semak nombor telefon bank di laman web atau di belakang kad ATM / Kredit.

04

TIPU PEMBELIAN DALAM TALIAN

Kaedah penipuan paling mudah / banyak berlaku dimana mangsa akan terpedaya oleh suspek dengan tawaran iklan jualan di media-media sosial dengan harga lebih murah dari pasaran.

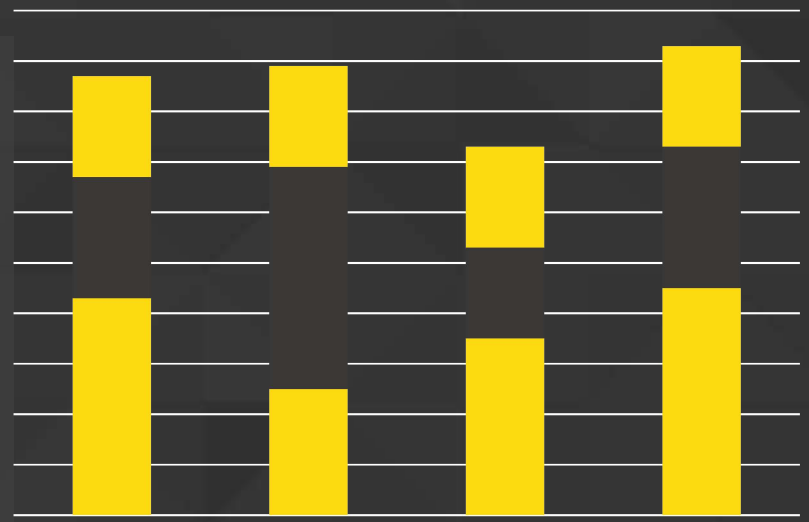
MODUS OPERANDI

Mangsa adalah PEMBELI

- Mangsa melihat iklan jualan di media sosial.
- suspek menawarkan harga jauh lebih murah dari pasaran.
- Mangsa diminta membuat pembayaran segera ke akaun bank yang diberikan suspek.
- Mangsa tidak menerima barang dan gagal menghubungi suspek.

Mangsa adalah PENJUAL

- Suspek menghubungi mangsa dan berminat dengan barang jualan mangsa
- Suspek an meminta mangsa (penjual) membuat pembayaran terlebih dahulu bagi urusan pemindahan wang dari akaun luar negara ke akaun tempatan.



Tips & Nasihat

- BERHATI-HATI dengan tawaran murah atau 'too good to be true'
- Beli dari laman web yang DIPERCAYAI dan mempunyai ciri KESELAMATAN
- Semak ulasan dan maklum balas pembeli lain
- Semak akaun bank atau nombor telefon di laman SEMAKMULE sebelum membuat transaksi

67,552 KES

Rekod PDRM untuk kes penipuan siber sejak 2017 sehingga 2021.

RM 2.23 B

Rekod kerugian dilaporkan dalam penipuan atas talian sejak 2017 sehingga 2021

05

LOVE SCAM

Penipuan cinta atau Love Scam adalah modus operandi yang kerap digunakan sindiket penipuan didalangi warga Afrika untuk memperdaya mangsa berbanding sindiket penipuan lain. Penipuan menggunakan modus operandi ini paling kerap digunakan kerana ‘kaedah’ itu dipercayai amat berkesan untuk memerangkap dan memperdaya mangsa.

MODUS OPERANDI

Hi honey, how do u do today? hope u have a good day today..

act hun.. i have a problem.. quite big problem.. my company i am working now having a problem.. so...

- ✓ Mangsa berkenalan dengan suspek di media sosial.
- ✓ Suspek menyamar menjadi askar, ahli perniagaan, jurutera oil & gas atau juruterbang dari luar negara.
- ✓ Antara taktik yang digunakan suspek adalah :-

Pemberian Hadiah

- ❖ Suspek ingin memberi hadiah mewah dari luar negara kepada mangsa sebagai tanda persahabatan
- ❖ Mangsa kemudian diminta membuat pelbagai bayaran (cukai, denda, proses dll) untuk menuntut barangan tersebut kononnya telah ditahan.

Pelaburan / wasiat

- ❖ Suspek akan meminta bantuan mangsa untuk membuat pelbagai bayaran kepada pihak lain bagi tujuan perniagaan atau mendapatkan wang pusaka di Malaysia.

TIPS & NASIHAT

01

JANGAN LAYAN

Jangan layan individu yang tidak dikenali di media sosial

02

JANGAN MUDAH PERCAYA

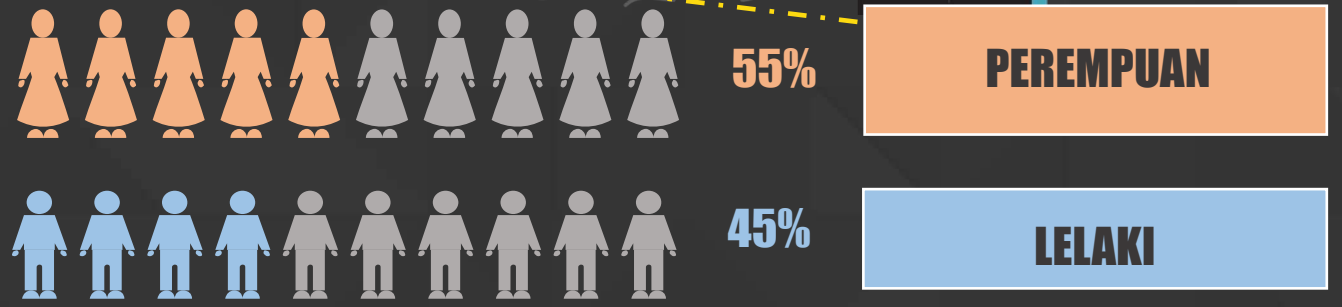
Jangan mudah percaya kepada kenalan di media sosial

03

SEMAK

Semak dengan pihak berkaitan sebelum membuat transaksi

INFO GRAFIK



06

PENYAMARAN TIPU PANGGILAN

Sindiket penipuan yang dipanggil Macau Scam didalangi oleh penduduk tempatan dan warga asing yang cuba memperdaya mangsa mereka dengan membuat panggilan mengatakan bahawa mereka daripada institusi kewangan.

Ia biasanya dilakukan menggunakan talian antarabangsa dari lokasi seperti China, Taiwan, Hong Kong dan ada juga dari dalam negara. Nama Macau Scam, tapi sebenarnya ada juga yang berpangkalan di Malaysia.

MODUS OPERANDI

Suspek menghubungi mangsa dengan menyamar sebagai :-

Mangsa dikatakan terlibat dengan kes jenayah atau mempunyai tunggakan bayaran cukai, pinjaman bank dll.

Mangsa diugut akan ditangkap dan didakwa. Mangsa dilarang daripada memberitahu kepada sesiapa.

Suspek akan meminta mangsa menyerahkan maklumat perbankan atau memindahkan wang ke akaun bank yang tidak dikenali bagi tujuan siasatan.

TIPS / NASIHAT

- JANGAN LAYAN panggilan telefon tidak dikenali.
- BERITAHU pasangan, rakan atau ahli keluarga tentang panggilan yang diterima.
- SEMAK dengan balai, bank atau agensi berkaitan untuk pengesahan
- JANGAN DEDAH maklumat perbankan kepada mana-mana pihak.

07

PINJAMAN TIDAK WUJUD

Satu sindiket penipuan yang menawarkan tawaran pinjaman secara mudah dan cepat kepada mangsa

TIPS / NASIHAT

- Ahlong adalah pemberi pinjam wang TANPA LESEN dan merupakan penjenayah.
- Jangan jadikan diri dan keluarga menjadi mangsa UGUTAN ahlong
- Pemberi pinjam wang berlesen hanya boleh berurusan di alamat operasi / pejabat yang diluluskan sahaja.
- Pemberi pinjam wang berlesen perlu mempamerkan lesen di tempat mudah dilihat di dalam premis

MODUS OPERANDI

Mangsa perlu mebayar bunga / faedah setiap minggu sehingga boleh membayar jumlah pinjaman sekaligus walaupun faedah yang dibayar melebihi jumlah pinjaman.

Menawarkan iklan pinjaman wang melalui media sosial, SMS atau poster.

Menjalankan urusan tanpa lesen dari Kementerian Perumahan dan Kerajaan Tempatan.

Menawarkan pinjaman yang mudah, cepat serta tanpa penjamin.

Kadar faedah yang tinggi dan terma pinjaman yang berubah-ubah.

Mangsa yang gagal atau lewat membuat bayaran akan diugut dan diancam.

Mangsa ditekan untuk membuat pinjaman dengan Ahlong lain untuk menyelesaikan hutang.

08

TIPU PELABURAN

Sindiket penipuan ini menawarkan skim-skim pelaburan tidak wujud yang mudah, modal kecil tetapi untung besar, tiada risiko dan tidak akan rugi bagi menarik mangsa-mangsa yang mudah terpedaya.

Trend-trend terkini menggunakan pelaburan jenis Bitcoin, Ethereum, NFT dll bagi menarik perhatian mangsa.

MODUS OPERANDI

1

Mangsa melihat iklan pelaburan di media sosial, melalui whatsapp atau melalui kenalan

2

Mangsa ditawarkan pelaburan yang :

1 unit RM200

,000.00

2 00%

mgu shj

- Mudah dan untung besar!
- Keuntungan berganda!
- Tiada risiko dan tidak rugi!

3

Mangsa akan menerima keuntungan pada 1 hingga 3 bulan pertama.

4

Mangsa kemudian gagal mendapatkan keuntungan yang dijanjikan dan wang kapital akan dilaburkan.

5

Suspek gagal dihubungi

TIPS / NASIHAT

1

JANGAN PERCAYA pada pelaburan dalam talian atau pelaburan yang ditawarkan oleh rakan.

2

SEMAK senarai syarikat dan laman sesawang yang tidak diberi kebenaran atau kelulusan di :-

BANK NEGARA MALAYSIA
www.bnm.gov.my
1-300-88-5465
(BNMTELELINK)

Suruhanjaya Sekuriti Malaysia
www.sc.com.my

3

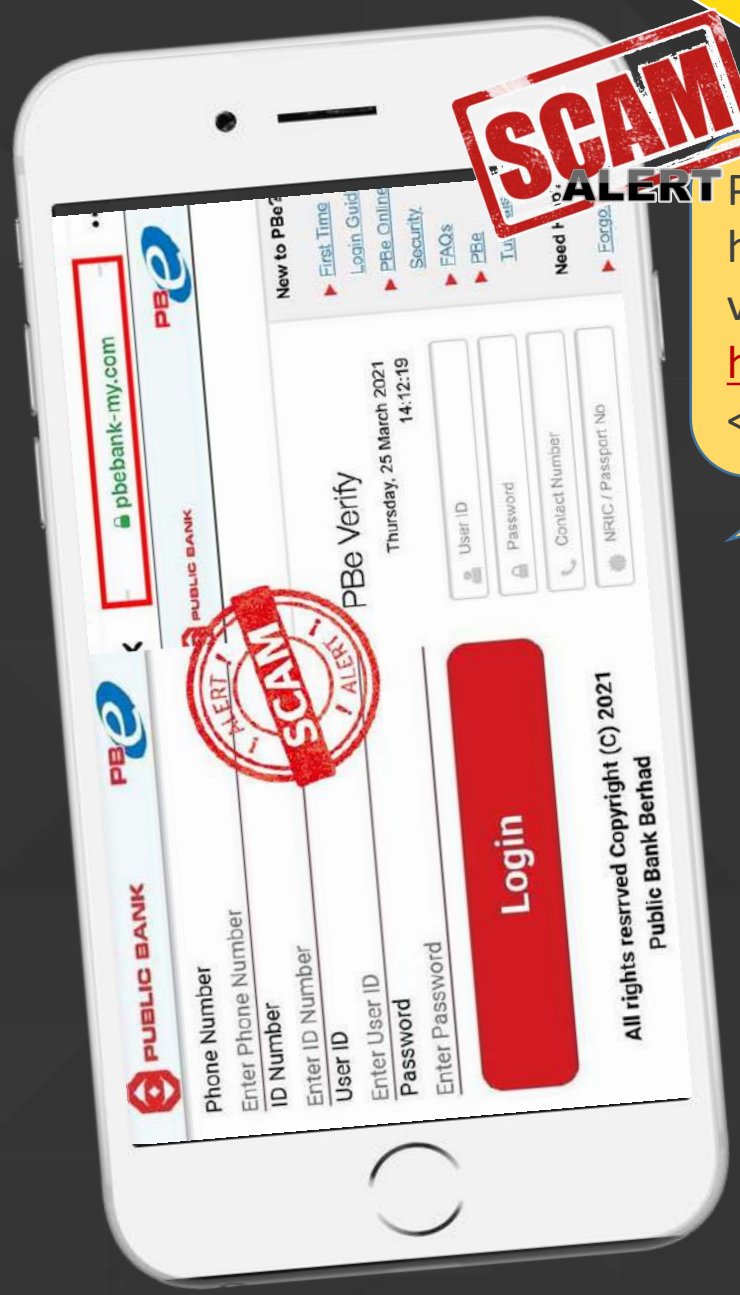
Semak akaun bank di laman **SEMAKMULE** sebelum membuat transaksi.

09

PHISHING

Merupakan kaedah mendapatkan maklumat perbankan orang lain melalui laman web palsu yang menyerupai laman web asal.

MODUS OPERANDI



PBB: Your account is judged as high risk by the system. PLS re-verify your account https://www.pbebanks.asia/ <security reminder is normal>

- Mangsa menerima SMS untuk mengemaskini maklumat perbankan internet dan diminta untuk menekan pautan pada SMS tersebut.
- Mangsa kemudian memasukkan maklumat perbankan seperti ID pengguna, kata laluan, nor kad ATM dll di dalam laman web phishing.
- Mangsa kemudian diminta menyerahkan nombor TAC kepada pihak bank yang menghubungi mangsa
- Suspek kemudian memindahkan wang dari akaun mangsa ke akaun keldai.

TIPS / NASIHAT

- **JANGAN TEKAN** pautan pada SMS dari nombor tidak dikenali.
- **SEMAK** laman web yang betul sebelum mengisi sebarang maklumat
- **JANGAN BERI** maklumat perbankan kepada mana-mana pihak.

10

KELDAI AKAUN

Individu yang menterahkan kad ATM serta nombor pin kepada individu lain dan akaun bank tersebut digunakan bagi tujuan jenayah.

MODUS OPERANDI

Sindiket meminta keldai akaun membuka beberapa akaun bank untuk disewa / dijual dengan alasan untuk urusan perniagaan / cuci duit judi dalam talian.

Terdapat beberapa cara digunakan sindiket untuk mendapatkan keldai akaun. Antaranya :

1

Sewa / Beli

Keldai akaun melihat tawaran iklan di media sosial yang menawarkan sewaan atau pembelian akaun bank.

Keldai akaun ditawarkan sebanyak RM100 hingga RM3,000 secara bulanan.

2

Pinjaman Ahlong

Keldai akaun yang ingin meminjam wang dari Ahlong diminta menyerahkan kad ATM sebagai cagaran.

Ahlong kemudian menjual kad tersebut kepada sindiket untuk digunakan bagi tujuan jenayah.

MODUS OPERANDI

3

Tawaran Kerja

Tawaran kerja oleh sindiket di media sosial atau media cetak.

Keldai akaun kononnya telah diterima bekerja dan diminta membuka akaun bank serta menyerahkan kad ATM untuk proses pembayaran gaji.

4

Beri Pinjam

Keldai akaun memberi pinjam kepada rakan yang baru dikenali di media sosial.

TIPS / NASIHAT

!! KELDAI AKAUN BOLEH DIDAKWA!!

JANGAN BERI

Jangan beri kad ATM atau akaun bank kepada mana-mana pihak untuk digunakan.

01

TANGGUNGJAWAB

Kad ATM dan akaun bank adalah tanggungjawab setiap pemilik.

02

BATALKAN

Batalkan kad ATM segera jika kehilangan kad.

03

SEMAK PENYATA

Semak penyata akaun dengan kerap. Semak dengan phak bank jika terdapat kemasukkan / pengeluaran wang yang mencurigakan.

04

10

BUSINESS EMAIL COMPROMISE

Penipuan ini menyasarkan penggodaman / memintas rangkaian emel dengan memperdaya mangsa membuat bayaran ke akaun diberi oleh suspek.

MODUS OPERANDI

'A'

'A' dan 'B' merupakan rakan niaga dan saling berhubung melalui emel.

'A" terima emel daripada 'B' tentang pertukaran akaun bank syarikat 'B'

'B

'A' tidak menyedari bahawa alamat emel yang asal dengan alamat emel yang dihantar oleh suspek adalah berbeza.

SUSPEK

Emel asal :
tech-orb@tech.com.my
Emel suspek :
tech-Orb@tech.cc

- ✓ 'A' membuat bayaran ke akaun bank yang diberikan suspek
- ✓ Mangsa tersedar telah ditipu apabila rakan niaga menghubungi mangsa memaklumkan belum menerima bayaran.

TIPS / NASIHAT

- ➢ **JANGAN TEKAN** pautan di dalam emel yang diterima dari pihak tidak dikenali.
- ➢ **SEMAK** alamat emel dengan teliti.
- ➢ **HUBUNGI** rakan niaga melalui telefon untuk pengesahan pertukaran akaun.
- ➢ Pastikan komputer di pejabat memasang dan mengemaskini **ANTIVIRUS** bagi mengelak serangan **MALWARE**.

DIREKTORI

Pastikan anda mengikuti perkembangan-perkembangan semasa berkaitan isu-isu jenayah komersil secara rasmi melalui laman-laman dan pautan yang tertera di bawah.
Sekiranya anda memiliki sebarang permasalahan / persoalan berkenaan jenayah komersil, anda dialu-alukan untuk menghubungi kami di talian seperti berikut :-

ALAMAT

JABATAN SIASATAN JENAYAH KOMERSIL
IBU PEJABAT POLIS KONTINJEN
POLIS DIRAJA MALAYSIA
PULAU PINANG
JALAN PENANG, GEORGETOWN, 10760.
PULAU PINANG
04-2221522

FACEBOOK

@JSJKPENANG
@JSJKPDRM
@CyberCrimeAlertRMP

- Menyampaikan maklumat kepada orang awam tentang modus operandi jenayah komersil dan siber yang terkini di Penang.

SEMAKMULE

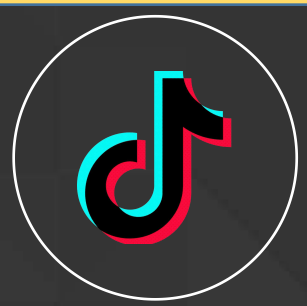
website:
https://ccid.rmp.gov.my/semakmule/

Google Play Store:
Check Scammers CCID

- Semak nombor akaun bank dan nombor telefon yang terlibat kes jenayah komersil

DIREKTORI

Pastikan anda mengikuti perkembangan-perkembangan semasa berkaitan isu-isu jenayah komersil secara rasmi melalui laman-laman dan pautan yang tertera di bawah.
Sekiranya anda memiliki sebarang permasalahan / persoalan berkenaan jenayah komersil, anda dialu-alukan untuk menghubungi kami di talian seperti berikut :-



TIKTOK

JSJK PENANG

- Memaparkan video-video trend jenayah siber terkini di Penang.

CCID SCAM RESPONSE CENTER

03-26101559
03-26101599

Waktu operasi:0800-2000Hrs

- Pertanyaan Modus Operandi kes tipu dalam talian
- Mangsa tipu dalam talian boleh menyalurkan maklumat transaksi pindahan wang.

CCID INFOLINE

013-2111222

Waktu operasi:0800-0000Hrs

- Semak laporan polis
- Semak status siasatan
- Menyalur maklumat kes-kes jenayah komersil

PUSAT RESPONS SCAM KEBANGSAAN (NSRC)

Apakah itu PUSAT RESPONS SCAM NEGARA (NSRC)?

PUSAT RESPONS SCAM NEGARA(NSRC) ialah pusat operasi untuk menyelaraskan tindak balas terhadap penipuan kewangan dalam talian termasuk pengesanan dana yang dicuri secara lebih cepat dan tindakan penguatkuasaan terhadap penjenayah.

Apakah jenis kes penipuan yang dikendalikan oleh NSRC?

Semua jenis penipuan secara atas talian di mana mangsa menyedari bahawa akaun bank mereka telah dipindahkan tanpa disedari atau mangsa telah diperdaya ntuk memindahkan wang secara atas talian.

Bagaimana NSRC membantu mangsa?

Selepas mendapat laporan, NSRC akan menyelaraskan tindak balas pantas oleh penguatkuasaan undang-undang, institusi kewangan dan syarikat perkhidmatan komunikasi bagi membantu mencegah mangsa daripada menghadapi kerugian lebih banyak, berusaha mengesan dana yang telah dicuri dan menjalankan siasatan terhadap jenayah penipuan tersebut serta mengenakan tindakan penguatkuasaan terhadap penjenayah.

Saya telah ditipu. Apakah patut saya lakukan?

Segera hubungi Hotline bank operasi anda atau hubungi hotline NSRC iaitu 997(0800-2000hrs/setiap hari). Tindakan ini boleh membantu anda mengurangkan kerugian yang mungkin dialami, walaupun tiada jaminan bahawa anda akan mendapat semula wang anda.

Apakah maklumat diperlukan untuk saya buat laporan?

Penerangan ringkas insiden, Butiran peribadi, Butiran penjenayah,Butiran transaksi

Dengan kewujudan NSRC, adakah saya masih perlu membuat laporan polis?

Ya, bagi membolehkan pihak polis memulakan siasatan rasmi. bagi memastikan tindakan segera diambil, hubungi bank operasi anda atau Hotline 997 terlebih dahulu sebelum membuat laporan di balai polis berdekatan.

disediakan oleh :

JABATAN SIASATAN JENAYAH KOMERSIL KONTINJEN PULAU PINANG

#JSJKPENANG

#ScamAlert
#BeSmartStayAlert
#JanganKataTakTahuKenalahAmbilTahu!