KLIK DENGAN BIJAK

"JANGAN SALAH KLIK"

Executive Talk Series #4

9 Jun 2022

Ts. Md Tahir bin Musa
Timbalan Pengarah
Suruhanjaya Komunikasi dan Multimedia Malaysia

PENGURUSAN RISIKO DALAM TALIAN

Agenda

- Terlebih kongsi
- Maklumat palsu
- Penipuan kewangan
- Keganasan siber
- Keselamatan komputer
- Kawalan kendiri

Risiko dalam talian

keganasan siber

kandungan bersifat jelik dan mengancam

Terlebih kongsi maklumat

jenayah siber

hasutan

fitnah

darknet/ dark web

perjudian

pornografi

maklumat palsu

buli siber

pelanggaran hak cipta

phishing

malware

Serangan Man in the middle (MitM)

penggunaan bermasalah

'love scam'

virus

kecurian identiti

penipuan kewangan

penggodaman

DDoS

TERLEBIH KONGSI

Apa itu terlebih kongsi?

- mengepos terlalu banyak informasi/ maklumat peribadi terutamanya di laman rangkaian sosial; dan
- membiarkan jutaan orang di Internet melihat informasi peribadi anda.

Antara maklumat yang tidak perlu dikongsi:

1) Alamat rumah
2) Nombor kad pengenalan
3) Nombor telefon
4) Gambar-gambar intim
5) Lokasi pergerakan terkini
6) Maklumat sulit/ rahsia
7) Pergerakan
8) Gambar anak
9) dlln.

Kenapa terlebih kongsi maklumat di media sosial?

- Pengaruh dan galakan daripada media sosial
- Meluahkan perasaan kecewa
- Mendapatkan perhatian
- Melepaskan emosi dan tekanan

Risiko terlebih kongsi

Mengurangkan produktiviti

Menjejaskan reputasi

Ancaman keselamatan

Perbandingan sosial

Kecurian identiti

Perceraian rumah tangga

Rompakan harta benda

Hendap siber

Contoh terlebih kongsi

Antara akibat terlebih kongsi

Celeb Superlatives: Disastrous oversharing, disastrous underplanning

Maria Puente, USA TODAY Published 4:31 p.m. ET Oct. 10, 2016

(Photo: Evan Agostini, AP)

CONNECT TWEET LINKEDIN COMMENT EMAIL MORE

USA TODAY's **Maria Puente** digs through the latest celebrity news for highlights ... and lowlights. Think high school yearbook superlatives — if Kid Cudi and Ashton Kutcher were classmates.

Most imprudent oversharing on social media: Kim Kardashian

She has always been completely open on her social media accounts, sharing with her zillions of followers minute by minute where she is, what she's doing, what's she's wearing (or not). Now she's rethinking all that after she was robbed at gunpoint in her luxury Paris apartment of more than $10 million in jewels on Oct. 2. In the hours and days before, she was posting with abandon, including a selfie flaunting a new $4.5 million, 20-carat diamond ring she got from husband Kanye West. That turned out to be top on the robbers' list. French police were clear about what happened: "It was really the celebrity who was targeted, with possessions that had been seen and noticed via social media, and it was these goods that the attackers targeted," chief spokeswoman Johanna Primevert told reporters.

CNN World | U.S. Politics | Money | Entertainment | Tech | Sport | Travel | Style | Health | Video | VR International Edition +

When oversharing online can get you arrested

By Lauren Russell, CNN

Updated 1323 GMT (2123 HKT) April 18, 2013

Richard Godbehere was arrested in February after posting a video of himself drinking and driving online.

Story highlights

Law enforcement can obtain virtually anything posted online and use it against a person

The five-minute video opens with a man cruising along in his car, cracking open a bottle of what appears to be Beck's beer and taking a swig.

Antara akibat terlebih kongsi

HOLIDAY

Burglars use social media to find next victims

(Shutterstock)

abc NEWS

Tuesday, December 23, 2014

There's a big warning about social media this holiday season. Experts say sharing too much online could make you a target for burglars. And you might not even know it.

Back in the day, you would have to peer in someone's window to know if they were gone. But these days, all it takes to know if someone's home is empty is to rummage through their social media.

"You gotta be careful," said burglary victim Lavern Cheatheam. "You think posting and checking in wherever you go is fun, but you are actually letting people know -- hey I am gone. Go over there and take what you want."

She should know. Her home was cleaned out after her daughter posted their family's Las Vegas vacation on her Facebook page, tipping off burglars who were monitoring to see if the family was out of town.

On survey out of the UK says more than 78 percent of burglars are using social media to find their targets.

33 COMMENTS

Kerana "Share Location" Di WhatsApp: Zaquan Adha Akui Mungkin Rumahnya Sudah Lama Diperhatikan

0 Like Tweet

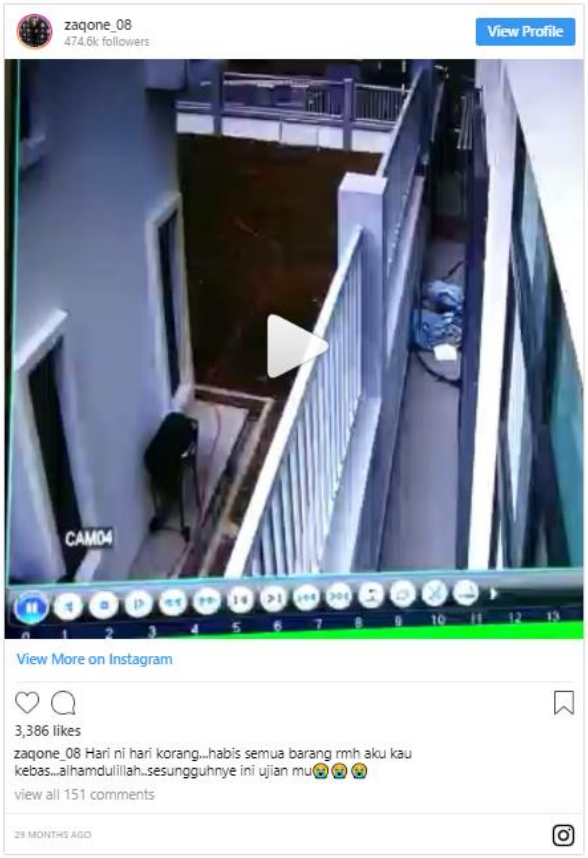
Written by Bella | April 26th, 2016

Baru-baru ini, rumah pasangan selebriti Zaquan Adha dan Ayu Raudhah telah dipecah masuk buat kali ketiga dan mereka mengalami kerugian mencecah RM200,000.

Zaquan menerusi portal Media Hiburan tidak menolak kemungkinan bahawa rumah mereka sudah lama diperhatikan apabila beliau sebelum ini pernah â€œshare locationâ€□ melalui aplikasi WhatsApp untuk mengadakan majlis rumah terbuka dan menerima kehadiran daripada beberapa orang yang mereka tidak kenali.

> *Ia bermula sewaktu kami mengadakan majlis rumah terbuka.Â Seperti orang lain, kami pun share location rumah supaya tetamu senang sampai.Â Tak sangka pula jadi viral sampai ada tetamu yang tak kenal pun datang.Â Selain itu, rumah kami memang sudah 'diperhatikan'.Â Pengawal rumah ada, cuma mereka bertugas pada waktu malam sahaja.*

Antara barang mereka yang hilang ialah 15 beg tangan milik Ayu Â yang berjenama Dior, Prada, Chanel, Louis Vuitton serta jam tangan Rolex dan New Balance milik Zaquan.



Zaquan sempat memuat naik video di akaun Instagram miliknya yang dirakam oleh CCTV.Â Ia menunjukkan pencuri tersebut masuk dengan memanjat pagar rumahnya.

Mungkin selepas ini Zaquan Adha dan Ayu Raudhah boleh menggunakan sistem keselamatan yang lebih baik jika tidak mahu pindah daripada kawasan perumahan terbabit. Anggaplah ini sebagai ujian Allah SWT dan mungkin ada rezeki yang lebih lagi buat anda berdua selepas ini.

Akibat terlebih kongsi

History of Terminations & Firings Because of Employee Social Media

May 7, 2013 By Jessica Miller-Merrell — 38 Comments

2017

February

Dan Grilo, a Hilary Clinton volunteer lost his job from Liberty Mutual after mocking a widow of a Navy Seal on Twitter.

January

School administrator and social media manager, Katie Nash roasts kid on Twitter loses job.

2016

December

Michigan firefighter, Ryan Hudson fired after posting racist comments about black lives matter on Facebook.

Canadian nurse, Carolyn Strom who vented on Facebook found guilty of unprofessional conduct.

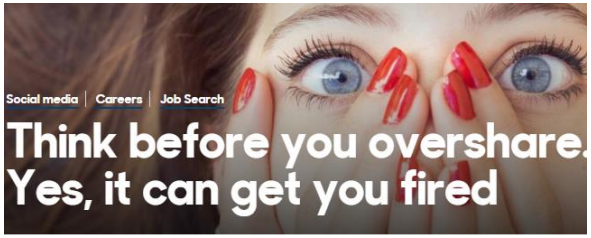
July

Police officer, Rodney Lee Wilson threatens child on Facebook and loses job.

June

Bank of America terminates employee after racists Facebook rank goes viral.

Two Memphis police officers suspended for Snapchat updates.



Has social media made us less inclined to share our opinions?

By Saadia Hashmy-Elsby
27 August 2016

In July The Telegraph reported that a British Council executive Angela Gibbins **will face disciplinary action** after writing a critical post about HRH Prince George. The newspaper also reported that an Instagram post about **feeding meat to vegan diners** in Derby, UK, got head chef Alex Lambert fired.

"Staff usage of social media reflects on the company even if staff members aren't officially managing that organisation's social media channels," says Chris Lee, head of digital strategy and training consultancy Silvester & Finch in London. Employees can easily let slip confidential information, or their opinions could reflect negatively on their firm, he says.

> *Because of this first-to-publish mentality; we can see why we're less inclined to self-filter because we're in such a hurry to produce something that's funny or shocking*

In 2015 UK firm Game Retail **dismissed one of its employees** over offensive but non-work related tweets. Despite the employee initially winning an unfair dismissal case Game Retail appealed and won.

Langkah menangani sikap terlebih kongsi

Kawal privasi dan reputasi dalam talian dengan mengamalkan prinsip asas seperti berikut:

1. Lakukan **KETETAPAN PRIVASI** untuk akaun media sosial.
2. Lindungi reputasi digital anda dengan **MEMADAMKAN** semua maklumat peribadi dan info negatif yang berpotensi merosakkan reputasi anda.
3. **KEMAS KINI** senarai kenalan media sosial. Padamkan orang yang tidak dikenali supaya mereka tidak dapat melihat perkongsian peribadi anda.
4. **FIKIR, NILAI DAN KAJI** maklumat sebelum berkongsi.
5. **JANGAN DEDAH MAKLUMAT PERIBADI ANDA.**

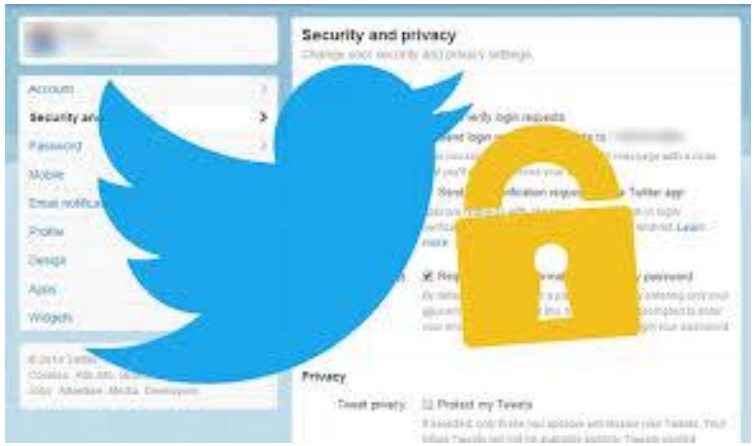
Utamakan privasi laman web anda

- Seperti diari yang boleh dikunci dengan mangga, Internet turut mempunyai fungsi yang membolehkan anda mengunci maklumat peribadi.

- Ia dipanggil ketetapan privasi, di mana anda boleh membenarkan orang lain untuk melihat informasi atau gambar tertentu sahaja.

- Anda juga boleh ‘menyembunyikan’ sesuatu maklumat yang anda tidak mahu dilihat oleh orang lain.

- Ketetapan privasi membenarkan anda memilih siapa yang boleh melihatnya dan siapa yang tidak.



Sesi interaktif

1. Adakah anda membuat ketetapan privasi media sosial?
2. Apakah risiko swafoto?
3. Jelaskan apakah aplikasi keselamatan, GPS dan geotagging?
4. Pernahkah anda membuat aduan berkaitan kandungan di media sosial?
5. Mengurus jejak siber – Buat carian nama sendiri dan lihat jejak digital anda. Nilai baik dan buruk setiap posting berkaitan anda. Ambil tindakan yang sewajarnya.

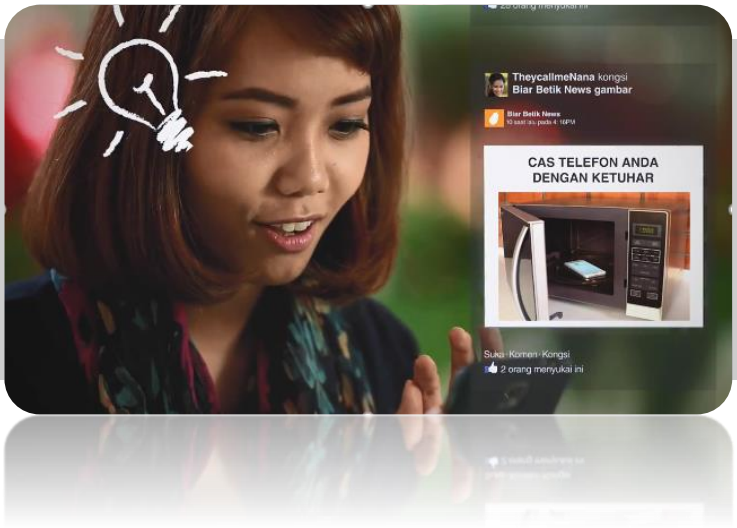
Sesi Interaktif

Apakah risiko swafoto?

Kesimpulan

Terlebih Kongsi tidak hanya memberitahu siapa diri anda, ia juga melibatkan isu keselamatan dan privasi anda dan keluarga.

Jadi, bijaklah berkongsi!

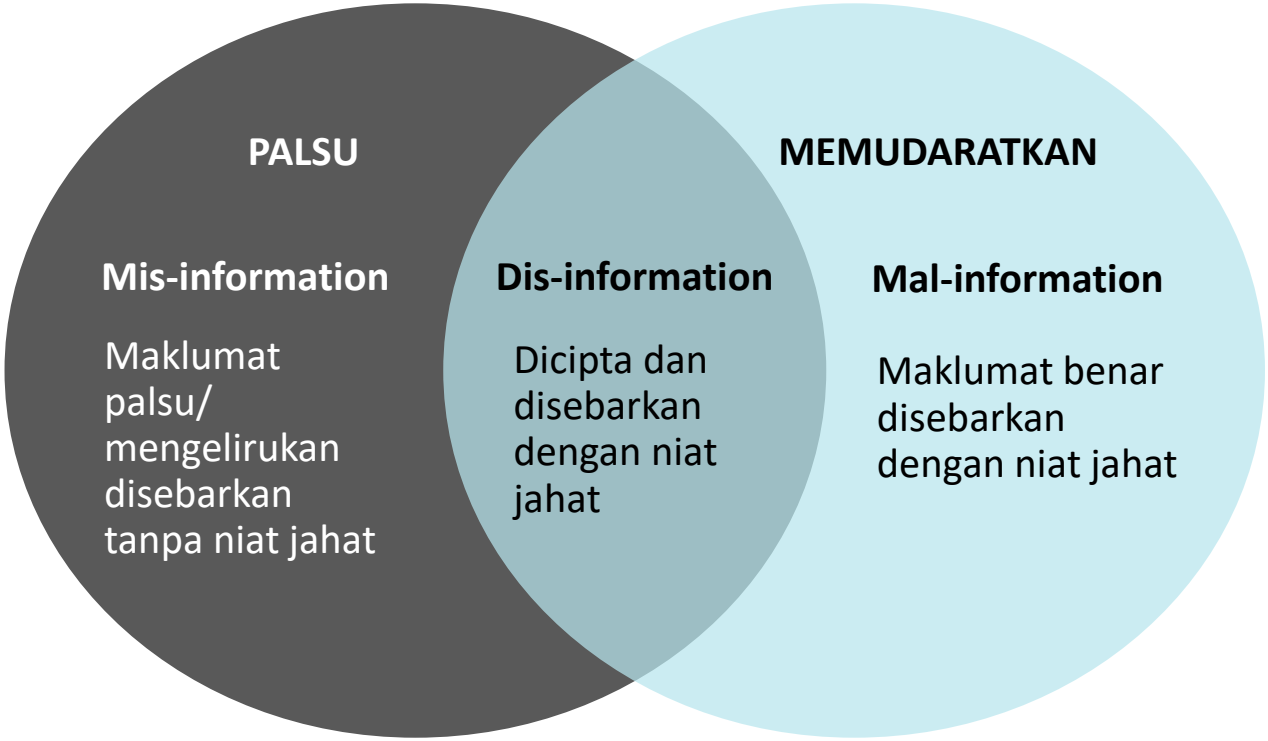


MAKLUMAT PALSU


"Jangan pergi pasar Kelana Jaya, ada kes COVID-19."
MCMC


Saya rasa
kalau kita periksa
suhu kat kepala,
boleh kena kanser.
Eh
mana ada.
Semak fakta dulu
sebelum berkongsi
pandangan.
MCMC
KEBEBASAN
BERSUARA
BUKAN
KEBEBASAN
BERBOHONG

Maklumat yang disebarkan tanpa kesahihan serta bukti yang sah



Sumber:
1. Claire Wardle
2. The Council of Europe report Information Disorder: Toward an interdisciplinary framework for research and policy making

Mendatangkan pelbagai kesan negatif jika tidak dibendung penyebarannya

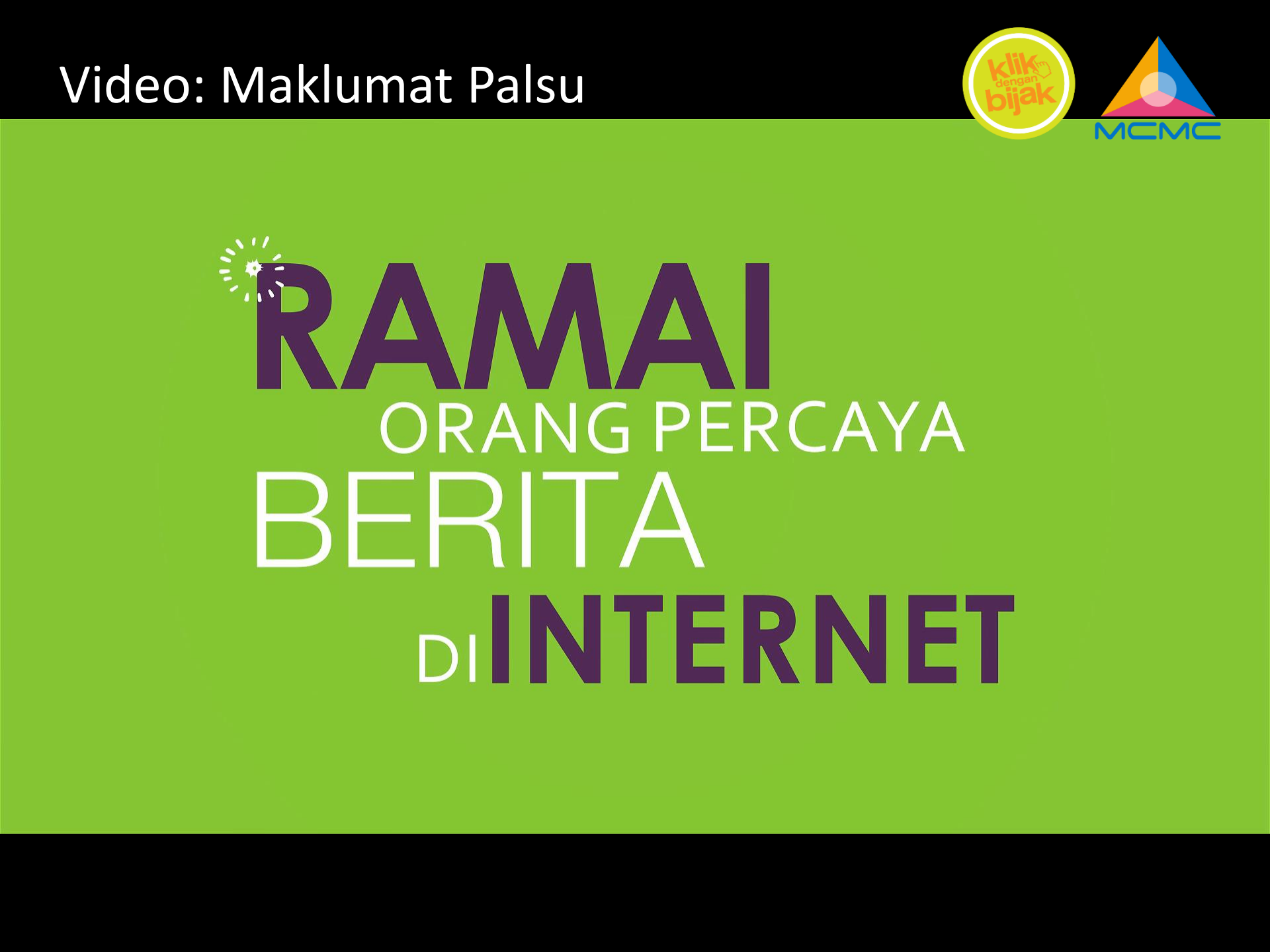
Mengaibkan individu atau pihak yang terlibat

Memberi kesan negatif kepada reputasi seseorang atau organisasi

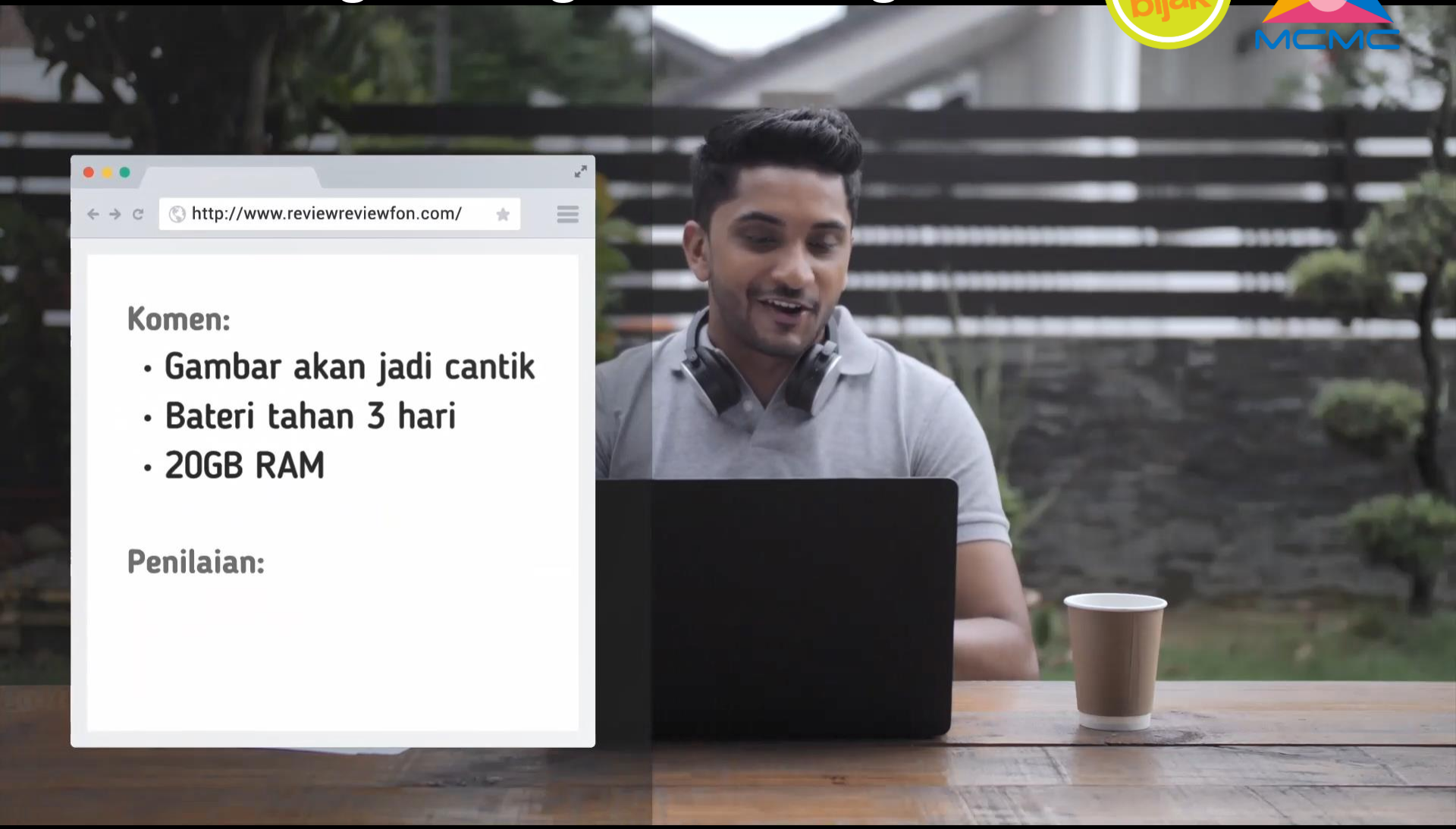
Menyebabkan kerugian jika melibatkan wang ringgit

Mengakibatkan penyebaran maklumat yang tidak benar kepada masyarakat

Video: Maklumat Palsu



Video: Jangan Kongsi Kebohongan



Video: Menentusahkan maklumat

Video: Semak fakta

Maklumat Palsu

Sesetengah berita dan maklumat diterima dalam talian sungguh menyakinkan, kelihatan betul, dan menarik sehingga sukar untuk menentukan sama ada ia palsu atau benar. **Berwaspada dan periksa sesuatu maklimat sebelum mempercayainya dan membuat perkongsian.**

Menilai kesahihan maklumat

S

Sumber
Source

Lihat asal usulnya. Adakah ia boleh dipercayai?
Pengarang: Siapakah pengarangnya? Apakah latar belakang dan kelayakan pengarang tersebut?
Tempoh Masa: Bilakah sumber itu diterbitkan? Adakah ia telah dikemas kini baru-baru ini?

U

Faham
Understand

Fahamkan apa yang anda baca. Pastikan kejelasannya.
Cari fakta, bukan pendapat atau pengalaman semata-mata. Apakah topik yang dibincangkan? Adakah ianya secara **mendalam atau ringkas**?
Matlamat: Kenapa pengarang memulakan topik tersebut? Apa yang dia mahu capai melalui penulisan tersebut?

R

Selidik
Research

Buat carian lebih mendalam dan melangkaui sumber awal. Periksa dan bandingkan dengan **sekurang-kurangnya 3 sumber berlainan.**

E

Menilai
Evaluate

Cari keseimbangan. Gunakan pertimbangan yang saksama. Lihat daripada sudut yang berbeza.

Kesan maklumat tidak tepat

Tapak kasut didakwa ada kalimah Allah, Bata rugi setengah juta ringgit akibat jadi mangsa viral palsu

6:56:00 PM | jejak rezeki

Syarikat Bata terpaksa mereka keluaran kasut sekolah baru bagi membersihkan dakwaan palsu yang mengatakan tapak kasut *B-First*mengandungi kalimah 'Allah'.

Tapak kasut didakwa ada kalimah Allah, Bata rugi setengah juta ringgit akibat jadi mangsa viral palsu

#000000;">Pengarah urusannya Paolo Grassi berkata pihaknya terpaksa menanggung kerugian lebih RM500,000 selepas dakwaan itu tular di media sosial dalam tempoh empat minggu.

Sumber: Berita Harian https://www.bharian.com.my/node/249566

Kesan maklumat tidak tepat

Kesan maklumat tidak tepat

PELAKON dan pengarah, AR Badul, ketika menerima kunjungan Pengerusi Perbadanan Kemajuan Filem Nasional Malaysia (FINAS), Datuk Samsuni Mohd Nor (kiri), di IJN, baru-baru ini. - Foto ihsan FINAS

Berita palsu susahkan keluarga, saudara-mara - AR Badul

Oleh Hanisah Selamat
hanisah@bh.com.my

KUALA LUMPUR: Pengarah dan pelakon, AR Badul, mendakwa berita palsu kematiannya yang tersebar sejak pagi tadi menyusahkan saudara-mara apabila ada antara mereka sudah menempah tiket kapal terbang untuk menghadiri majlis pengebumiannya.

Katanya, ramai anggota keluarganya tinggal di Singapura, sekali gus desas-desus yang sampai ke telinga mereka membuatkan masing-masing kelam kabut mencari penerbangan ke Kuala Lumpur sementara menunggu kesahihan berita.

Kesan maklumat tidak tepat

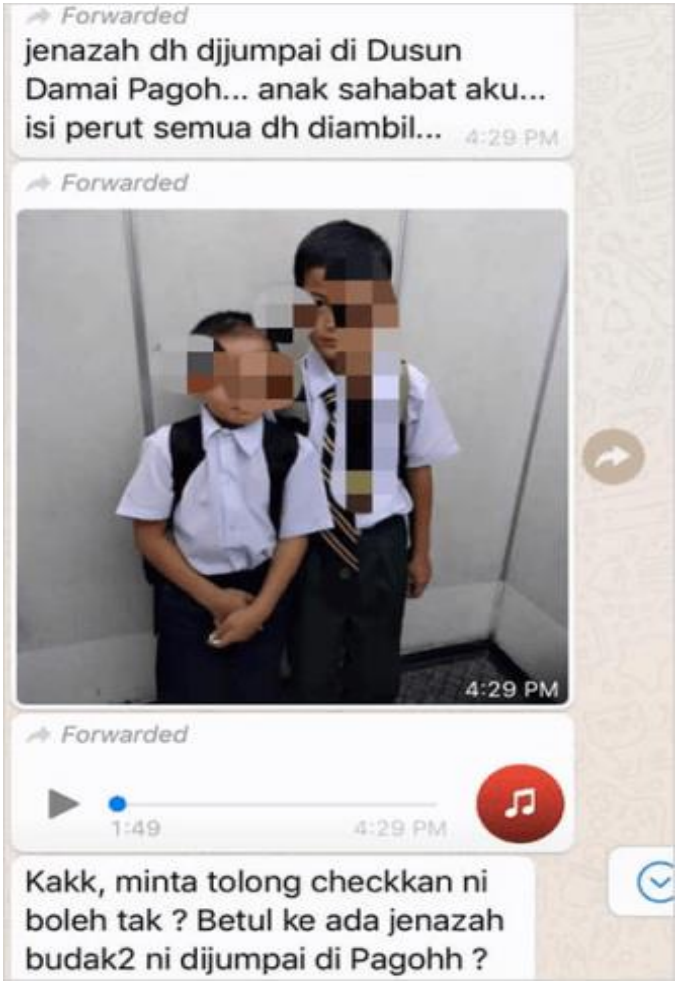
KETUA Polis Daerah Muar, Asisten Komisioner Zaharudin Rasip. - Foto Adi Safri

Tiada kes kanak-kanak dibunuh, isi perut dikorek di Pagoh

Oleh Badrul Kamal Zakaria
badrulkamal@nstp.com.my

MUAR: Polis Muar mengesahkan tidak menerima sebarang laporan berkaitan kes berkaitan penemuan mayat kanak-kanak dengan isi perutnya diambil sebagaimana yang viral di media sosial hari ini.

Ketua Polis Daerah Muar, Asisten Komisioner Zaharudin Rasip, berkata pihaknya juga mengesahkan tiada sebarang kejadian yang berlaku di Dusun Damai, Pagoh di sini, sebagaimana yang didakwa dalam media sosial berkenaan.



c|net | Health and Wellness

FEATURED FITNESS SLEEP HEALTHY EATING CAREGIVING PERSONAL CARE

5G coronavirus conspiracy theory leads to 77 mobile towers burned in UK, report says

Attacks on cell towers continue.

Corinne Reichert May 7, 2020 8:34 a.m. PT 86 LISTEN · 01:09

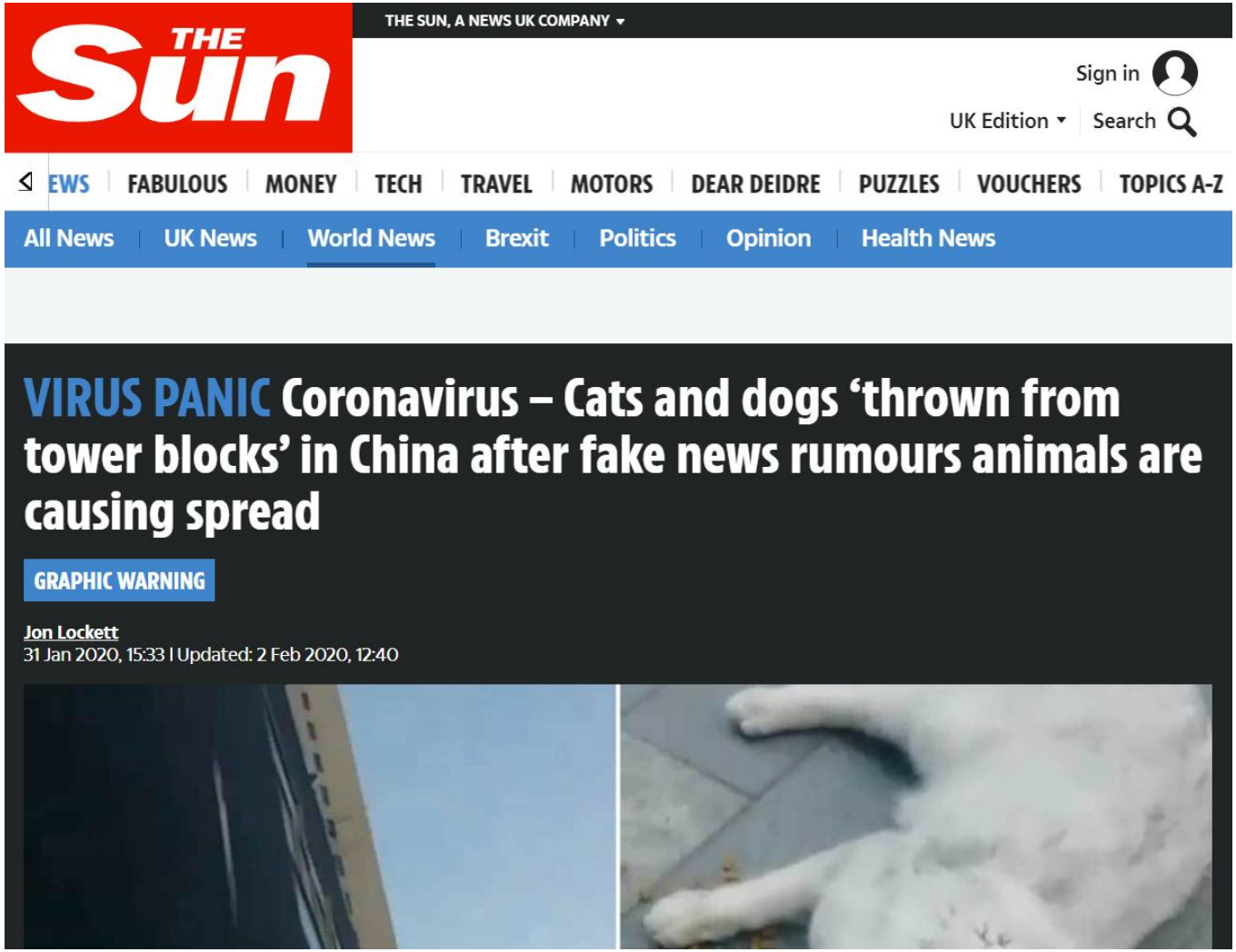
Almost 80 mobile towers have reportedly been burned down in the UK due to false coronavirus conspiracy theories that blame the spread of COVID-19 on 5G. The arson attacks began in early April, with 77 towers now damaged, Business Insider reported Wednesday citing industry group Mobile UK.

"Daily attacks are very low now but have not stopped entirely," a Mobile UK spokesman told Business Insider.

As of April 21, 40 employees of one UK carrier have also been attacked physically or verbally, according to BT CEO Philip Jansen. "We've even had one Openreach engineer stabbed and put in hospital," Jansen said.

The conspiracy theory is false -- radio waves can't cause a virus. Facebook, YouTube and Twitter have all committed to taking down misinformation. UK carriers have also asked people to stop burning mobile towers, and the UK's national medical director called the 5G conspiracy theory "complete and utter rubbish."

Kesan maklumat tidak tepat



klik dengan bijak

MCMC

South China Morning Post News Comment Lifestyle More + SIGN IN/UP

Opinion

Editorial *by SCMP Editorial*

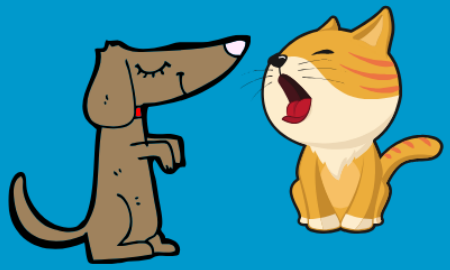
Spread of fake news worsens an already bad public health crisis

- Responsible use of social media is more essential now than ever as rumours about the new coronavirus only fuel panic; we need to be alert, not alarmed

SCMP Editorial
Published: 9:35pm, 2 Feb, 2020

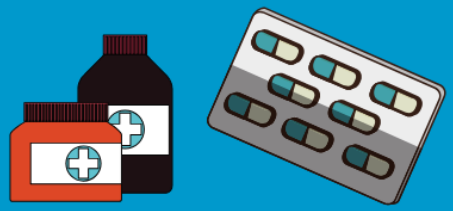
World Health Organization

Can pets at home spread the new coronavirus (2019-nC0V)?



Does the new coronavirus affect older people, or are younger people also susceptible?

Are antibiotics effective in preventing and treating the new coronavirus?



Are there any specific medicines to prevent or treat the new coronavirus?

Contoh kes 1

SIASATAN TERHADAP PENTADBIR AKAUN APLIKASI FACEBOOK 'YEOH PATSY' DI BAWAH SEKSYEN 233(1)(a) AKTA KOMUNIKASI DAN MULTIMEDIA 1998 BERHUBUNG KANDUNGAN BERSIFAT PALSU MENGENAI WABAK COVID-19

Analisa kandungan mendapati kandungan yang diadukan oleh orang awam adalah bersifat palsu berikutan pihak Jabatan Kesihatan Negeri Pulau Pinang melalui kenyataan bertarikh 28/01/2020 mengesahkan bahawa kandungan yang dimuatnaik oleh suspek adalah bersifat palsu.

Contoh kes 2

SIASATAN TERHADAP PENTADBIR AKAUN FACEBOOK ‘AFENDY SAID’ DI BAWAH SEKSYEN 233(1)(a) AKTA KOMUNIKASI DAN MULTIMEDIA 1998 BERHUBUNG KANDUNGAN BERSIFAT PALSU MENGENAI WABAK COVID-19

Analisa kandungan mendapati gambar yang disiasat telah diedit dengan menggunakan aplikasi percuma di mana suspek telah memasukkan gambar sekumpulan warga China yang diambil oleh jurugambar akhbar antarabangsa, AFP iaitu Nicolas Asfouri bertajuk “***China deploys army medics to overwhelmed virus epicentre***” bertarikh 25/02/2020.

Seterusnya suspek telah mengedit gambar tersebut pada laman web ‘breakyourownnews’ dengan memasukkan *headline*: “***ALL COUNTRIES EXCEPT MALAYSIA***” serta Ticker (sub-headline) “***ALL COUNTRIES HAS BANNED CHINESE TOURIST EXCEPT MALAYSIA***”

Video: Mengesah Informasi

RANGKAKERJA MCMC DALAM MENANGANI MAKLUMAT PALSU

SEBENARNYA.MY (*FACT-CHECK & CROWDSOURCING*)

- Lebih 290 juta hit (2017 – 2021)
- Media sosial dan saluran permesejan segera (IM)

KOORDINASI ANTARA AGENSI

- *Operational Working Group –Unverified News Online (OWG-UNO)*
- COVID-19: Rapid Response Team

ADVOKASI DAN PEMERKASAAN PENGGUNA

- Keterlibatan media
- Inisiatif kesedaran: Klik Dengan Bijak dan Sukarelawan ICT Malaysia
- The Truth Campaign

KAWALSELIAAN BERSAMA PENYEDIA PLATFORM

- Penurunan maklumat palsu yang boleh mendatangkan mudarat fizikal
- Kerjasama dengan *fact checker* pihak ke-3

UNDANG-UNDANG

- Kanun Keseksaan (Seksyen 505)- Pernyataan membawa kerosakan awam
- AKM 1998- Seksyen 233- Penggunaan tidak wajar kemudahan rangkaian atau perkhidmatan rangkaian, dll.

Sumber: Jabatan Media Baharu, MCMC. 2022.

SEBENARNYA.MY- *FACT-CHECK* dan *CROWDSOURCING*

- **PUSAT SEHENTI AWAM**
- **TENTUSAHKAN m**aklumat yang diterima di Internet
- **SALURKAN** berita untuk penentusahan
- **4.8 JUTA HIT SETIAP BULAN** selepas dilancarkan (2017 – 2021)
- **569 ARTIKEL** diterbitkan melibatkan penyangkalan berita palsu, penjelasan, dan memberi kesedaran terhadap jenayah berkaitan pandemik COVID-19.

SEBENARNYA.MY

Tidak Pasti Jangan Kongsi

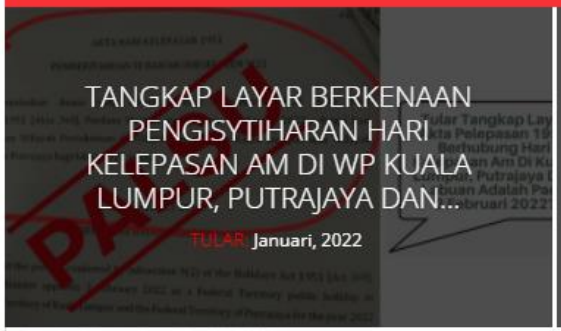
BUKAN SEMUANYA BENAR DI INTERNET !

TIDAK PASTI, JANGAN KONGSI

Layari *sebenarnya.my* untuk mengesahkan kesahihan maklumat.

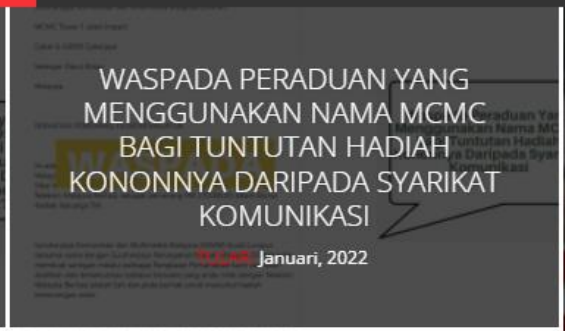
UTAMA | NASIONAL | SOSIAL | INFO | LOGO | COVID-19 | SALUR KEPADA KAMI

BERITA TERKINI



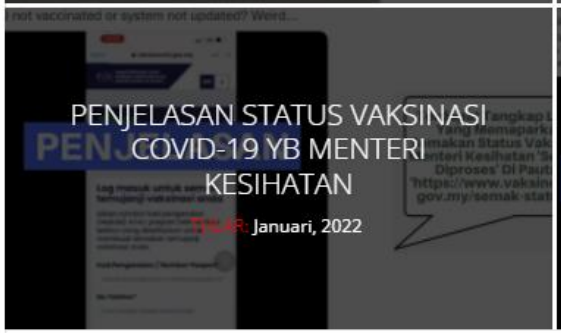
TANGKAP LAYAR BERKENAAN PENGISYTIHARAN HARI KELEPASAN AM DI WP KUALA LUMPUR, PUTRAJAYA DAN...

TULAR Januari, 2022



WASPADA PERADUAN YANG MENGGUNAKAN NAMA MCMC BAGI TUNTUTAN HADIAH KONONNYA DARIPADA SYARIKAT KOMUNIKASI

TULAR Januari, 2022



PENJELASAN STATUS VAKSINASI COVID-19 YB MENTERI KESIHATAN

TULAR Januari, 2022

TIADA PELEPASAN AIR DARI EMPANGAN DURIAN TUNGGAL

TULAR Januari, 2022

KEJADIAN AIR DERAS BERLAKU DI SUNGAI TELEMONG BUKAN DI TASIK KENYIR

TULAR Disember, 2021

Sesi Interaktif

Eksplorasi Sebenarnya.my

Panduan Dalam Menggunakan Hak Kebebasan Bersuara

PENIPUAN KEWANGAN

Apa itu penipuan kewangan dalam talian?

Aktiviti di mana peralatan komputer atau rangkaian digunakan sebagai medium untuk melakukan jenayah yang melibatkan kerugian wang ringgit atau kecurian maklumat peribadi.

Kes penipuan dalam talian catat kerugian lebih RM1.61 bilion

DIANA AZIS | | 14 Mac 2022

Sebanyak 51,631 kes penipuan dalam talian dilaporkan dari 2019 hingga 2021 melibatkan kerugian lebih RM1.61 bilion. - Foto 123RF

Sebanyak 51,631 kes penipuan dalam talian dilaporkan dari 2019 hingga 2021 melibatkan kerugian lebih RM1.61 bilion.

Tahun 2019:
5,725 kes dilaporkan
Kerugian: > RM250 juta.

Tahun 2020:
6,003 kes dilaporkan
Kerugian: Hampir RM290 juta.

Tahun 2021 – Mac:
1,392 kes dilaporkan
Kerugian: RM38 juta

Jenis-jenis *scam*/penipuan

1. **Scam 409**
   - Penipuan yang menggabungkan penyamaran (kerabat diraja, ahli politik, bekas pemimpin negara) dengan variasi skim bayaran pendahuluan di mana surat dihantar atau diemel kepada mangsa. Mangsa ditawarkan peluang untuk perkongsian jutaan dollar yang akan dikeluarkan dari negara yang bergolak (politik, perang, dlln.).

2. Penipuan melalui panggilan telefon
   - *Scammer* akan membuat panggilan dan menyamar sbg pegawai polis/kastam/bank. *Scammer* biasanya akan mengugut mangsa dan meminta mereka menyerahkan maklumat kewangan.

3. Penipuan pinjaman tidak wujud
   - *Scammer* akan menghubungi mangsa melalui media sosial, sms atau telefon untuk memujuk mangsa memohon pinjaman yang tidak wujud.

4. Penipuan pembelian dalam talian
   - Pembeli tidak menerima barang yang dibeli walaupun telah membuat bayaran atau menerima barangan yang lain daripada yang diiklankan

5. Phishing
   - Cubaan penipuan melibatkan teknik mencuri maklumat sulit dengan menggunakan penyamaran. Menggunakan e-mail sebagai medium.

Kejuruteraan Sosial

APA ITU SERANGAN KEJURUTERAAN SOSIAL?

Kejuruteraan sosial ialah seni memanipulasikan mangsa menerusi muslihat dan penipuan supaya mangsa memberikan maklumat sulit dan wang. Penjenayah mengeksploitasi kepercayaan seseorang untuk mengetahui butiran perbankan, kata laluan atau data peribadinya.

Siapakah sasarannya?
Semua orang!
Golongan berusia, terutamanya, mudah terdedah kepada bahaya ini, tetapi individu di semua peringkat umur, di seluruh dunia dan dari semua latar belakang adalah berisiko.

Mengapakah orang ramai membiarkan diri mereka ditipu?
Teknik kejuruteraan sosial semakin canggih dan cara komunikasi yang digunakan selalunya kelihatan sangat profesional. Penjenayah tahu cara untuk memanipulasi sehingga boleh meyakinkan mangsa mereka.

Mengapakah kejuruteraan sosial digunakan?
Pada kebiasaannya, ianya lebih mudah untuk mengeksploit kecenderungan semula jadi seseorang untuk mempercayai orang lain daripada mencari cara untuk menggodam perisiannya.

Faktor kelemahan
Manusia. Penjenayah mengeksploit sikap mempercayai atau kesanggupan mangsa untuk membantu orang lain, atau menggunakan ugutan untuk mendapat hasil yang mereka inginkan.

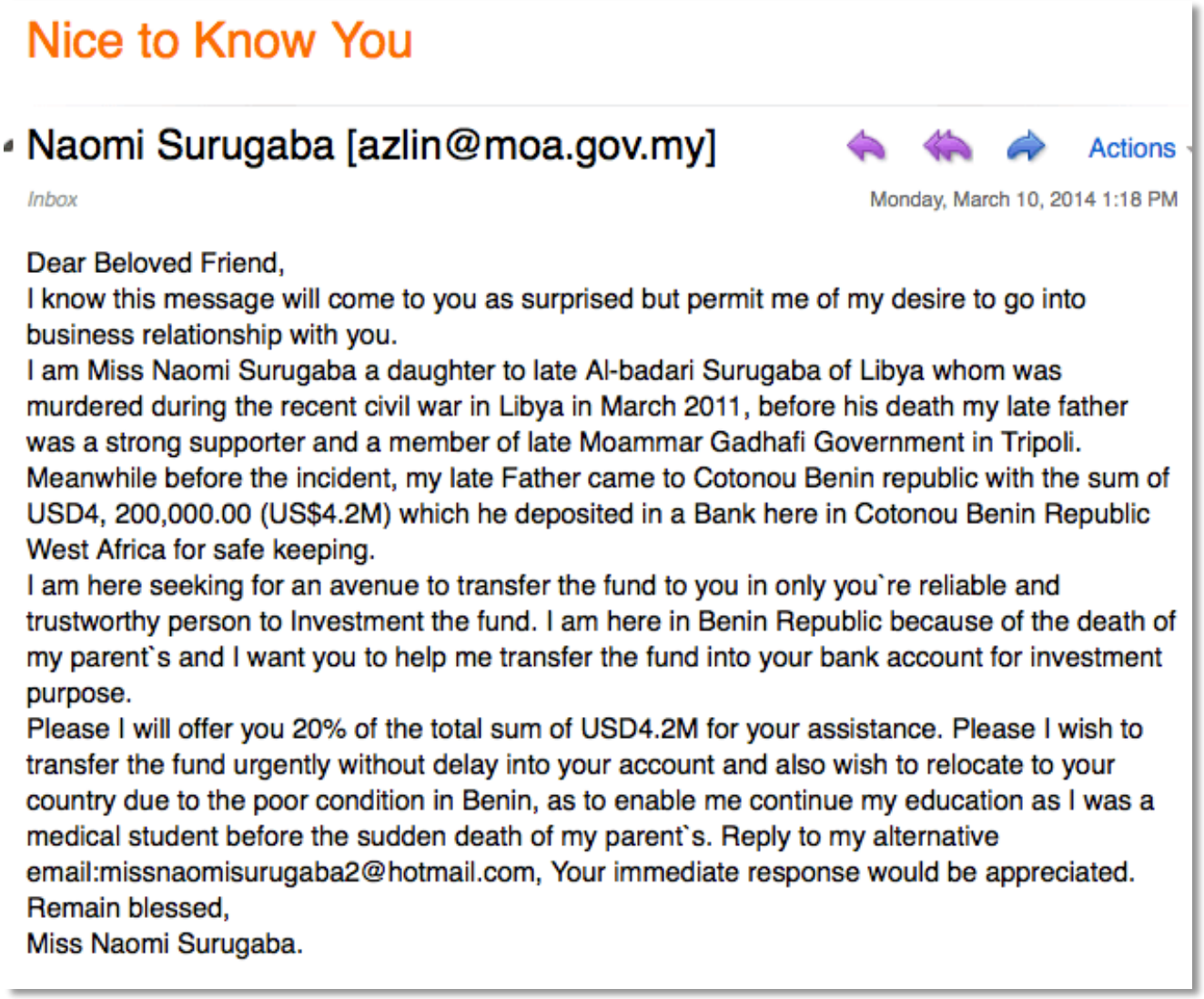
E-mel daripada rakan
Hai Hamzah, tempat ini boleh menjadi destinasi percutian kita. Ia hebat! Pautan

Tahniah, anda menang RM30,000!
Loteri, hadiah utama peraduan dan sebagainya.

Mengumpan
PENDAPATAN LUMAYAN RM5,000 SEMINGGU DARI RUMAH!!!

Jawapan kepada soalan yang anda tidak pernah tanya
Kendalian komputer peribadi anda telah semakin perlahan. Log masuk untuk mula memperbaiknya secara percuma.

Nigerian/ 409 scam



Nice to Know You

Naomi Surugaba [azlin@moa.gov.my] Actions

Inbox Monday, March 10, 2014 1:18 PM

Dear Beloved Friend,
I know this message will come to you as surprised but permit me of my desire to go into business relationship with you.
I am Miss Naomi Surugaba a daughter to late Al-badari Surugaba of Libya whom was murdered during the recent civil war in Libya in March 2011, before his death my late father was a strong supporter and a member of late Moammar Gadhafi Government in Tripoli.
Meanwhile before the incident, my late Father came to Cotonou Benin republic with the sum of USD4, 200,000.00 (US$4.2M) which he deposited in a Bank here in Cotonou Benin Republic West Africa for safe keeping.
I am here seeking for an avenue to transfer the fund to you in only you`re reliable and trustworthy person to Investment the fund. I am here in Benin Republic because of the death of my parent`s and I want you to help me transfer the fund into your bank account for investment purpose.
Please I will offer you 20% of the total sum of USD4.2M for your assistance. Please I wish to transfer the fund urgently without delay into your account and also wish to relocate to your country due to the poor condition in Benin, as to enable me continue my education as I was a medical student before the sudden death of my parent`s. Reply to my alternative email:missnaomisurugaba2@hotmail.com, Your immediate response would be appreciated.
Remain blessed,
Miss Naomi Surugaba.

Nigerian/ 409 *scam*

Greetings to you my friend,

I know this will come to you as a surprise because you do not know me.
I am John Alison I work in Central Bank of Nigeria, packaging and courier department.

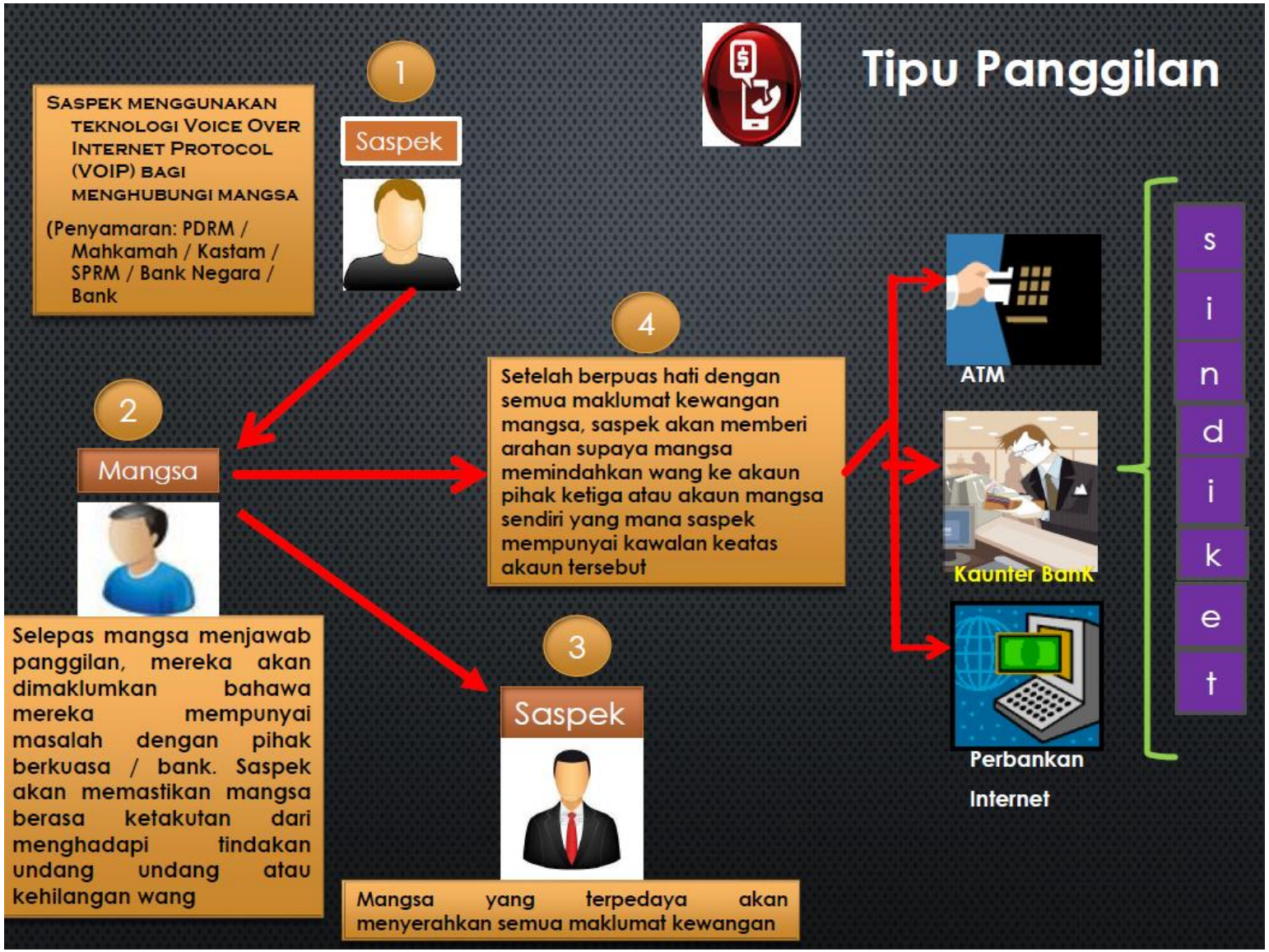
I got your contact among others from a search on the internet and I was inspired to seek your co-operation, I want you to help me clear this consignment that is already in theEurope which I shipped through our CBN accredited courier agent. The content of the package is $20,000,000.00 all in $100 bills, but the courier company does not know that the consignment contains money.

All I want you to do for me now is to give me your mailing address, your private phone and fax number, and I believe that at the end of the day you will have 50% and 50% will be for me. My identity must not be revealed to anybody.

If this arrangement is okay by you, you can call

Phone: +234 8028776685
Email:john_alison444@yahoo.com

Tipu Panggilan



Contoh Tipu Panggilan

Doktor pun kena tipu Macau Scam

Oleh Shahrinnahar Latib
cnews@nstp.com.my

KUANTAN: Sudah banyak pendedahan mengenai penipuan sindiket Macau Scam di media massa, namun masih ramai terus menjadi mangsa dengan kes terbaru membabitkan seorang seorang doktor di Raub.

Mangsa yang berusia 72 tahun kerugian RM30,000 selepas terpedaya dengan lakonan sindiket penipuan itu.

Dalam kejadian pada 18 Jun lalu, mangsa dihubungi oleh suspek yang mengaku dari Mahkamah Tinggi Alor Star dan mendakwa warga emas itu mempunyai kes iaitu hutang cukai bagi syarikat yang didaftarkan atas namanya berjumlah RM17,600.

Ketua Jabatan Siasatan Jenayah Komersial Negeri, Superintendan Mohd Wazir Mohd Yusof, berkata mangsa menafikan perkara itu dan diminta oleh suspek untuk membuat laporan polis dengan Ibu Pejabat Polis Daerah (IPD) Alor Star menggunakan talian telefon.

"Pada 28 Jun lalu, mangsa dihubungi oleh seorang lagi suspek menggunakan talian 04-7741222 yang mengaku sebagai pegawai polis dari IPD Alor Star.

"Mangsa dimaklumkan bahawa beliau bukan sahaja ada kes hutang, malah turut terbabit dengan kes pengubahan wang haram yang menggunakan akaun banknya," katanya dalam satu kenyataan media, di sini, hari ini.

Mohd Wazir berkata, mangsa menafikan perkara berkenaan dan diminta untuk memberikan nama pengguna serta kata laluan bagi perbankan atas talian akaun CIMB untuk tujuan audit oleh pihak Bank Negara Malaysia (BNM).

"Mangsa yang percaya kemudian memberikan semua data peribadi, termasuk nombor TAC yang diterimanya kepada suspek. Tidak lama kemudian, mangsa yang tidak berpuas hati membuat panggilan ke pihak CIMB untuk membuat semakan.

"Hasil semakan mendapati wang berjumlah RM30,000 dalam akaun CIMB miliknya dipindahkan ke akaun pihak ketiga iaitu akaun Hong Leong Bank tanpa pengetahuan mangsa. Mangsa kemudian membuat laporan polis di IPD Raub, semalam," katanya.

Mangsa *Scam*

Sinar Harian

>> BERITA > SEMASA > Guru rugi RM48,000 jadi mangsa 'Love Scam'

Guru rugi RM48,000 jadi mangsa 'Love Scam'

| | 26 Jun 2021

>> BERITA > SEMASA > Penolong pegawai farmasi rugi lebih RM21,000 ditipu Macau Scam

Penolong pegawai farmasi rugi lebih RM21,000 ditipu Macau Scam

NORAFIDAH ASSAN | | 21 April 2021

>> EDISI > UTARA > Pegawai bank ditipu RM3 juta angkara Love Scam

Pegawai bank ditipu RM3 juta angkara Love Scam

SYAJARATULHUDA MOHD ROSLI | | 08 Jun 2019

astro AWANI

Guru mangsa Love Scam kerugian RM63,440

Adie Sufian Zulkefli
Jun 2, 2021 12:57 MYT

BH ONLINE

Rugi RM419,012, ditipu Macau Scam

Mohd Amin Jalil - Ogos 6, 2020 @ 2:51pm
bhnews@bh.com.my

Pesara kerajaan rugi RM40,000 ditipu 'Sarjan Fauzi'

Nur Izzati Mohamad - September 6, 2020 @ 2:56pm
bhnews@bh.com.my

Kerani, guru jadi mangsa Macau Scam

Oleh Nur Izzati Mohamad - Jun 2, 2021 @ 2:26pm
bhnews@bh.com.my

myMetro

Macau Scam: Pegawai bank rugi hampir RM2 juta

Nurul Hidayah Bahaudin
nurul.hidayah@hmetro.com.my

Jenayah Terancang

‘Akademi’ Macau Scam tumpas, penulis skrip turut dicekup

AYOB Khan Mydin Pitchay (kanan) menunjukkan carta aliran sindiket Macau Scam yang melatih pekerja untuk menyamar bagi menipu orang ramai pada sidang akhbar di IPK Johor di Johor Bahru. -UTUSAN/KHAIRUL MOHD ALI

Oleh KHAIRUL MOHD ALI 21 Oktober 2021, 8:20 pm

- pengurus akaun, tenaga pengajar, ejen dan operator pusat panggilan
- modus operandi kumpulan sindiket itu adalah melatih pekerja-pekerja baru mengenai teknik penipuan dengan menyamar sebagai pegawai kutipan hasil daripada sebuah bank tempatan.
- merekrut pekerja untuk bertugas di pusat panggilan Macau Scam di luar negara antaranya Kemboja, Dubai dan Emiriah Arab Bersatu (UAE) atau pun dalam negara

Tip Mengatasi Tipu Panggilan

mudah

JANGAN PERCAYA

pada panggilan telefon ...

#beSmart

BEAT THE SCAMMERS

Polis / Makamah / SPRM / Kastam

yang beritahu anda terlibat dengan jenayah
yang anda akan ditangkap
yang anda boleh dikenakan hukuman gantung

KERANA ...

Polis tak telefon dulu penjenayah minta izin / beritahu nak tangkap.

BERTINDAK ...

Matikan panggilan telefon.
Pergi ke balai Polis berhampiran untuk bertanya. Malu bertanya, sesat jalan.
Tak salah, jangan takut.

Pegawai Bank Negara atau lain-lain Bank

yang beritahu anda ada tunggakan kad kredit / pinjaman
yang sambungkan panggilan anda kepada Polis

LAGI JANGAN PERCAYA ...

Jika anda tak pernah daftar kad kredit atau buat loan dengan bank tersebut.

KERANA ...

Bukan masalah anda jika ada orang guna identiti anda untuk buat pinjaman / kad kredit. Masalah bank yang luluskan.

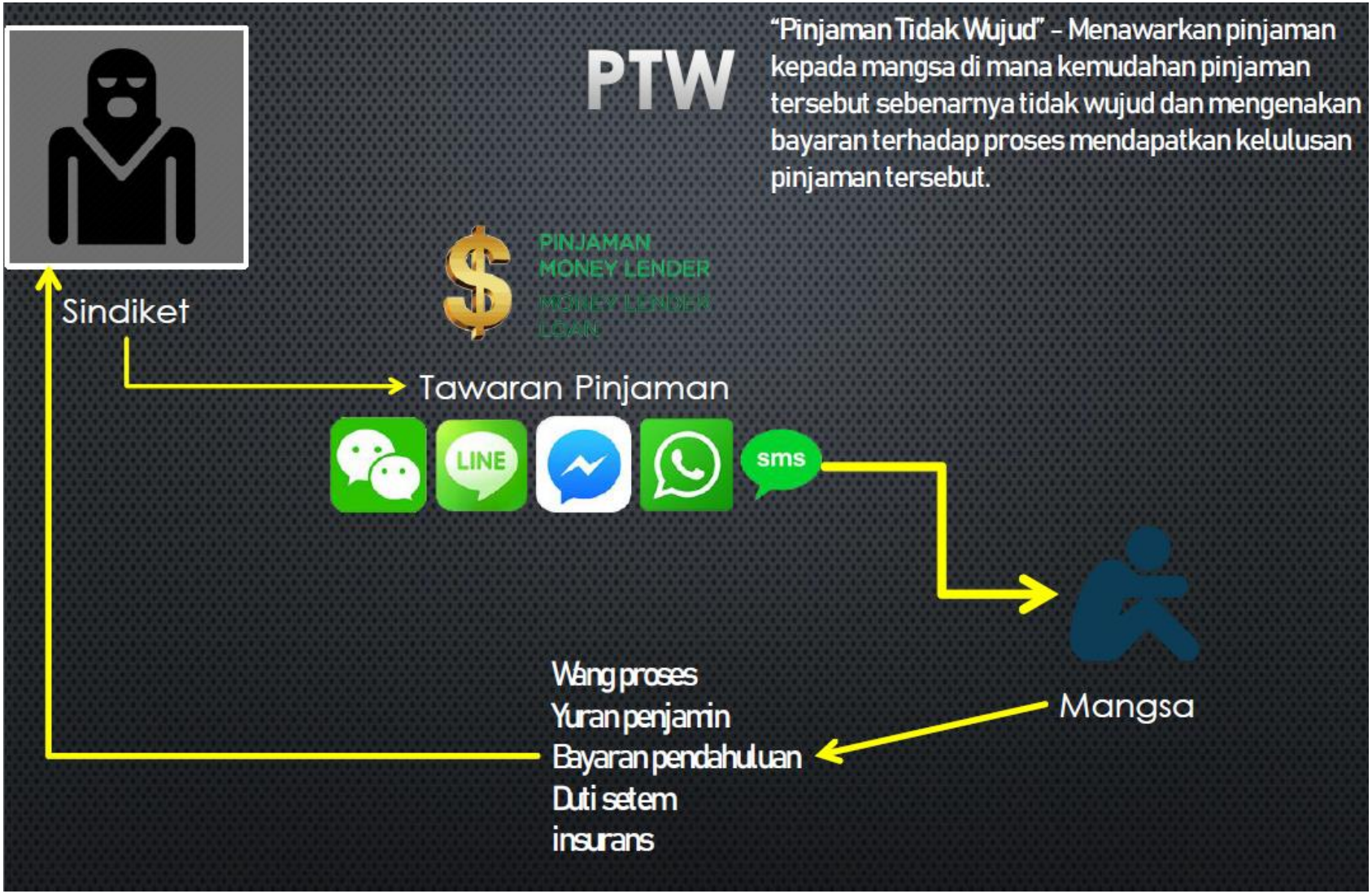
BERTINDAK ...

Matikan panggilan telefon.
Teruskan hidup dan berbanggalah kerana anda BIJAK.

‘Scam’ SMS


SCAM ALERT
TIPU SMS
hadiah
NESTLE
CELCOM
#BeSmart
PERNAH MENERIMA MESEJ INI ??
RM0.00 Tahniah...!!!
SimCard/Whatsapp anda Telah berjaya menangi wang tunai
RM18,000.00
from NESTLE (M)
No'Reff/Siri: "582547"
Pengesahan no reff/siri hadiah dan cara terima hadiah. Sila layari laman web..!!!
➞ http://peraduanmynestle.webs.com
Untuk keterangan lanjut. Sila hubungi pusat layanan Nestle Contest 2018 di*
WhatsApp Office
➞ https://wa.me/+601125274249*
Call Office
☎ +6011-5797-5657
Note: sila reply mesej ni untuk klik/ layari laman web
aduan NESTLÉ® 2018
Tahnia Kepada Pemenang utama...!!!
Wang Tunai RM18,000
* No.Ref : "475869" +6011 233XXXX
* No.Ref : "433477" +6013 350XXXX
* No.Ref : "582547" +6011 240XXXX
* No.Ref : "114477" +6011 335XXXX
* No.Ref : "255789" +6011 244XXXX
Tahnia Kepada Pemenang Kedua...!!!
Wang Tunai RM12,000
* No.Ref : "227799" +6011 216XXXX
* No.Ref : "099575" +6013 433XXXX
* No.Ref : "277769" +6013 456XXXX
* No.Ref : "335577" +6013 724XXXX
* No.Ref : "142434" +6011 313XXXX
Tahnia Kepada Pemenang Ketiga...!!!
Wang Tunai RM8,000
* No.Ref : "878787" +6019 851XXXX
MENYERTAI PERKHIDMATAN & PROMOSI INI ADALAH SANGAT MUDAH!
Butiran: Meriahkan sambutan Anda tahun ini dengan berbagai hadiah wang tunai yang ditawarkan. Sungguh mudah untuk menjadi pemenang, jom sertai sekarang!
Cara-cara penyertaan:
1. Pemenang NESTLE akan di hantarkan message WhatsApp untuk Nombor Reff pemenang Sila rujuk senarai yang turut serta melalui aplikasi WhatsApp.
2. Setiap Bukti Nombor Reff message Aplikasi WhatsApp HANYA layak untuk 1 penyertaan melalui WhatsApp sahaja.
Hantarkan Maklumat diri anda melalui Aplikasi WhatsApp:
Melalui Aplikasi WhatsApp Tuliskan nama penuh, nombor pengenalan dan Nombor Reff Pemenang, Bersama dengan nama bank, Gambar Kad Bank depan & belakang yang diguna, dengan lengkap dan jelas. Hantar Melalui WhatsApp ke +6011 2527 4249
Example:
No Reff : 2547XXX
Nama : Momaxxxxxx bin Ismaxxxx
No IC/Mykd : 72010xxxxx-No Ref : 23xxxx
Name bank : Bank Islam, CIMB, BSN, Bank Rakyat, RHB, Ambank, Muamalat. Etc
Gambar Kad Bank depan belakang
Tekan Nombo WhatsApp +6011 2527 4249 untuk isi Borang maklumat diri anda.
BANK ISLAM
VISA
ANDA TELAH MENDEDAHKAN MAKLUMAT DIRI ANDA DAN AKAUN BANK MILIK ANDA KEPADA SASPEK !!

Scam pinjaman tidak wujud



Contoh *scam* pinjaman tidak wujud

Pelajar ditipu RM12,580

Oleh Shahrinnahar Latib
news@nstp.com.my

PEKAN: Seorang pelajar institusi pengajian tinggi mendakwa kerugian RM12,580 akibat terperdaya dengan tawaran pinjaman oleh sebuah syarikat yang diiklan menerusi internet.

Kejadian bermula pada 22 Februari lalu apabila mangsa berusia 23 tahun yang berasal dari Taman Melor di sini, tertarik dengan iklan yang dipromosikan oleh syarikat terbabit.

Ketua Jabatan Siasatan Jenayah Komersial (JSJK) Pahang, Superintendan Mohd Wazir Mohd Yusof, berkata mangsa kemudian mengisi butir peribadi seperti nama, emel, nombor telefon, jenis pinjaman, gaji bersih, jumlah pinjaman dan alamat di laman sesawang berkenaan.

Syarikat terbabit kemudian menghantar emel balas dan mangsa menghubungi semula syarikat itu.

"Mangsa kemudian menerima pesanan menerusi ringkas WhatsApp daripada ejen syarikat pinjaman berkenaan.

"Selepas perbincangan melalui aplikasi WhatsApp, mangsa bersetuju membuat pinjaman peribadi RM10,000 dengan bayaran bulanan RM200 bagi tempoh 60 bulan," katanya ketika dihubungi, hari ini.

Berdasarkan perbincangan itu, mangsa diminta membayar RM11,580 untuk bayaran guaman, cukai barang dan perkhidmatan dan dokumentasi.

Mohd Wazir berkata, pada 24 Februari lalu, mangsa memasukkan wang tunai RM1,000 ke akaun sebuah bank sebagai deposit pinjaman.

Katanya, seterusnya mangsa membuat beberapa kali transaksi yang keseluruhannya berjumlah RM12,580 ke akaun yang sama sehingga kelmarin.

"Mangsa akhirnya sedar dia ditipu dan membuat laporan di Ibu Pejabat Polis Daerah (IPD) Pekan, semalam," katanya,

Sementara itu, dalam kes berasingan, seorang mekanik berputih mata kerugian RM6,950 selepas diperdaya sindiket yang menawarkan pinjaman wang yang tidak wujud di laman sosial Facebook, bulan lalu.

Mohd Wazir berkata, mangsa berusia 32 tahun berminat untuk membuat pinjaman wang selepas melihat iklan di FacebookIMoney pada 18 Jun lalu.

"Mangsa kemudiannya berhubung dengan ejen pemberi pinjaman berkenaan bernama Nick dan menyatakan mahu membuat pinjaman wang berjumlah RM25,000.

"Nick mengarahkannya membuat pembayaran wang bagi yuran memproses permohonan dan yuran peguam.

"Pada hari yang sama, mangsa memasukkan wang berjumlah RM6,950 ke akaun dalam akuan CIMB yang diberikan oleh suspek. Setelah memasukkan wang itu, mangsa berasa ditipu dan membuat laporan polis di IPD Kuantan, kelmarin," katanya.

Beliau berkata, kedua-dua kes ini disiasat mengikut Seksyen 420 Kanun Keseksaan kerana menipu, yang memperuntukkan hukuman penjara maksimum 10 tahun dan sebat, serta boleh dikenakan denda jika sabit kesalahan.

Scam pembelian dalam talian

PENIPUAN BELIAN ATAS TALIAN (ELECTRONIC PURCHASE)

mudah.my Malaysia's Largest Marketplace
Alibaba.com
carousell

Laman Sesawang Jualan

Pembeli

Penjual

- Talian telefon
- Email
- IP Address
- Akaun Bank

- Kerugian wang
- Kehilangan barangan
- Identiti / akaun perbankan digunakan
- Pencerobohan akaun portal (hilang kredit / wang)
- Menjadi keldai akaun penjenayah lain

Contoh penipuan jual beli internet

PETALING JAYA: Kes penipuan di internet bagai tiada penghujungnya apabila kumpulan-kumpulan penipu terus menyasarkan laman-laman popular jualan barangan dalam talian untuk mencari mangsa.

Jika sebelum ini penjual sering dikaitkan sebagai penipu, namun trend itu telah bertukar apabila pembeli pula dikesan menipu di laman web jualan barangan dalam talian.

Penyangak dalam talian ini dilihat semakin berani apabila mereka menggunakan pendekatan yang lebih mesra, iaitu berurusan secara langsung dengan peniaga melalui telefon, menjadikan peniaga yang diumpan lebih yakin dengan mereka.

Modus operandinya cukup mudah iaitu dengan menghubungi mana-mana individu yang mengiklankan barangan yang ingin dijual dalam talian dan berpura-pura menjadi pembeli yang kononnya sangat berminat dengan barangan yang diiklankan.

Bagi memastikan mangsa lebih cepat masuk ke perangkap yang dipasang, penyangak tersebut sanggup menawarkan bayaran yang lebih tinggi daripada harga asal.

Seorang pengiklan yang enggan dikenali berkata, dia terkejut apabila dihubungi seorang 'pembeli segera' selepas tidak sampai lima minit mengiklankan kamera yang ingin dijualnya di sebuah laman jualan barang popular di negara ini.

"Tidak sampai lima minit, seseorang kononnya dari UK (United Kingdom) menghubungi saya melalui 'WatsApp' menyatakan minat untuk membeli kamera yang saya iklankan. Katanya dia mahu menghadiahkan kamera itu untuk sepupunya di Amerika Syarikat.

"Saya macam terpukau...ikutkan hati memang saya nak jual sangat kamera tu, tapi atas nasihat kawan-kawan, saya tidak segera menjualnya.

"Dia di UK dan nak belikan untuk sepupu di AS. Itu sudah membuatkan saya curiga. Kenapa mahu beli dari Malaysia?

"Lagipun dia tak banyak bertanya tentang kamera saya, tetapi terus mahu beli siap tawar untuk tambah RM300 untuk bayar 'Poslaju' ke AS. Bagaimana pula dia tahu tentang Poslaju?," katanya kepada mStar Online baru-baru ini.

Antara salinan perbualan mangsa dengan individu yang didakwa cuba menipu untuk membeli sebuah kamera.

Lebih membuatkan penjual kamera itu bimbang apabila pembeli berkenaan seolah-olah tergesa-gesa meminta maklumat tentang dirinya seperti nama penuh, nombor akaun bank dan butiran lain.

Kes #1

Seorang lagi mangsa yang pernah ditipu empat tahun lalu terkejut apabila taktik penipuan itu semakin berjaya memperdaya penjual barangan dalam talian.

Katanya, dia mengalami kerugian kira-kira RM2,000 gara-gara ditipu individu yang kononnya mahu membeli barang untuk sepupunya di Nigeria.

"Dia beritahu sudah masukkan duit ke dalam bank tetapi duit ditahan oleh pihak bank yang mahukan resit penghantaran item sebagai bukti. Saya percaya kerana memang saya terima emel yang dihantar oleh bank kepada saya.

"Jadi saya pergi pos barang yang saya jual, tetapi sekali lagi dia minta bayaran RM1,000 dengan alasan tertentu. Akibatnya saya kerugian lebih kurang RM2,000 berserta barang saya," katanya sambil mengakui bertindak terburu-buru ketika itu.

Seorang lelaki yang deknali sebagai Hasan pula nyaris menjadi mangsa penipuan apabila kereta yang diiklankan di internet untuk dijual mendapat pembeli dari luar negara yang sanggup membayar dengan harga lebih tinggi.

"Kami berurus niaga guna Paypal. Saya bernasib baik sebab apabila saya pergi bank untuk kesan nombor paypal itu mendapati ia merupakan maklumat palsu dan tidak wujud dalam sistem syarikat berkenaan," katanya.

Kes #2

Mengulas mengenai perkara ini, Penolong Pengarah Jenayah Siber dan Multimedia Jabatan Siasatan Jenayah Komersial Bukit Aman Asisten Komisioner Kamaruddin Md Din berkata, selain pembeli terdapat banyak laporan penipuan daripada penjual.

Katanya, siasatan mendapati kebanyakan mereka sebenarnya hanya mahu mendapatkan maklumat untuk menipu peniaga atau pihak ketiga dengan
teknik 'phishing'.

"Saya menasihatkan orang ramai yang sering menjalankan urusniaga jualan di internet supaya berhati-hati dengan sesiapa sahaja, sama ada peniaga atau pembeli yang mencurigakan.

"Seboleh-bolehnya bayaran biarlah dibuat secara COD (cash on delivery)," katanya.

Pengerusi Tribunal Tuntutan Pengguna Malaysia Reihana Abd Razak berkata, dalam kes peniaga yang ditipu pembeli, mereka perlu membuat tuntutan di Mahkamah Sivil.

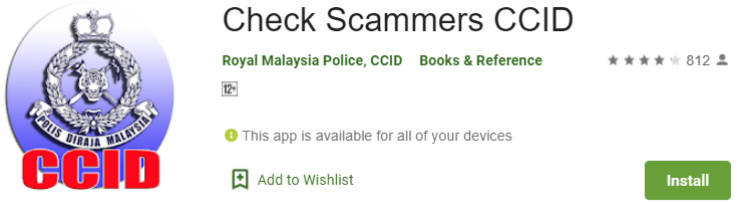
"Jika mereka datang kepada kita, pihak tribunal nasihatkan mangsa supaya memfailkan tuntutan mereka di Mahkamah Sivil.

"Itulah satu-satunya saluran yang boleh digunakan peniaga yang mendakwa mereka ditipu," katanya.

Semak akaun yang telah dilaporkan sebagai *scam*

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

Aplikasi oleh PDRM



Penipuan *phishing*

- Phishing adalah jenayah siber di mana mangsa dihubungi melalui email, telefon, atau mesej teks oleh individu yang menyamar sebagai sebuah institusi yang sah untuk mengumpan mangsa supaya memberikan data peribadi seperti maklumat peribadi, perincian perbankan atau kad kredit, dan kata laluan.

- Maklumat tersebut kemudiannya digunakan untuk mengakses akaun penting dan boleh mengakibatkan kecurian identiti dan kerugian kewangan.

Ciri-ciri yang selalu terdapat pada medium phishing

- Terlalu hebat untuk dipercayai
- Mendesak/ Menggesa
- *Hyperlinks*
- Lampiran
- Penghantar yang tidak dikenali/ disangka

Contoh emel *phishing*

From: Bank Negara Malaysia

To: Undisclosed, recipients:

Subject: Incoming payment (Action Required)

Attachment: BNMNOTICE.pdf , 146.6 KBytes

You have a credit instruction for an incoming payment. As our security precaution, all payments above Ten Thousand Ringitt (RM 10,000), require extra verification from Bank Negara Malaysia.

Kindly download the attachment to complete the verification and receive this payment.

Thank you
Bank Negara Malaysia

-----Original Message-----
From: Bank Negara [mailto:tonya.r.durant@vanderbilt.edu]
Sent: 10 October, 2016 9:31 AM
To: Undisclosed recipients:
Subject: Important notice - Incoming funds on hold

Important message regarding an incoming payment to your account.

Download the attachment to view details.

Thank you
Bank Negara Malaysia

BNM.pdf (1 page)

Bank Negara

PHISHING EMAIL

BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Dear Customer,

You have a pending payment slated on your account. Additional security verification is required to complete this transaction.

In order to resolve this issue and receive the payment, follow the reference below

Follow the reference below to proceed

Click Here

Regards,
Bank Negara Malaysia

From: Inland Revenue Board Malaysia [mailto:taxrefunds@hasil.gov.my]
Sent: 11 August 2010 14:55
To: undisclosed-recipients
Subject: Tax Refunds Notification

Tax Refund Notification

After the calculations of your fiscal activity of the first quarter of 2010, we have determined that you are eligible to receive a tax refund of 2812.49 MYR. Please submit the tax refund request and allow 10-14 days in order to process it.Click on your bank link below

Click www.maybank2u.com.my to submit your tax refund request

Note : A refund can be delayed a variety of reasons, for example submitting invalid records or applying after deadline.

Yours Sincerely

Inland Revenue Board Malaysia.

LHDN

PHISHING EMAIL

http://www.pharmashoponline.com/pub/IRBM/www.maybank2u.com/Index.htm

LHDN
MALAYSIA

Dear Valued Taxpayer,

Please be informed that the INLAND REVENUE BOARD OF MALAYSIA has concluded the account audit for the previous tax quarter and after a critical review of your tax column you are qualified for an income tax refund of [redacted] which is your accumulated tax excesses till date.

Kindly click below to submit a refund request to enable us process and remit your refunds into your bank account.

Submit Request

Note: Mobile verification is a mandatory security exercise to protect you against tax refund fraud, kindly complete the same for your security.

You are adviced to complete the request carefully to avoid any delay in the payment of your refunds as the same may be delayed if you:

- Fail to verify your mobile number **AND/OR**
- Submit inaccurate/incomplete account information.

Attention: If you have received this email in your spam folder, mark it as "Not spam" in other to complete request.

Contoh emel *phishing*

Maybank

We are hereby notifying you that we've recently suffered a DDos-Attack on one of our's Online Banking server. For security reasons you must complete the next steps to verify the integrity of your Maybank account. If you fail to complete the verification in the next 24 hours your account will be suspended.

Here's how to get started:

1. Log in to **Maybank** online account **(click here)**.

2. You must request for TAC via **Maybank online banking** - your TAC will be sent via SMS to the mobile phone number you registered.
(you can find the "**Request a TAC**" button in the Utilities menu of your account)

3. Logout from your account and close the browser.

4. When you have received the **TAC (Transaction Authorization Code)** on your mobile phone, **go to our secured verification server** and submit the requested information (Username, password and TAC). **(click here) to go on our secured server.**

5. Please allow 48 hours for processing.

Please comply and thanks for understanding.

Maybank

PHISHING EMAIL

Subject: Final Notification

Greetings from Maybank2u!

Due to the new enhanced security program that was installed on our server, our customers can now perform daily online transactions with peace of mind knowing of there private finanacial information is well protected.

Please visit the Maybank2u website in this message and validate your details on our new security server.

Log on to www.maybank2u.com to complete the validation process.

P.S. The Link in this message will expire within 24 hours. **TAC** will be required during update.

Thank you & have a good day ahead!

Warm Regards,

Maybank2u Team

FRAUDULENT

citi

CitiBank

PHISHING EMAIL

Dear CitiBank customer,

Recently there have been a large number of identity theft attempts targeting CitiBank customers. In order to safeguard your account, we require that you confirm your banking details.

This process is mandatory, and if not completed within the nearest time your account may be subject to temporary suspension.

To securely confirm your Citibank account details please go to:

https://web.da-us.citibank.com/signin/scripts/login/user_setup.jsp

Thank you for your prompt attention to this matter and thank you for using CitiBank!

Citi® Identity Theft Solutions

Do not reply to this email as it is an unmonitored alias

A member of citigroup

Copyright © 2004 Citicorp

OCBC Online Banking

Hi Valued Customer,

Did you know we offer SMS security for OCBC Online Banking?

It's another way we can protect you online by texting a unique code for authorizing funds transfers, resetting your passwords or changing your details.

Get notified when:

- Login alert from unauthorized location
- Fund Transfer alert
- Change of password

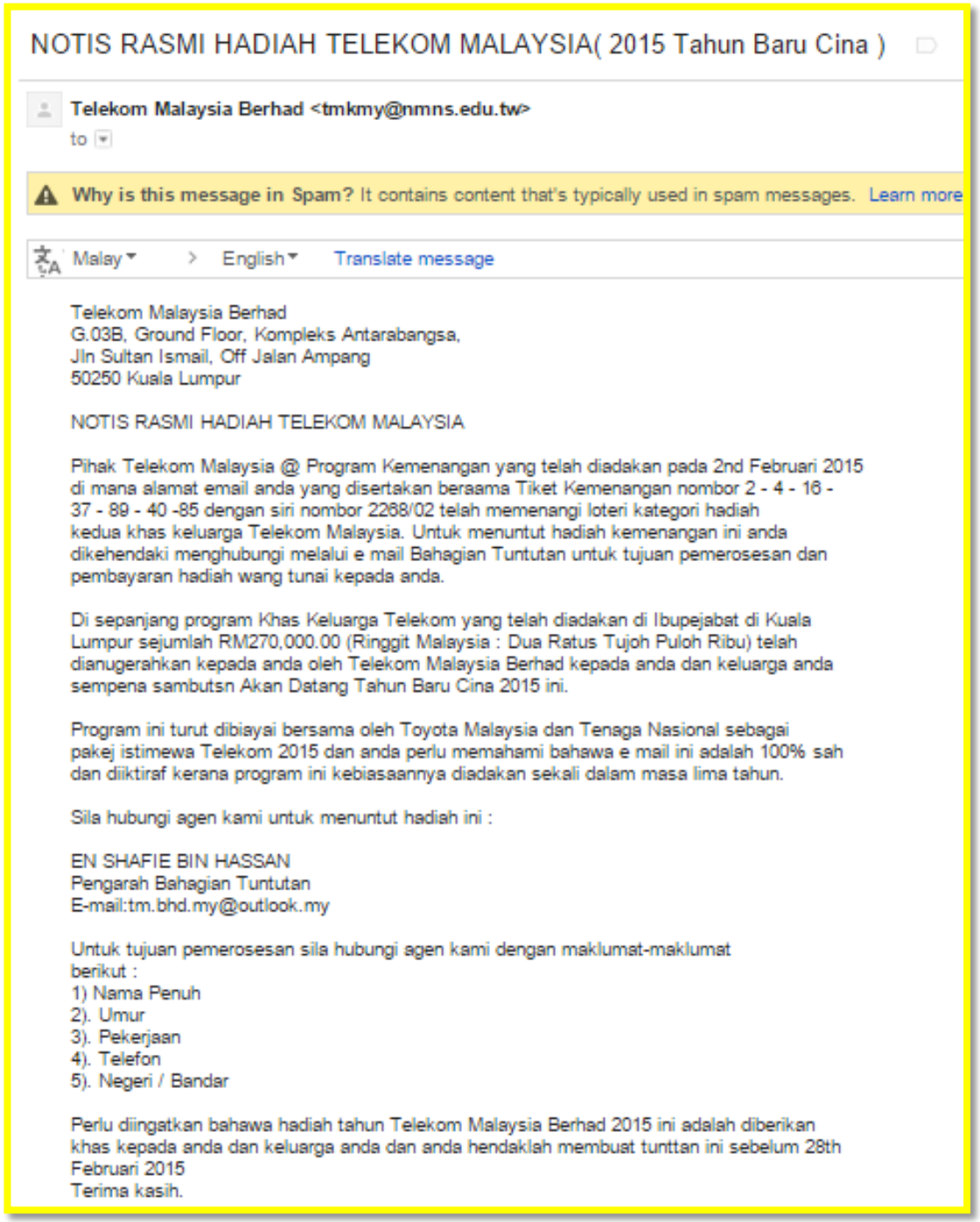
Register for SMS Security now – it only takes a couple of minutes to set up.

Kind Regards,
OCBC Bank

OCBC

PHISHING EMAIL

This is an example of a phishing email.
Note: this email is not sent by OCBC Bank



NOTIS RASMI HADIAH TELEKOM MALAYSIA(2015 Tahun Baru Cina)

Telekom Malaysia Berhad <tmkmy@nmns.edu.tw>
to

Why is this message in Spam? It contains content that's typically used in spam messages. Learn more

Malay > English Translate message

Telekom Malaysia Berhad
G.03B, Ground Floor, Kompleks Antarabangsa,
Jln Sultan Ismail, Off Jalan Ampang
50250 Kuala Lumpur

NOTIS RASMI HADIAH TELEKOM MALAYSIA

Pihak Telekom Malaysia @ Program Kemenangan yang telah diadakan pada 2nd Februari 2015 di mana alamat email anda yang disertakan beraama Tiket Kemenangan nombor 2 - 4 - 16 - 37 - 89 - 40 -85 dengan siri nombor 2268/02 telah memenangi loteri kategori hadiah kedua khas keluarga Telekom Malaysia. Untuk menuntut hadiah kemenangan ini anda dikehendaki menghubungi melalui e mail Bahagian Tuntutan untuk tujuan pemerosesan dan pembayaran hadiah wang tunai kepada anda.

Di sepanjang program Khas Keluarga Telekom yang telah diadakan di Ibupejabat di Kuala Lumpur sejumlah RM270,000.00 (Ringgit Malaysia : Dua Ratus Tujoh Puloh Ribu) telah dianugerahkan kepada anda oleh Telekom Malaysia Berhad kepada anda dan keluarga anda sempena sambutsn Akan Datang Tahun Baru Cina 2015 ini.

Program ini turut dibiayai bersama oleh Toyota Malaysia dan Tenaga Nasional sebagai pakej istimewa Telekom 2015 dan anda perlu memahami bahawa e mail ini adalah 100% sah dan diiktiraf kerana program ini kebiasaannya diadakan sekali dalam masa lima tahun.

Sila hubungi agen kami untuk menuntut hadiah ini :

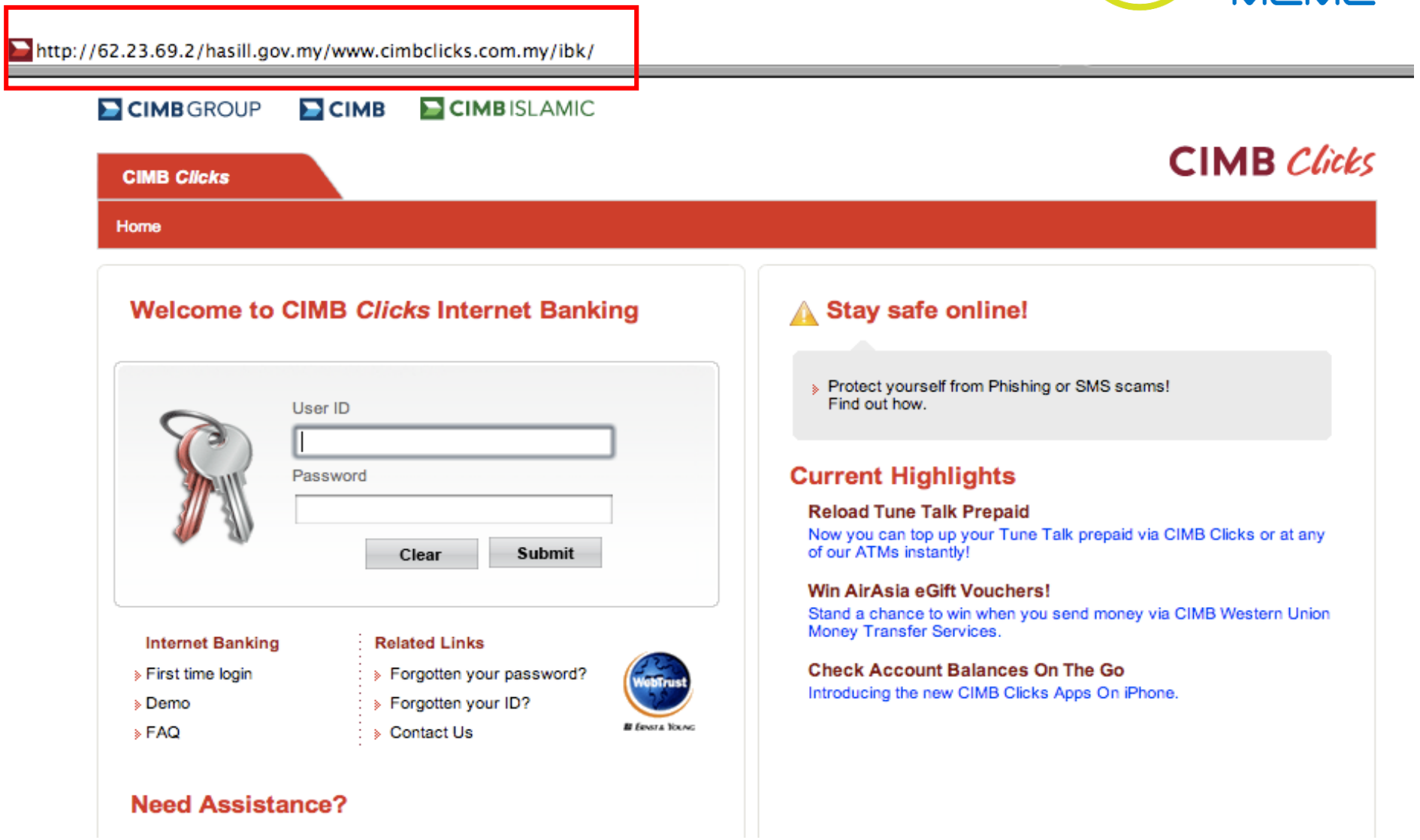
EN SHAFIE BIN HASSAN
Pengarah Bahagian Tuntutan
E-mail:tm.bhd.my@outlook.my

Untuk tujuan pemerosesan sila hubungi agen kami dengan maklumat-maklumat berikut :
1) Nama Penuh
2). Umur
3). Pekerjaan
4). Telefon
5). Negeri / Bandar

Perlu diingatkan bahawa hadiah tahun Telekom Malaysia Berhad 2015 ini adalah diberikan khas kepada anda dan keluarga anda dan anda hendaklah membuat tunttan ini sebelum 28th Februari 2015
Terima kasih.

Contoh emel *phishing*- Ganjaran wang

Contoh laman *phishing* bank



Sebaran penipuan *phishing* melalui media sosial

"KFC Giveaway - Ramadan RM200 free vouchers"

"KFC Women's Day win a KFC's Family Feast Bucket"

"KFC birthday/anniversary celebration - KFC offers 3000 Family barrels / Snack Buckets for everyone"

"8x / 3x Snack Plate Combo only RM 20 for 30th Feb 2020"

"We're looking for people born in [month]! ...to win $500 KFC Vouchers"

"KFC Pertandingan, menangi RM 2,000 KFC Baucar"

"Get 3 free big meals from KFC on occasion of its birthday/anniversary"

- http://kfc.com-cc.com
- http://m6ae.com/kfc
- http://kfc.com-oc.com
- http://meal.freecoupons.xyz
- 3bigmeals.com-oc.com
- http://www.kfc-box.club/
- https://kfc-vip.vip/kfc/?th=kfcen

KFC's version of Sebenarnya.my
https://dinein.kfc.com.my/scam-alert

Phishing- Kecurian identiti

Jangan Jadi Mangsa Curi Identiti

Diterbitkan: Khamis, 2 November 2017 10:20 AM

Oleh: YUEN MEI KING
editor@mstar.com.my

Gambar hiasan.

(Ubah saiz teks)

PETALING JAYA: Dia berkelakuan pelik apabila menambah semua kenalan di akaun baharu Facebooknya dan meminta wang daripada mereka.
Mendakwa kehilangan telefon, dia turut meminta nombor telefon semua orang.

Bagaimanapun bukan dia yang berkelakuan pelik itu.

Seorang eksekutif syarikat berumur 30an, Kam, menjadi mangsa pencuri identiti yang membuat akaun palsu menggunakan nama dan gambarnya.

Setelah membuat pemeriksaan di tetapan keselamatan Facebook, dia mendapati penjenayah siber itu berjaya mengakses akaun peribadinya.

"Mengikut rekod (history) di Facebook, terdapat peranti tidak dikenali mendaftar masuk ke akaun saya dari lokasi lain.

"Selepas menyedari ada sesuatu yang tidak kena, kawan-kawan terus menghubungi saya.

"Mereka juga berhenti membalas mesej di Facebook apabila dia mula meminta wang," ujar Kam.

Tambah Kam, dia terus menukar kata laluan Facebook selepas menyedari perkara tersebut.

Kam merupakan salah satu contoh kes kecurian identiti yang semakin berleluasa.

Insiden kecurian identiti yang mana maklumat peribadi mangsa dicuri dan diekspolitasi meningkat sebanyak 16 peratus daripada 220 kes pada 2015 kepada 255 kes pada tahun lalu.

Sebanyak 262 kes telah dilaporkan kepada CyberSecurity Malaysia (CSM) dari Januari hingga September tahun ini.

Nama penuh, nombor kad pengenalan, tarikh lahir, nombor akaun bank, alamat e-mel, nombor telefon, alamat rumah dan tempat kerja merupakan antara data yang sering dicuri.

Pencuri identiti akan menggunakan data tersebut untuk menyamar sebagai mangsa, membuat pinjaman, membeli barangan mewah, memalsukan kad kredit, membuat penipuan atas talian dan memindahkan wang daripada akaun yang disasarkan.

"Ada juga yang menggunakan data-data berkenaan untuk aktiviti di laman web 'gelap' bagi menyembunyikan identiti sebenar mereka," ujar Ketua Pegawai Eksekutif CSM, Datuk Dr Amirudin Abdul Wahab kepada *The Star*.

Katanya, maklumat peribadi mangsa turut dijual di pasaran gelap.

Menurutnya lagi, pencuri identiti biasanya mencuri maklumat mangsa dengan membuat panggilan palsu dan juga dengan pendekatan kejuruteraan sosial.

"Mereka menyamar sebagai agensi penguatkuasa, syarikat telekomunikasi atau bank, dan mendakwa mangsa mempunyai isu yang perlu diselesaikan.

"Selepas itu mereka akan mengugut atau menakutkan mangsa bagi mendapatkan maklumat peribadi.

Menurut Amirudin, laman web yang menggunakan kata laluan mudah adalah yang paling berisiko untuk diakses oleh penjenayah siber.

Dalam pada itu, beliau turut menasihatkan agar orang ramai mengurangkan perkongsian maklumat peribadi di media sosial.

Tambahnya lagi, pengguna seharusnya memantau siapa yang boleh melihat aktiviti mereka di laman sosial.

"Tetapkan mod sulit (private) bagi akaun anda dan tambah kenalan yang dikenali sahaja," ujarnya.

Peningkatan kes sedemikian berlaku susulan dakwaan kecurian data melibatkan nombor telefon di Malaysia sebelum ini.

Insiden itu dilaporkan berlaku pada 2014 menerusi portal dalam talian *lowyat.net*.

Susulan kejadian melibatkan 46.2 juta nombor telefon itu, Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) dilaporkan telah berjumpa dengan syarikat telekomunikasi dan masih lagi menyiasat mengenai kes berkenaan.

Bagi mengelakkan kes sedemikian, pengguna dinasihatkan supaya menggunakan kata laluan berbeza bagi setiap akaun.

Mereka juga perlu mengaktifkan fungsi yang menambah lapisan keselamatan bagi melindungi akaun atas talian mereka.

Phishing- Kecurian identiti

Berhati-hati risiko kecurian identiti

29 JULAI 2016

Facebook Twitter WhatsApp Email More 2.7K

Berhati-hati risiko kecurian identiti

A- A+ (Ubah saiz teks)

PADA mulanya Manan (bukan nama sebenar) tidak ambil kisah apabila kawan-kawannya bercerita tentang RAM Credit Information Sdn Bhd (RAMCI), agensi rujukan kredit yang tidak asing lagi di negara ini.

Syarikat itu secara kebetulan mengadakan kempen kesedaran akan pentingnya laporan kredit di tempat kerja Manan di Ipoh.

Pengawal keselamatan berusia pertengahan 20an itu berasakan tidak perlu untuk menyemak laporan hutangnya sehinggalah kawan-kawannya menyakinkan Manan supaya berbuat demikian.

Lagi pun perkhidmatan yang ditawarkan oleh RAMCI adalah percuma.

Nasib baik pengawal keselamatan itu akur dengan cakap kawan-kawannya.

Apabila disemak, Manan mendapati ada permohonan pinjaman bank atas namanya untuk jumlah RM10,000 dan permohonan itu sedang dalam proses untuk diluluskan.

Manan terkejut kerana tidak pernah membuat permohonan pinjaman itu!

Beliau bernasib baik kerana masih sempat menghubungi bank berkenaan supaya membatalkan permohonan pinjaman itu sebelum wang itu diserah kepada individu yang tidak dikenali.

BUKAN KEJADIAN TERPENCIL

Satu lagi contoh kes yang melibatkan kecurian identiti melibatkan En Ng (bukan nama sebenar) berusia 33 tahun dari Kota Bharu.

Beliau tidak pernah tahu tentang kecurian identiti ini sehingga menjadi mangsa penipuan licik ini.

Semuanya bermula apabila Ng menerima notis daripada syarikat peruncit elektronik dan perabot yang mengingatkan tunggakan bayaran untuk empat barang yang dibelinya berjumlah kira-kira RM11,200.

Ng segera membuat laporan polis dan berjumpa dengan peruncit itu untuk mendapatkan maklumat pembelian itu.

Beliau diberitahu maklumat itu akan hanya dikeluarkan dalam laporan hutang. Apabila beliau menghubungi RAMCI untuk mendapatkan laporan itu, beliau diberitahu maklumat tunggakan bayaran itu akan hanya dikeluarkan selepas siasatan ke atas kes itu selesai.

KEJADIAN KECURIAN IDENTITI

Dua kes kecurian identiti itu adalah antara contoh yang dikongsi dengan penulis dalam wawancara dengan RAMCI baru-baru ini.

Agensi itu juga berkongsi hasil tinjauan yang julung-julung kali dijalankan berkait dengan kes kecurian identiti.

Antara hasil tinjauan ialah 14 peratus responden pernah mengalami kes kecurian identiti sementara 26 peratus lagi kenal seseorang yang pernah menjadi mangsa.

Ketua Pegawai Eksekutif RAMCI, Dawn Lai menyifatkan hasil tinjauan itu sebagai membimbangkan dan orang ramai perlu memandang serius kes itu.

"Rakyat Malaysia semakin terdedah kepada kecurian identiti. Dengan perkembangan pesat internet, semakin ramai membuat pembelian dalam talian. Ini membuka jalan untuk kes curi identiti," jelas Lai.

Antara kaedah yang digunakan untuk mencuri identiti ini ialah dengan MyKad yang dicuri, kehilangan dokumen peribadi yang dipos serta secara tidak sedar memberi maklumat peribadi apabila menerima panggilan telefon atau emel palsu.

"Apa yang perlu ialah sikap berhati-hati apabila membuat pembelian dalam talian dan menjaga rapi maklumat peribadi.

"Jangan guna kata laluan yang mudah atau menggunakan kata laluan yang sama untuk semua akaun. Catat sebarang urus niaga dalam talian, syarikat yang anda buat urus niaga itu dan pastikan laman sesawang itu selamat," tegas Lai.

KERUGIAN KEWANGAN BESAR

Menurut Lai, lazimnya kecurian dikaitkan dengan rompakan fizikal yang melibatkan kehilangan harta benda.

Bagaimanapun, kecurian identiti boleh mendatangkan musibah besar.

Tambah beliau, dalam sesetengah kes, wang pinjaman sudah dikeluarkan dan mangsa terpaksa membayar pinjaman sementara menunggu kes diselesaikan.

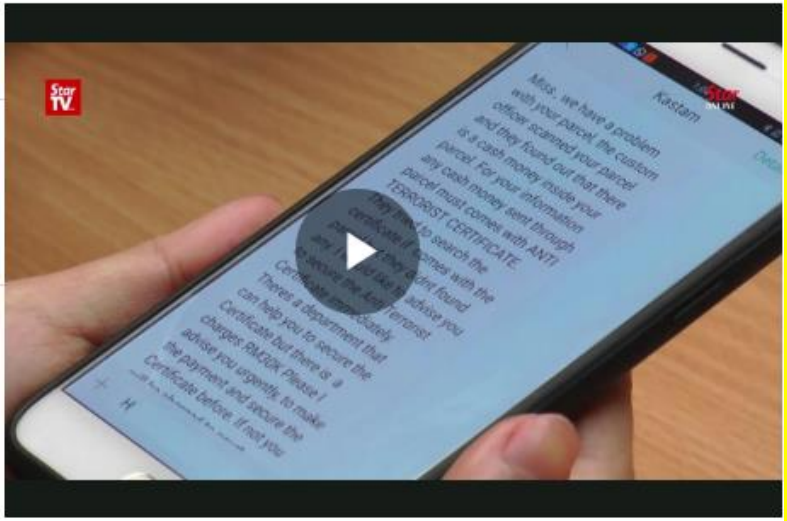
Langkah ini bagi mengelakkan kedudukan kredit mereka terjejas atau nama mereka disenaraihitamkan.

Bentuk penipuan yang lain

Woman cheated of RM135,000 in parcel scam

NATION

Thursday, 21 Dec 2017



KUALA LUMPUR: Parcel scams continue to haunt Malaysians as yet another person falls for the con, being cheated out of RM135,000.

This time, the victim, known only as Cheah, said she had first gotten to know a man – Tsung James – online after he messaged her on social media on the pretext of striking up a friendship.

Cheah, who started talking to Tsung on Dec 5, said after a few days, he told her that he was sending a parcel to her as a Christmas gift.

"He told me: 'I am buying a present for my mother. So, I want to buy you a gift as well.'

"I didn't think anything of it. I let him send it," she told reporters at a press conference called by MCA Public Services and Complaints Department head Datuk Seri Michael Chong here yesterday.

She claimed that Tsung had told her that among the contents of the parcel were a laptop, an iPhone 8 Plus, bottles of perfume and a Louis Vuitton bag.

Scam tawaran pekerjaan

** Manual To Get Started **

Welcome To [redacted]

"How To Make RM 30 For Every Email You Process And Get Paid Weekly"

You can just imagine how nice to get an income from home doing simple email processing and get paid RM 30.00 per email you process. There is NO limitations to the amount of emails you process and your potential income is unlimited. You can work at your Own Pace & choose your Own Time. It takes just few minutes to process each email. This is an income opportunity you can take advantage of and make Good Money from the comfort of your own home.

Step 1: Post Job Advertisement

You can start posting job advertisement at [redacted] (most recommend as simple step involve), Facebook, Yahoo, Twitter or any social networking sites/groups, etc. If you do not know where to start, try to Google Search for "free ads posting", "free job posting sites" etc.

Samples of Free Posting Website:-

** [redacted]

MALAYSIA

M'sian Student Shares How She Applied for Typing Job Via FB and Got Scammed

Published 9 months ago on December 21, 2017
By Ling Kwan

Source: Oriental Daily

[redacted]
[redacted]
April 14 at 9:30pm

RM 300-800 Per Week: Home Based Data Entry Typists ~
Genuine Work-From-Home Employment Opportunity To Earn Extra Income.
You only need to: -
(1) Advertise & process customer data that is sent via email.
(2) Working from home, cyber cafe, offices, colleges, and others.
(3) Any time (set your own time schedule).
Requirements:
* Aged 16 years and above
* Basic knowledge of computer (typing, Internet, email, etc.)
* No prior experience necessary
*Can work according to the instructions / guidelines

SCAM??

FAKTOR UTAMA MENJADI MANGSA PENIPUAN DALAM TALIAN

Keadaan Hidup

- Rasa terpinggir/kesunyian
- Hilang pekerjaan
- Perubahan negatif dalam status kewangan
- Bimbang tentang hutang

Sumber: AARP Survey of American Adults, 2014

Pengetahuan

- Tidak tahu bahawa bank tidak menghantar e-mel kepada pelanggan untuk meminta mereka mengklik pautan bagi tujuan pengesahan maklumat peribadi
- Tidak tahu bahawa sesebuah laman web boleh berkongsi maklumat yang diperolehinya dengan pihak ketiga walaupun mempunyai dasar privasi.

Tingkah Laku

- Melayari laman web yang menghendaki pengunjung membaca dasar privasi dan syarat perjanjian
- Membuka e-mel daripada sumber yang tidak dikenali
- Menjual produk di laman lelong dalam talian
- Membuat pembelian menerusi laman pemindahan bayaran dalam talian
- Mendaftar untuk tawaran percubaan masa terhad percuma
- Memuat turun aplikasi
- Mengklik pada iklan timbul (*pop-up*)
- Sikap terburu-buru

Apa yang anda perlu lakukan ? 1/3

1. Gunakan **kata laluan yang unik, bijak, dan selamat** untuk semua akaun dalam talian (perbankan, media sosial, beli belah dalam talian, dlln.)
2. **Jangan klik** apa-apa pautan atau iklan yang menawarkan sesuatu yang terlalu bagus.
3. **Jangan klik lampiran dalam emel** atau membuka pautan dalam kandungan emel yang tidak disangka penerimaannya. Padam atau abaikan e-mel yang mencurigakan. Jangan balas emel tersebut.
4. **Laporkan** mesej atau emel sebagai spam kepada penyedia perkhidmatan atau jabatan yang mengendalikan rangkaian Internet di pejabat anda.
5. **Jangan hantar duit atau dokumen** berkenaan maklumat peribadi, walaupun salinan.
6. **Jangan beri apa-apa maklumat** melalui panggilan telefon. Tamatkan panggilan tersebut.

Sumber: INTERPOL/ SCAN Institute/ Norton

Apa yang anda perlu lakukan ? 2/3

1. **Jangan berikan maklumat akaun atau kad bank** (contoh: kad kredit atau debit). Jangan kongsi maklumat kad ATM.
2. **Taip URL perbankan** di dalam pelayar atau jadikan ia *bookmark* atau *favorite*.
3. **Jangan tertipu** dengan logo dan lamanweb yang serupa dengan yang asal.
4. **Pantau akaun kewangan anda.** Perhatikan jika ada transaksi yang mencurigakan seperti pembayaran yang mempunyai rujukan “test”. Ia salah satu taktik penjenayah siber.
5. Jangan akses perbankan dalam talian semasa menggunakan **Wi-fi awam atau di kafe siber.**
6. Pastikan URL sesuatu laman web yang anda layari mempunyai “https” di awalannya dan ikon mangga berkunci, terutamanya bank.
7. Gunakan versi **pelayar web terkini.**

Sumber: INTERPOL/ SCAN Institute/ Norton

Apa yang perlu anda lakukan? 3/3

1. **Telefon nombor awam atau khidmat pelanggan** syarikat yang mengatakan anda telah memenangi sesuatu daripada mereka. Selalunya pusat khidmat pelanggan akan tahu jika syarikat mereka menawarkan sesuatu untuk dimenangi.
2. **Tamatkan hubungan dengan suspek! Jangan cuba balas dendam.**
3. **Kumpulkan maklumat/ bukti** – emel, chat, resit dsb.
4. **Laporkan** suspek kepada admin laman-laman yang bertanggungjawab- laman *online dating,* membeli belah, perkhidmatan e-mel- atau pihak berkuasa yang berkaitan (seperti PDRM, KPDNHEP, Bank Negara Malaysia).
5. Sentiasa **kemas kini pengetahuan** mengenai keselamatan dalam talian, terutamanya penipuan dalam talian. Rujuk kepada media sosial Jabatan Siasatan Jenayah Siber PDRM.

Sumber: INTERPOL/ SCAN Institute/ Norton

Kesimpulan

Berhati hati sebelum terkena.
Jika tawarannya terlalu lumayan, periksa dahulu sebelum klik!

KEGANASAN SIBER

Keganasan siber

Definisi

Perbuatan jenayah yang bertujuan menimbulkan ketakutan orang awam, kumpulan individu atau individu tertentu, dilakukan demi mencapai matlamat politik dan perbuatan ini dalam apa jua keadaan adalah salah walau apa pun pertimbangan politik, falsafah, idealogi, kaum, etnik, agama dan alasan lain untuk mewajarkan tindakan mereka.

Contoh kumpulan pengganas

Ku Klux Klan (AS), National Action (UK),
Aum Shinrikyo (Jepun), Lord's Resistance Army (Uganda), Real IRA (Ireland, UK), Al Qaeda, Al Shahab (Somalia), Hezbollah (Lebanon), Boko Haram (Nigeria),
Lashkar-e-Taiba (Pakistan), dan ISIS/Daesh.

National Action

Boko haram

Ku Klux Klan

Taliban

Aum Shinrikyo

Kenapa kumpulan pengganas menggunakan Internet dan media sosial ?

- Sebagai provokasi melalui penghantaran amaran video
- Pengambilan penyokong yang berpotensi dari luar kawasan pangkalan (dunia tanpa sempadan)
- Merancang jadual protes, untuk penyelarasan, memberitahu dunia
- Mesej dari media sosial cepat tersebar di kalangan radikal berbanding usaha mereka untuk mencari maklumat di Internet
- Murah dan senang dicapai, mempermudahkan penyebaran mesej secara meluas dan membolehkan komunikasi tanpa batasan
- Platform interaksi dengan kumpulan sasaran untuk menyebarkan mesej/ rangkaian kumpulan dalam masa nyata (segera) (video, penyataan)
- Tayangan serangan secara “Live” lebih mempunyai impak dan mencapai objektif (ketakutan)
- Kumpulan sasar yang bertepatan– belia celik teknologi
- Kelahiran ‘lone wolves’

Bagaimana kumpulan pengganas mengeksploitasi Internet dan media sosial

- Keganasan siber
- Propaganda dan publisiti
- Perlombongan data
- Pengumpulan dana
- Pengambilan ahli baru
- Komunikasi dan rangkaian
- Kawalan dan arahan
- Penyebaran maklumat palsu

Antara kumpulan pengganas

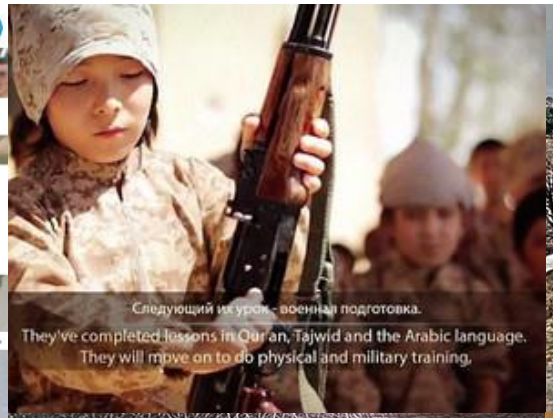
Ku Klux Klan

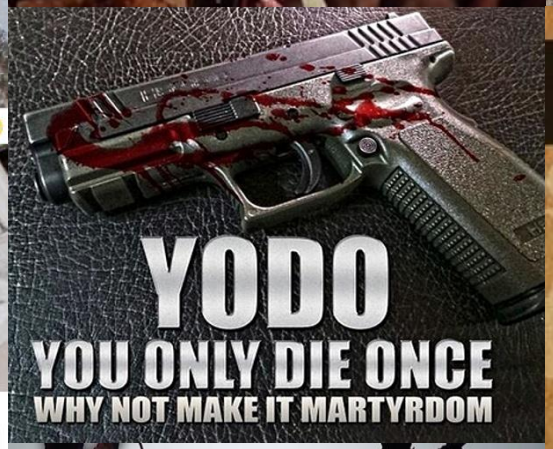
Real IRA

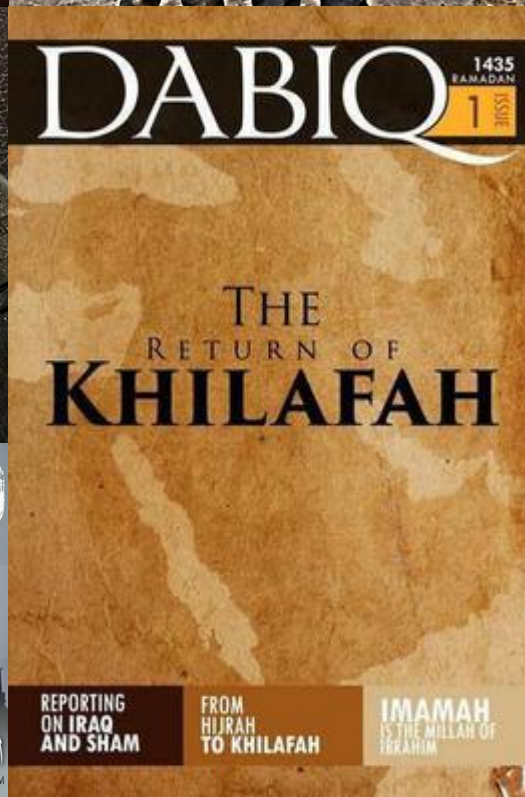
National Action

Aum Shinrikyo

Sebaran ideologi melalui media sosial







Sebaran ideologi melalui media sosial

Propaganda posted on social media by The Base, a violent neo-Nazi group with members in the U.S. and Canada.

Sumber: US neo-Nazi group recruits young Australians, secret recordings reveal. Sydney Morning Herald

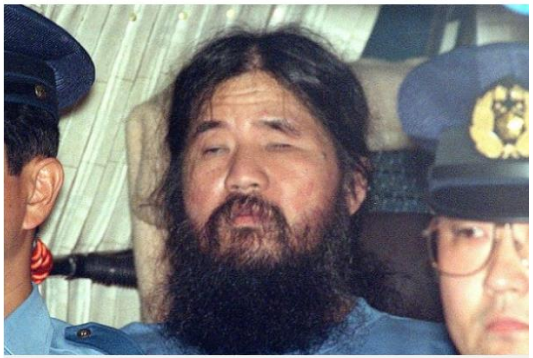
Tayangan serangan secara “live”

Serangan pengganas di Christchurch, New Zealand

Contoh serangan kumpulan pengganas di seluruh dunia

Dalang serangan gas sarin Tokyo digantung

Diterbitkan: Jumaat, 6 Julai 2018 9:26 AM



Shoko Asahara.

(Ubah saiz teks)

KETUA kultus Aum Shinrikyo, Shoko Asahara yang melakukan serangan cecair sarin terhadap penumpang di stesen kereta api bawah tanah pada 1995, akhirnya menjalani hukuman mati bersama beberapa pengikutnya.

Kira-kira 13 maut dalam serangan gas sarin di kereta api bawah tanah di Tokyo.

Ancaman selepas 9/11

HANAFARIZA HARUN
16 SEPTEMBER 2014

INSIDEN serangan berani mati pada 11 September 2001 yang menyebabkan ranapnya Pusat Dagangan Dunia (WTC) di New York, Amerika Syarikat selepas dirempuh sebuah pesawat penumpang Boeing 767 nyata menggemparkan dunia.

Serentak serangan sekitar jam 9 pagi (waktu tempatan) itu, Kementerian Pertahanan AS (Pantagon), turut dirempuh sebuah pesawat mengakibatkan separuh bangunannya runtuh.

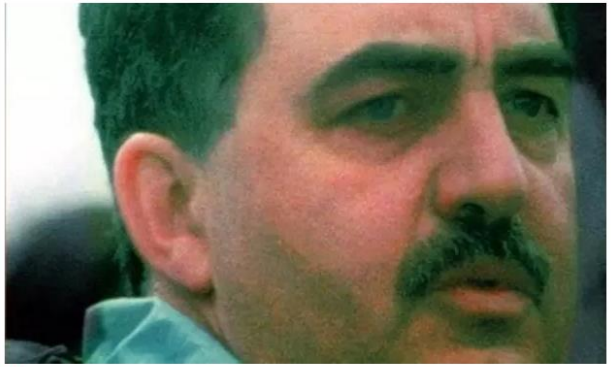
Bukan itu sahaja, serangan diteruskan apabila bangunan dewan perwakilannya, Capitol Hill diikuti Jabatan Negara dan bahagian sayap barat Rumah Putih juga diserang.

Serangan digelar sebagai 9/11 itu didakwa dilakukan kumpulan militan Al-Qaeda. Seramai 19 ahli kumpulan terbabit merampas empat buah kapal terbang penumpang komersil sebelum bertindak merempuh Menara Berkembar WTC.

Kejadian 13 tahun lalu itu masih segar di ingatan sehingga ke hari ini dan telah meninggalkan kesan besar ke atas masyarakat antarabangsa terutamanya apabila hampir 3,000 nyawa terkorban dalam serangan itu.

Real IRA founder guilty of bomb plan during Prince Charles visit

'Arsenal of weapons and explosives' was found at home of Seamus McGrane before Prince Charles's 2015 visit to Ireland



▲ Seamus McGrane was said to have discussed a bombing during the historic royal visit, Ireland's special criminal court was told on Tuesday. Photograph: RTE

One of the founders of the Real IRA has been found guilty of planning a bomb attack during Prince Charles's visit to Ireland in 2015.

Seamus McGrane was said to have discussed a bombing during the historic royal visit, Ireland's special criminal court was told on Tuesday.

Contoh serangan kumpulan pengganas di seluruh dunia

ISIS dakwa bertanggungjawab atas serangan maut London

Pasukan forensik melakukan pemeriksaan di lokasi serangan pengganas di London Bridge pada Ahad. Foto Reuters

(Ubah saiz teks)

KUMPULAN militan Daesh dilaporkan telah memberi amaran bahawa terdapat satu lagi serangan terhadap Britain pasti akan berlaku, dua hari sebelum tujuh orang maut dalam serangan di London Bridge.

Akhbar mingguan *Al-Naba* yang diterbitkan dalam wilayah yang diduduki badan pengganas itu dan disiarkan secara dalam talian, membuat ancaman tersebut di dalam satu artikel mengenai pengebom serangan Manchester, Salman Abedi.

Menurut laporan kepada PJ Media, artikel itu menceritakan tentang seorang tentera dari Daesh telah melakukan keganasan di seluruh Britain.

"Kehadiran mereka membuat tentera di bandar-bandar, menggerakkan pasukan polis di jalan-jalan berikutan kebimbangan terhadap serangan baharu yang tidak dapat dielakkan."

Insiden yang berlaku pada Sabtu malam itu turut mengakibat 48 orang cedera.

Tiga pengganas yang menaiki sebuah van putih merempuh orang ramai di London Bridge sebelum meluru keluar dari kenderaan itu dan menikam mereka secara rawak. - Mail Online

Suspek ISIS dalam serangan Paris dan Belgium diberkas

Apr 10, 2016 | 05:30 AM

0 Kongsi

MOHAMED ABRINI: Dipercayai 'orang bertopi' yang kelihatan dalam klip video keselamatan di lapangan terbang Brussels.

BRUSSELS: Seorang anggota kumpulan militan ISIS, Mohamed Abrini, yang dikehendaki dalam serangan pengganas di Paris pada November lalu, merupakan antara lima suspek yang ditangkap di sini kelmarin, dengan Abrini juga dikaitkan dengan serangan bom di Brussels bulan lalu.

Pihak berkuasa Belgium sedang memastikan sama ada Abrini, 31 tahun, merupakan 'orang bertopi' yang kelihatan dalam klip video keselamatan di lapangan terbang Brussels dengan dua lagi pengebom nekad pada 22 Mac lalu.

PARIS DISERANG PENGGANAS

Dunia terkejut

Nov 15, 2015 | 05:30 AM

NAZRI HADI SAPARIN

0 Kongsi

HULURKAN BANTUAN: Pasukan bomba memberi rawatan kepada seorang lelaki yang cedera dekat dewan konsert Bataclan selepas serangan di Paris, malam kelamrin. - Foto REUTERS

DUNIA dikejutkan dengan siri serangan tersusun oleh kumpulan militan ISIS yang membunuh dengan kejam sekurang-kurangnya 128 orang awam dan menyebabkan sekitar 200 lagi cedera, 99 daripada mereka cedera parah di Paris lewat malam kelmarin.

Berita mengejutkan itu diterima warga setempat sekitar waktu subuh semalam dan ramai bersatu hati mengutuk serangan tersebut sambil menyifatkannya satu jenayah kemanusiaan.

Tindakan terhadap keganasan di Malaysia

1. Kementerian Luar Negeri telah mengadakan “International Deradicalization and Countering Violent Extremism 2016” yang dihadiri oleh wakil-wakil negara ASEAN dan rakan-rakan strategik di Kuala Lumpur.

2. Malaysia telah menubuhkan Regional Digital Counter-Messaging Communication Center yang telah beroperasi bermula May 2016 dengan kerjasama Amerika Syarikat.

3. MCMC akan bekerjasama dengan PDRM untuk mengenalpasti dan menyekat laman sesawang dan akaun media sosial yang mempromosi idealogi radikal, keganasan dan ekstremisme.

4. JAKIM telah mengeluarkan fatwa berikut mengenai isu umat Islam Malaysia yang berjuang atas nama Isis:
   a) Seruan jihad dan mati syahid yang dipegang oleh ISIS adalah bercanggah dengan Islam dan boleh membawa kepada kekufuran kerana mereka menghalalkan darah sesama umat Islam.
   b) Tindakan umat Islam dari Malaysia yang telah ataupun yang ingin berjuang atas nama jihad di bumi Syria bagi menyokong golongan ISIS atau ISIL adalah sia-sia kerana perjuangan mereka tidak tergolong sebagai jihad dan kematian mereka juga tidak dikategorikan sebagai syahid menurut kerangka Hukum Syarak.

Tip memerangi ekstremisme

Bagaimana ibu bapa boleh melindungi anak-anak:

- Menjadi ibu bapa yang mempelajari asas Internet dan kemahiran literasi media digital. (indoktrinasi vs. media digital literasi)
- Memastikan saluran komunikasi dengan anak sentiasa terbuka.
- Dengar masalah dan jangan menghakimi mereka.
- Bercakap tentang manfaat dan risiko Internet.
- Ingatkan anak-anak supaya berhati-hati bila berkenalan dengan rakan dalam talian.
- Fikir sebelum berkongsi apa-apa dalam talian.
- Ibu bapa seharusnya meluangkan masa dan berusaha untuk mempelajari ilmu yang lebih mendalam tentang agama.
- Mengambil tindakan proaktif.

Kaedah bagi ibu bapa untuk mengesan proses pengantunan (*grooming*):

- Aplikasi kawalan ibu bapa dapat membantu mengawasi aktiviti anak dalam talian sama ada berbayar atau percuma, bergantung kepada keperluan.
- Peka terhadap perubahan tingkah laku anak-anak yang mendadak.

KESELAMATAN KOMPUTER

Mengapa penting untuk melindungi komputer anda?

- Memastikan maklumat peribadi contohnya email anda tidak dibaca atau diperiksa oleh orang yang tidak dikenali.

- Memelihara integriti maklumat.

- Melindungi komputer daripada dijangkiti virus, malware, spyware dan ancaman lain.

- Mengelakkan komputer anda daripada diekspolitasi penggodam untuk menyerang sistem lain, contohnya sistem berprofil tinggi seperti sistem kerajaan atau kewangan. Penggodam juga boleh melihat segala aktiviti dan merosakkan komputer anda.

Jenis insiden komputer yang dilaporkan di Malaysia

- Berkaitan kandungan
- Kod jahat
- Spam
- Laporan kerentanan
- Gangguan siber
- Pencerobohan
- Percubaan pencerobohan
- Penafian perkhidmatan
- Penipuan

Perisian hasad

Perisian hasad atau *malware* merupakan program atau perisian yang dirancang bertujuan menyusup atau merosakkan sistem komputer secara rahsia.

3 jenis perisian hasad

Mencari dan mencuri keuntungan, iaitu spyware, adware, botnet, keylogger dan dialer.

Bersembunyi dalam komputer, antaranya adalah Trojan horse, rootkit, backdoor.

Perisian hasad

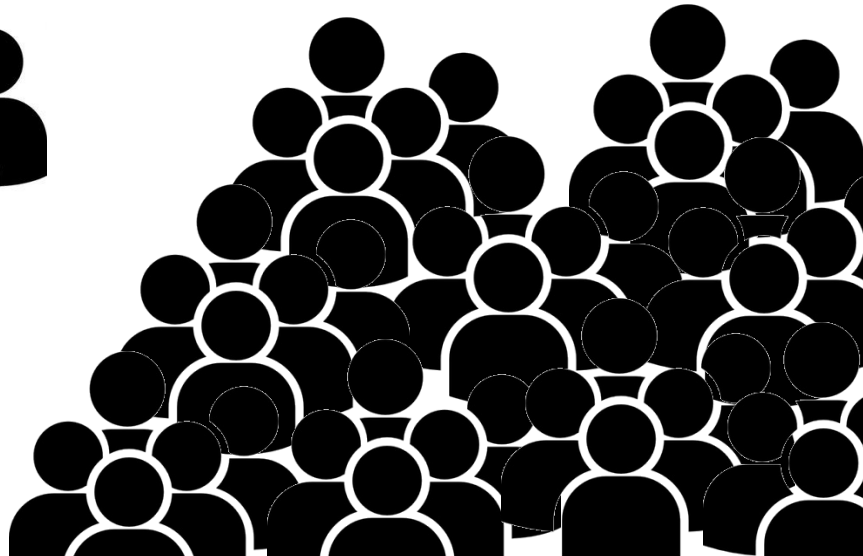
Menjangkiti komputer seperti *virus* dan *worm*

Bagaimana perisian hasad tersebar melalui media sosial ?

Penjenayah siber menghantar pautan berniat jahat daripada akaun media sosial kepada senarai rakan-rakan.

Rakan menerima mesej tersebut dan Klik berlaku pada pautan. Lebih banyak akaun media sosial akan terjejas.

Kitaran berterusan…



Tip mencipta kata laluan yang kukuh dan selamat

- Guna sekurang-kurangnya 8 karaktor.
- Guna gabungan huruf (huruf besar dan kecil), nombor dan symbol.
- Guna kata kunci berlainan untuk setiap akaun dalam talian.
- Tukar kata kunci setiap 6 bulan.

- Jangan tulis kata kunci anda. Jika terpaksa, pastikan ia diletakkan di tempat selamat (contohnya laci berkunci).
- Jangan guna maklumat peribadi seperti nama, alamat, email, nombor telefor, nombor kad pengenalan, nama ibu, tarikh lahir dan sebagaina.
- Jangan guna kata laluan yang senang untuk diteka seperti nama binatang peliharaan, nama samaran, nama sekolah dan sebagainya.

Contoh: Ayah suka nyanyi lagu Getaran Jiwa untuk ibu.

Ay <3 GJ IB

Contoh: Ay<3GJIB

Idea untuk mencipta kata laluan yang kukuh dan mudah diingati:

1. Fikir dan cipta satu ayat menarik yang mudah diingati. Anda boleh memilih tajuk lagu, buku atau filem, pasukan sukan kegemaran dan sebagainya.
2. Pilih huruf pertama atau dua huruf pertama.
3. Tukar beberapa huruf menjadi simbol.
4. Jadikan beberapa huruf sebagai huruf besar dan kecil.
5. Jika anda terpaksa menggunakan kata laluan yang sama untuk semua akaun anda, tambah sesuatu pada permulaan atau pengakhiran supaya ianya unik untuk laman tersebut.

Panduan keselamatan komputer

Padam email yang tidak diketahui

Jika anda menerima email dari seseorang yang tidak dikenali, jangan buka email tersebut. Terus padamkannya.

Jangan muat turun atau buka lampiran melainkan ia sudah dijangka atau telefon pengirim untuk kepastian.

Hidupkan/pasang 'firewall'

'Firewall' menghalang penggodam daripada mendapat akses komputer anda dengan mengehadkan bilangan port yang dibuka untuk awam . Pastikan penghala (router) tanpa wayar anda mempunyai firewall terbina.

Jangan klik pada pautan iklan

Elakkan klik pada mana-mana iklan yang tidak dikenali dan diketahui.

Pastikan komputer anda dikemaskini

- Pastikan komputer anda dilindungi dengan perisian anti-virus yang bereputasi, semua 'patch' keselamatan dan kemaskini.
- Jalankan imbasan virus secara kerap (setiap hari atau setiap minggu)
- Tutup atau 'restart' komputer bila diminta oleh program untuk memastikan perisian dan kemaskini keselamatan dipasang dengan betul.

Sentiasa berwaspada dengan keadaan sekeliling

Pastikan keselamatan kawasan sebelum meninggalkan komputer anda:

- Kunci tingkap dan pintu, simpan kunci di tempat yang selamat dan jangan kongsi kod, kad atau kunci akses.
- Pastikan anda mengunci peralatan mudah alih dan bahan sensitif sebelum anda meninggalkan tempat tersebut.

Gunakan kata laluan yang kukuh dan selamat

Kata laluan yang kukuh tidak semestinya mengandungi kombinasi huruf dan nombor atau siri karakter yang rumit. Ia boleh terdiri daripada cerita yang hanya anda mengetahuinya.

Panduan keselamatan komputer

Elak laman web yang tidak boleh dipercayai

Komputer anda mungkin dijangkiti virus atau spyware jika anda melayari laman web yang diragui seperti laman pornografi.

Berhati-hati dengan peranti luaran

Kebanyakan program virus akan melancarkan secara automatik apabila pemacu USB atau peranti simpanan dimasukkan ke dalam komputer. Amat mudah untuk dijangkiti kerana anda tidak perlu membuka atau memuat turun fail tersebut.

Tutup komputer

Tutup, kunci, log keluar atau pastikan komputer atau peranti anda dalam mod tidur sebelum meninggalkannya tanpa pengawasan. Peranti/komputer anda haruslah dilengkapi dengan kata laluan untuk ‘startup/wake up’

Minimumkan simpanan

Padamkan dan jangan simpan maklumat sensitif atau salinan tunggal data kritikal, projek, fail dalam peranti mudah alih melainkan ianya dilindungi dengan betul.

Pastikan keselamatan rangkaian tanpa wayar anda

Berhati-hati kerana sesiapa sahaja yang berdekatan termasuklah mana-mana penggodam boleh mengakses maklumat dalam peranti anda atau melakukan ‘piggyback’ ke atas rangkaian anda.

Elakkan p2p

Elakkan daripada menggunakan perisian perkongsian fail p2p. Anda mungkin memuat turun fail lagu yang telah dijangkiti malware.

Sesi interaktif

1. **Adakah anda mengunci telefon/akaun/profil anda dengan kata laluan yang selamat?**

2. **Apakah perlindungan yang diperlukan untuk memastikan komputer anda selamat?**

KAWALAN KENDIRI

APA ITU KAWALAN KENDIRI ?

- Keupayaan seseorang mengawal emosi, keinginan/ nafsu, dan tindakan di ruangan siber
- Perlakuan beretika
- Mekanisme paling berkesan untuk mengawal selia Internet

Mengapa kawalan kendiri perlu?

1. Mengurangkan kawal seliaan pihak berwajib.
2. Kesukaran mengawasi semua jenis saluran dalam talian.
3. Medium global tanpa nama.
4. Masyarakat Internet telah menegaskan akta kebebasan bersuara.
5. Pengguna individu mempunyai akses kepada pelbagai maklumat.
6. Kesejahteraan emosi- Keupayaan untuk menenangkan diri bila marah dan menghiburkan diri bila sedih.
7. Kesejahteraan emosi dan tingkah laku
8. Memperkasa dan menguatkan jati diri.

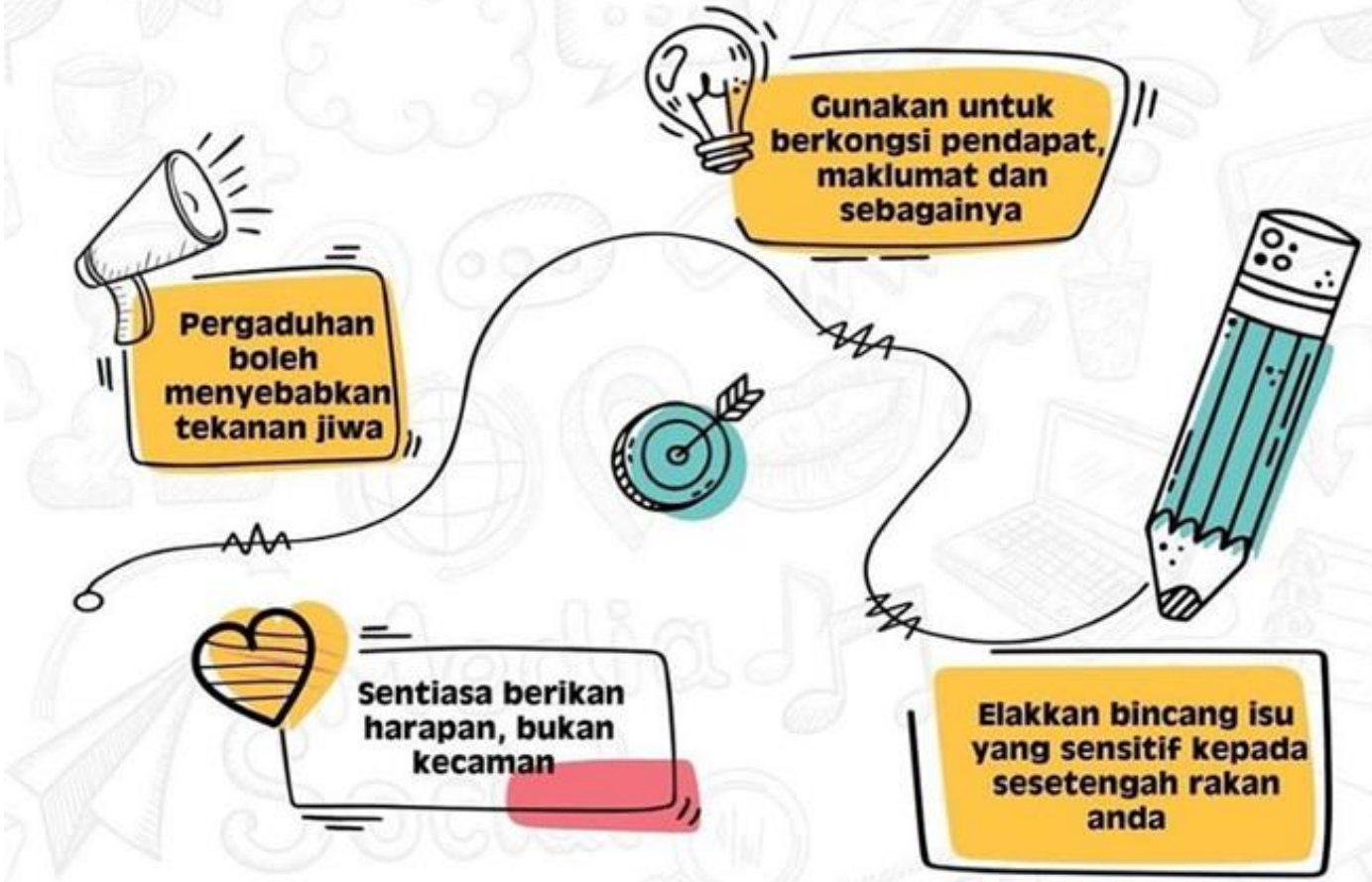
klik dengan bijak

MCMC

TIP KAWALAN KENDIRI

- **BERHATI-HATI** bila berkongsi dan tag foto. Elak *oversharing*- Maklumat anda mengumpan penjenayah siber.
- **PADAM** maklumat peribadi dan yang negatif. Bina profil positif dalam talian.
- **LAPOR** kandungan tidak sesuai kepada pembekal perkhidmatan Internet dan pihak berkuasa.
- **JANGAN** berjumpa dengan orang yang tidak dikenali di tempat sunyi. Pilih tempat awam yang selamat.
- Lawak jenaka anda mungkin **TIDAK KENA** dengan orang lain.
- Pastikan emosi dan fizikal anda stabil. **ELAK** tindakbalas yang terburu-buru**.**
- Jadikan **UNDANG-UNDANG SEBAGAI PERINGATAN** sebelum mengemaskini status.

Guna Media Sosial Secara Positif



KLIK DENGAN BIJAK KLIK DENGAN BIJAK WWW.KLIKDENGANBIJAK.MY

Jendela
Jalinan Digital Negara

MALAYSIA ICT VOLUNTEER

MCMC

pakej
Pelan Accelerator Kurier Negara

Pupuk
Perkasa Pendigitalan Usahawan Kecil

follow lerr…

SEBENARNYA.MY
Tidak Pasti Jangan Kongsi

klik dengan bijak

PUSAT INTERNET KOMUNITI
PEDi
www.mcmc.gov.my

CHECK YOUR LABEL

Suruhanjaya Komunikasi dan Multimedia Malaysia

skmm_mcmc

MCMCTV

SKMM_MCMC

Terima Kasih

Like & follow…

www.klikdenganbijak.my

@klikdenganbijak

@klikdenganbijak

klikdenganbijak

#klikdenganbijak