Disediakan oleh
Jabatan Siasatan Jenayah Komersial
Polis Diraja Malaysia

Dengan Kerjasama

celcomdigi whoscall

Trend Terkini
Jenayah Komersil

Dikemaskini pada Disember 2022

ISI KANDUNGAN

BIL	ISI KANDUNGAN	MUKA SURAT
1.	Keldai Akaun	1 - 4
2.	Macau Scam	5 - 9
3.	Love Scam	10 - 12
4.	Jenayah E-Dagang	13 - 16
5.	Phishing	17 - 22
6.	Business Email Compromise (BEC)	23 - 25
7.	Tipu Nombor TAC	26 - 27
8.	Pinjaman Tidak Wujud (PTW)	28 - 29
9.	Tipu Pelaburan	30 - 32

KELDAI AKAUN

KELDAI AKAUN

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

Bagaimana seseorang itu boleh menjadi keldai akaun?

1. SERAH / BERI PINJAM

Pemilik akaun menyerahkan kad ATM dan nombor pin kepada **rakan, kenalan dalam talian atau Ahlong** untuk digunakan tanpa pemantauan pemilik akaun sendiri.

2. JUAL / SEWA

Pemilik akaun menjual atau menyewa kad ATM dan nombor pin kepada pihak lain dan menerima bayaran.

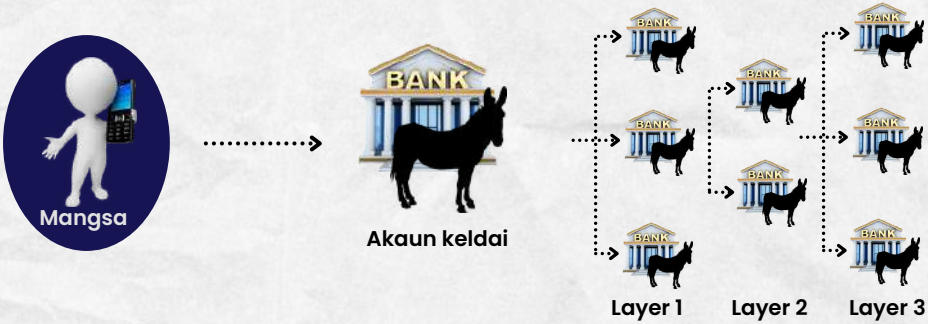
3. TAWARAN KERJA

Pemilik akaun ditawarkan pekerjaan untuk membuat transaksi wang dari akaun persendirian ke akaun pihak ketiga dan dibayar komisen.

KELDAI AKAUN BOLEH DITANGKAP DAN DIDAKWA !

Apa itu 'LAYERING' AKAUN BANK ?

Kaedah pindahan wang secara berperingkat yang digunakan sindiket penipuan bagi melambatkan proses mengesan wang mangsa.



- Mangsa memindahkan wang ke akaun keldai (*layer* 1) yang diberikan suspek / sindiket.
- Wang dari akaun keldai *layer* 1 akan segera dipindahkan ke beberapa *layer* akaun keldai yang lain oleh sindiket pindahan wang bagi menyukarkan wang tersebut dikesan.
- Wang hasil penipuan tersebut kemudian akan dikeluarkan oleh sindiket pengeluaran wang bagi menghapuskan jejak wang dari sistem perbankan.

Tahukah anda

Dalam tempoh kurang dari 5 minit, wang mangsa penipuan boleh dipindahkan ke dua peringkat (layer) akaun keldai dengan menggunakan perkhidmatan perbankan internet.

PEMILIK AKAUN KELDAI
BOLEH DIDAKWA
DI BAWAH UNDANG-UNDANG MALAYSIA

SEKSYEN 109 KANUN KESEKSAAN
Menyubahati sesuatu perkara

SEKSYEN 411 KANUN KESEKSAAN
Menerima harta dengan curang

SEKSYEN 424 KANUN KESEKSAAN
Mengalih atau menyembunyikan harta dengan curangnya dengan tipuan.

SEKSYEN 420 KANUN KESEKSAAN
Menipu dengan curangnya mendorong supaya harta diserahkan.

SEKSYEN 120B KANUN KESEKSAAN
Pakatjahat jenayah.

SEKSYEN 4(1) AMLATFPUAA 2001
Kesalahan penggubahan wang haram.

SEKSYEN 137 AKTA PERKHIDMATAN KEWANGAN
Larangan menerima deposit.


Saya dari LHDN. Awak ada bayaran cukai tertunggak.
Saya polis. Awak terlibat dengan jenayah dan akan ditangkap.
Saya dari mahkamah. Ada waran tangkap atas nama kamu.
Siapa saya sebenarnya ?

MACAU SCAM

MACAU SCAM
(Penyamaran Tipu Panggilan)

~ MODUS OPERANDI ~

Suspek menghubungi mangsa dengan menyamar sebagai penguatkuasa, institusi kewangan atau syarikat perkhidmatan.

- Polis
- LHDN
- SPRM
- Bank
- Syarikat Kurier
- BigPay
- TM
- Kastam
- Mahkamah

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.

~ TIP & NASIHAT ~

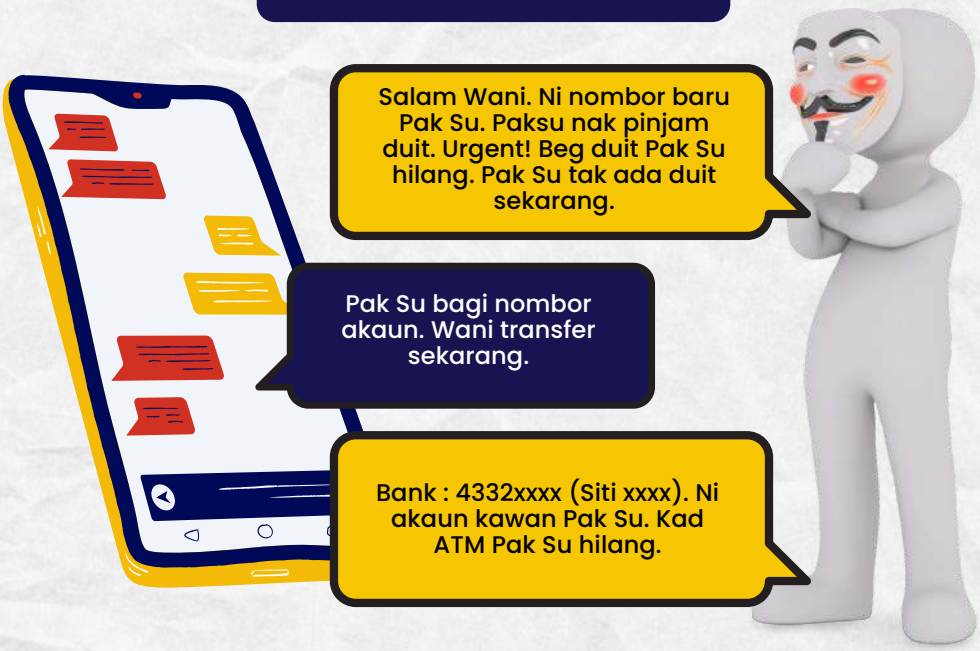
JANGAN LAYAN panggilan telefon yang tidak dikenali.

SEMAK dengan balai, bank atau agensi berkaitan untuk pengesahan.

BERITAHU pasangan, rakan atau ahli keluarga tentang panggilan yang diterima.

MACAU SCAM

MENYAMAR KENALAN



- Suspek menghubungi mangsa melalui telefon atau media sosial , whatsapp atau Telegram.
- Suspek menyamar sebagai kenalan (ahli keluarga/ rakan lama).
- Suspek meminta untuk meminjam duit daripada mangsa dengan pelabagai alasan seperti berikut :-

  - untuk tujuan perniagaan.
  - telah diragut dan memerlukan wang untuk perbelanjaan.
  - membayar bil rawatan atau membeli barang keperluan.

MACAU SCAM

~ TREND SEMASA ~

1 BUKA AKAUN BANK BARU

- Mangsa diminta membuka akaun bank baru dengan mendaftarkan no. telefon yang diberikan suspek.
- Mangsa diarahkan menyerahkan maklumat perbankan seperti no. kad ATM dan no. pin.
- Mangsa diarahkan memindahkan semua wang simpanan dari akaun lain ke akaun yang baru dibuka.

→ Membolehkan suspek daftar dan akses ke perbankan internet akaun mangsa serta mendapat no. TAC tanpa pengetahuan mangsa.

2 MENYERAHKAN KAD ATM

- Mangsa diarahkan meninggalkan kad ATM milik mangsa di lokasi-lokasi tertentu yang tidak mempunyai CCTV.

→ Akaun bank mangsa juga boleh digunakan sindiket sebagai akaun keldai.

~ TIP & NASIHAT ~

Jangan serah maklumat perbankan anda kepada mana-mana pihak.

MACAU SCAM

BAGAIMANA MANGSA BOLEH TERPEDAYA ?

Suspek akan menakutkan mangsa dengan cara ugutan dan menakut-nakutkan mangsa:

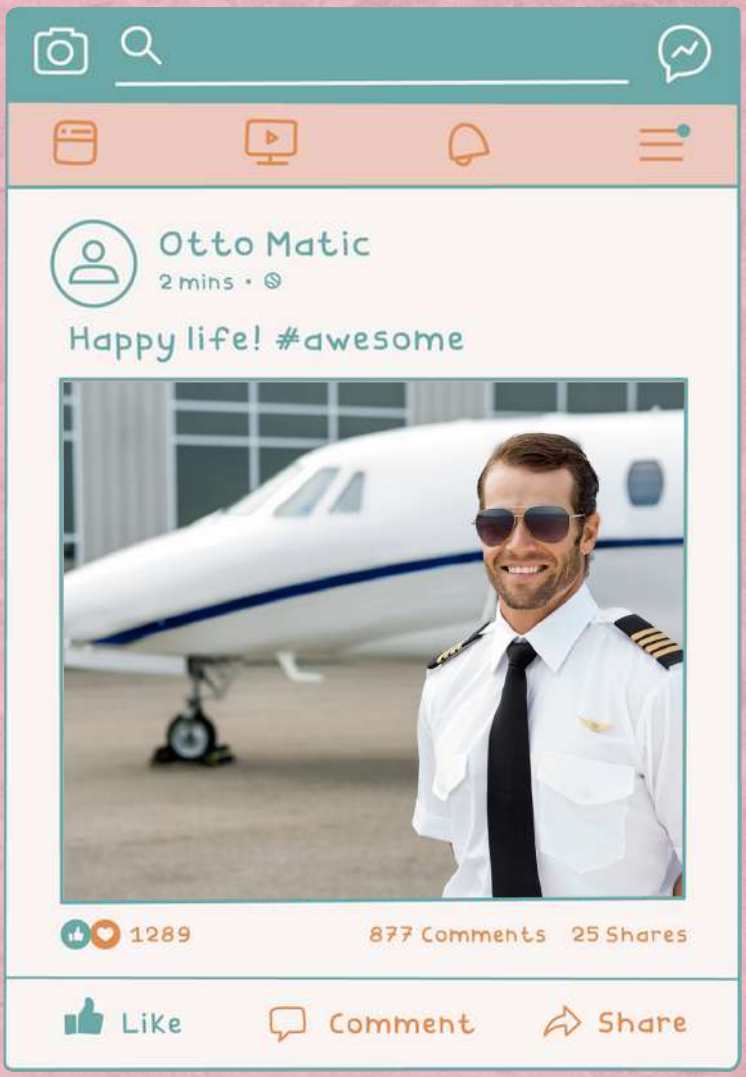
SIAPA YANG MUDAH MENJADI MANGSA ?


Mudah cemas


Mudah takut


Tidak berkongsi masalah


Tidak mengikuti isu jenayah semasa


Otto Matic
2 mins
Happy life! #awesome
1289
877 Comments
25 Shares
Like
Comment
Share

LOVE SCAM

LOVE SCAM

~ MODUS OPERANDI ~

1. Berkenalan

2. Minta bayaran

1. Berkenalan

- Mangsa berkenalan dengan suspek melalui media sosial.
- Suspek akan menyamar sebagai juruterbang, peniaga, tentera atau jurutera *oil & gas.*
- Suspek akan menggunakan kata-kata manis sehinga mangsa jatuh cinta.
- Suspek kemudian memperdaya mangsa dengan alasan-alasan berikut :
  - Beri hadiah
  - Pelaburan perniagaan
  - Wasiat
  - Bayaran bil hospital

2. Minta bayaran

- Mangsa kemudian dihubungi oleh pihak ketiga yang menyamar sebagai syarikat kurier, kastam atau peguam meminta bayaran dari mangsa bagi mendapatkan bungkusan / harta yang dijanjikan suspek.

LOVE SCAM

~ TIP & NASIHAT ~

- JANGAN LAYAN individu yang tidak dikenali di media sosial.
- Jangan MUDAH PERCAYA kepada kenalan di media sosial.
- SEMAK dengan pihak/agensi berkaitan sebelum membuat transaksi.
- JANGAN PERCAYA tawaran 'too good to be true'.

SIAPA YANG MUDAH MENJADI MANGSA ?

Individu yang tamak.

Individu yang kesunyian.

JENAYAH E-DAGANG

JENAYAH E-DAGANG

~ MODUS OPERANDI ~

MANGSA SEBAGAI PEMBELI

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

MANGSA SEBAGAI PENJUAL

- Suspek menghubungi mangsa dan berminat dengan barang jualan mangsa.
- Suspek kononnya telah tersalah memasukkan amaun dan meminta mangsa memulangkan semula baki wang.
- Suspek menunjukkan resit transaksi palsu.
- Suspek turut mengugut akan membuat laporan polis jika mangsa enggan memulangkan wang baki.

JENAYAH E-DAGANG

~ TIP & NASIHAT ~

1. BERHATI-HATI dengan tawaran murah atau 'too good to be true'.

2. Beli dari laman web yang DIPERCAYAI dan mempunyai ciri KESELAMATAN.

3. Semak ulasan dan maklum balas pembeli lain.

4. Semak akaun bank atau nombor telefon di laman SEMAKMULE sebelum membuat transaksi.

5. Jangan berurusan di luar platform atau 'PM' tepi.

SEMAKMULE CCID

Download on Google Play

semakmule.rmp.gov.my

JENAYAH E-DAGANG

~ TREND SEMASA ~

1 KERETA RECON LUAR NEGARA

- Melihat iklan di media sosial.
- Berurusan hanya dalam talian.
- Diminta membuat bayaran pengangkutan, kastam, upah dll.

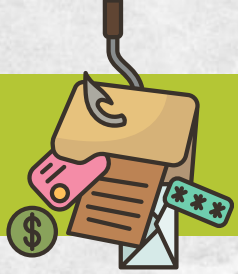
2 TAWARAN KERJA

- Ditawarkan kerja dalam talian.
- Perlu menyelesaikan tugasan yang diberikan dalam tempoh ditetapkan.
- Mangsa perlu membuat bayaran dahulu sebelum terima komisen.
- Mangsa hanya terima komisen untuk tugasan pertama dan kedua.

3 EMAS

- Melihat iklan di media sosial.
- Berurusan hanya dalam talian.
- Diminta membuat bayaran ke akaun keldai.

PHISHING



PHISHING

Kaedah mendapatkan maklumat peribadi seperti perbankan orang lain melalui laman web palsu yang menyerupai laman web asal.

~ MODUS OPERANDI ~

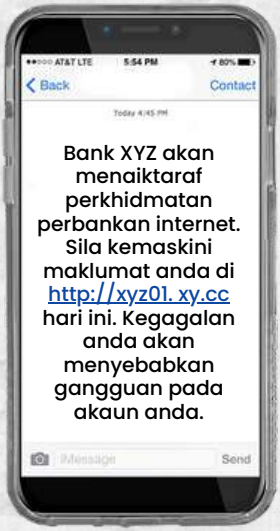
- Mangsa menerima SMS atau emel bersama pautan (link) ke laman web palsu bank / syarikat.
- *Scammer* akan menggunakan helah seperti :-
  - Mangsa perlu kemaskini akaun bank.
  - Mangsa perlu mengisi maklumat perbankan untuk tujuan siasatan (*mangsa Macau Scam*)
  - Mangsa dikatakan memenangi hadiah atau mendapat bantuan kewangan.
  - Mangsa dikehendaki memuat turun aplikasi pembayaran bagi tujuan perkhidmatan / pembelian barangan (fail APK).
- Mangsa kemudian memasukkan ID pengguna dan kata laluan pada laman web palsu. Tanpa mangsa sedari mangsa telah mendedahkan maklumat perbankan internet kepada *scammer*.

~ TREND SEMASA ~

1. **KEMASKINI AKAUN BANK**
2. **MENANG HADIAH / BANTUAN**
3. **APLIKASI TELEFON (APP SCAM)**

PHISHING

1 KEMASKINI AKAUN BANK



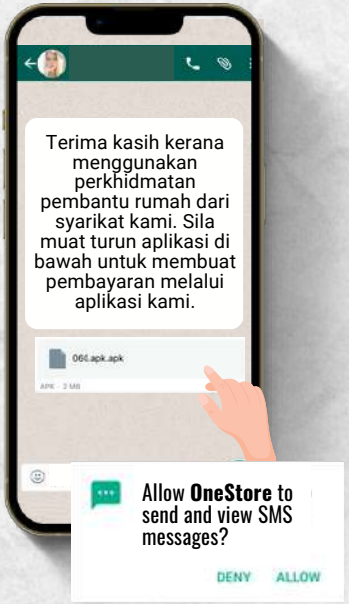
1. Mangsa terima SMS kononnya dari bank minta mangsa kemaskini akaun bank.
2. Mangsa diminta tekan pautan (*link*) pada SMS.
3. Mangsa dibawa ke laman web perbankan palsu dan memasukkan ID dan kata laluan.
4. Mangsa dihubungi suspek yang menyamar sebagai pihak bank dan meminta no. TAC.
5. Tanpa mangsa sedari, wang dalam akaun bank mangsa dipindahkan ke akaun lain

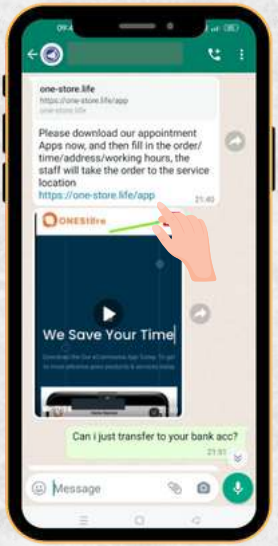
PHISHING

2 MENANG HADIAH / BANTUAN

1. Mangsa terima SMS menerima bantuan kewangan / hadiah.
2. Mangsa diminta tekan pautan (*link*) pada SMS.
3. Mangsa dibawa ke laman web syarikat yang palsu.
4. Mangsa diminta memasukkan no.pin akaun e-wallet.
5. Tanpa mangsa sedari, wang dalam akaun e-wallet mangsa telah dipindahkan.

3 APLIKASI TELEFON (APP SCAM)





1. Mangsa melihat iklan jualan barang di media sosial.
2. Mangsa menghubungi suspek melalui whatsapp dan tidak berjumpa.
3. Suspek meminta mangsa muat turun aplikasi telefon bimbit (APK file) dan install pada telefon bimbit mangsa.
4. Mangsa masuk ke laman web perbankan palsu dan memasukkan maklumat akaun bank / kad kredit mangsa
5. Page error terpapar. Tanpa mangsa sedari, wang dalam akaun bank mangsa dipindahkan ke akaun yang tidak dikenali.

PHISHING

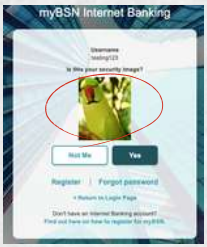
~ TIP & NASIHAT ~

1

Jangan tekan pautan (link) yang diterima dari nombor atau emel yang tidak dikenali.

2

Pastikan alamat laman web perbankan adalah betul. Bookmark alamat laman web perbankan pada browser internet.



gambar / frasa keselamatan

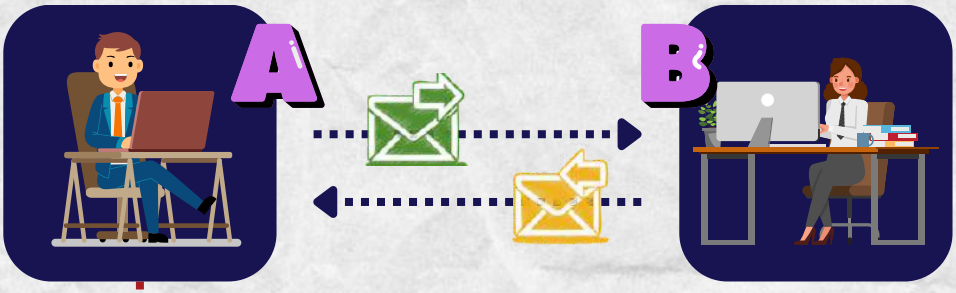
3

Pastikan frasa / gambar keselamatan adalah betul sebelum memasukkan kata laluan.

BUSINESS EMAIL COMPROMISE (BEC)

BUSINESS EMAIL COMPROMISE

~ MODUS OPERANDI ~



- 'A' dan 'B' merupakan rakan niaga dan saling berhubung melalui emel.
- 'A' terima emel daripada 'B' tentang pertukaran akaun bank syarikat 'B'.
- 'A' tidak menyedari bahawa alamat emel yang asal dengan alamat emel yang dihantar oleh suspek adalah berbeza.

Emel asal : tech-orb@tech.com.my
Emel suspek : tech-0rb@tech.cc

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

BUSINESS EMAIL COMPROMISE

~ TIP & NASIHAT~

1

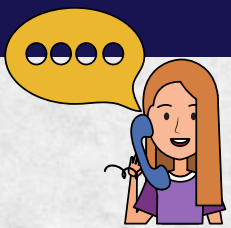
JANGAN TEKAN pautan di dalam emel yang diterima dari pihak tidak dikenali.

2

SEMAK alamat emel dengan teliti.

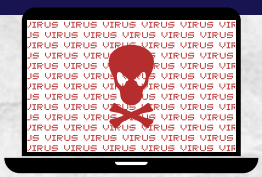
3

HUBUNGI rakan niaga melalui telefon untuk pengesahan pertukaran akaun.



4

Pastikan komputer di pejabat memasang dan mengemaskini ANTIVIRUS bagi mengelak serangan MALWARE.



TIPU NOMBOR TAC

TIPU NOMBOR TAC

~ TIP & NASIHAT ~

JANGAN KONGSI nombor keselamatan bank / nombor TAC kepada mana-mana individu.

Abaikan SMS atau whatsapp dari orang yang tidak dikenali.

HUBUNGI segera pihak bank untuk menyekat perbankan internet.

PINJAMAN TIDAK WUJUD (PTW)

PINJAMAN TIDAK WUJUD

~ MODUS OPERANDI ~

- Suspek mengiklankan tentang pinjaman wang di media cetak, media sosial atau SMS.
- Mangsa hanya berurusan melalui telefon atau whatsapp dan tidak pernah berjumpa suspek.
- Suspek tidak mempunyai pejabat dan biasanya menunjukkan sijil SSM yang palsu.
- Mangsa diminta membuat pelbagai bayaran seperti wang jaminan, duti setem, insurans dan bayaran guaman ke akaun bank keldai.
- Suspek kemudian menghilangkan diri dan gagal dihubungi.

~ TIP & NASIHAT ~

Pastikan pinjaman dibuat dengan syarikat pemberi pinjam wang yang berlesen.

Semak lesen atau nama syarikat dengan pihak Kementerian Perumahan dan Kerajaan Tempatan (KPKT).

Urusan pinjaman perlu dilakukan di **PEJABAT** pemberi pinjam wang dan dipaparkan **LESEN.**

TIPU PELABURAN

TIPU PELABURAN

~ MODUS OPERANDI ~

- Mangsa melihat iklan pelaburan di media sosial (Facebook, Instagram dll.), melalui aplikasi chat (whatsapp, telegram, wechat dll.) atau melalui kenalan.
- Mangsa ditawarkan pelaburan yang :-

  keuntungan besar dan berganda

  tiada risiko dan tidak akan rugi

- Mangsa akan menerima keuntungan pada 24 jam hingga 6 bulan pertama.
- Menggunakan nama brokers pelaburan yang sah atau berdaftar luar negara.
- Mangsa diminta membuat bayaran ke akaun atas nama individu atau syarikat yg tiada kaitan dgn pelaburan yg dilaburkan.
- Mangsa kemudian gagal mendapatkan keuntungan yang dijanjikan dan wang kapital yang dilaburkan.
- Suspek gagal dihubungi.

TIPU PELABURAN

~ TIP & NASIHAT ~

- Melabur di platform yang betul dan berdaftar dengan Bank Negara Malaysia dan Suruhanjaya Sekuriti Malaysia.
- Dapatkan nasihat kewangan dari ejen yang berdaftar.
- Jangan percaya pada pelaburan yang menawarkan keuntungan lumayan dalam masa yang singkat.
- Jangan masukkan wang ke akaun bank yang tiada kaitan dengan pelaburan yang dibuat.
- 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
(603) 6204 8999

CIRI-CIRI PELABURAN PALSU

PULANGAN TINGGI

Mangsa dijanjikan kadar faedah, pulangan atau keuntungan yang jauh lebih tinggi daripada pulangan yang ditawarkan oleh institusi kewangan berlesen untuk deposit.

LABUR SEGERA

Mangsa diminta untuk menyertai pelaburan dengan segera kerana tawaran tersebut hanya untuk jangka masa pendek.

PELABURAN LUAR NEGARA

Mangsa diminta untuk melabur dalam skim luar negara. Mangsa tidak dapat memeriksa pejabat atau mengesahkan status pelaburan di laman web mana-mana pihak berkuasa pengawalseliaan.

JABATAN SIASATAN JENAYAH KOMERSIL
POLIS DIRAJA MALAYSIA

Dikemaskini pada Disember 2022
oleh Bahagian Siasatan Jenayah Siber & Multimedia