KESELAMATAN SIBER
PERANAN BERSAMA

OLEH:

AGENSI KESELAMATAN SIBER NEGARA
NOVEMBER 2018

KANDUNGAN

- Penggunaan Internet di Malaysia
- Keselamatan & Ancaman Siber
- Kesedaran Keselamatan Siber Sektor Awam

PENGGUNAAN INTERNET DI MALAYSIA

DIGITAL IN MALAYSIA
JANUARY 2018

31.83 million

Total Population

25.08 million

Internet Users

21.62 million

Unique Mobile Users

24.00 million

Active Social Media Users

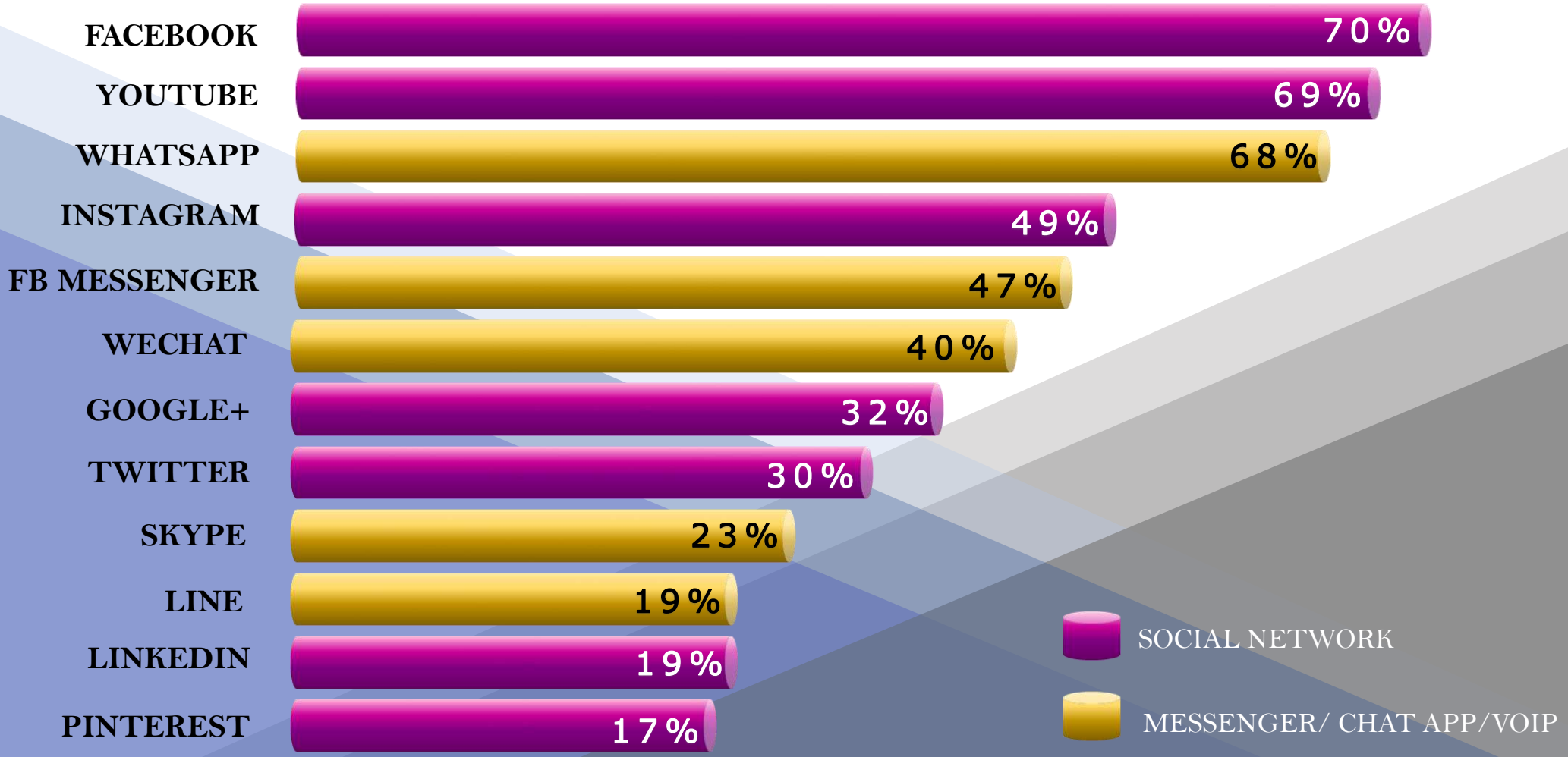
22.00 million

Active Mobile Social Users

Sumber: https://www.slideshare.net/wearesocial/digital-in-2018-in-southeast-asia-part-2-southeast-86866464

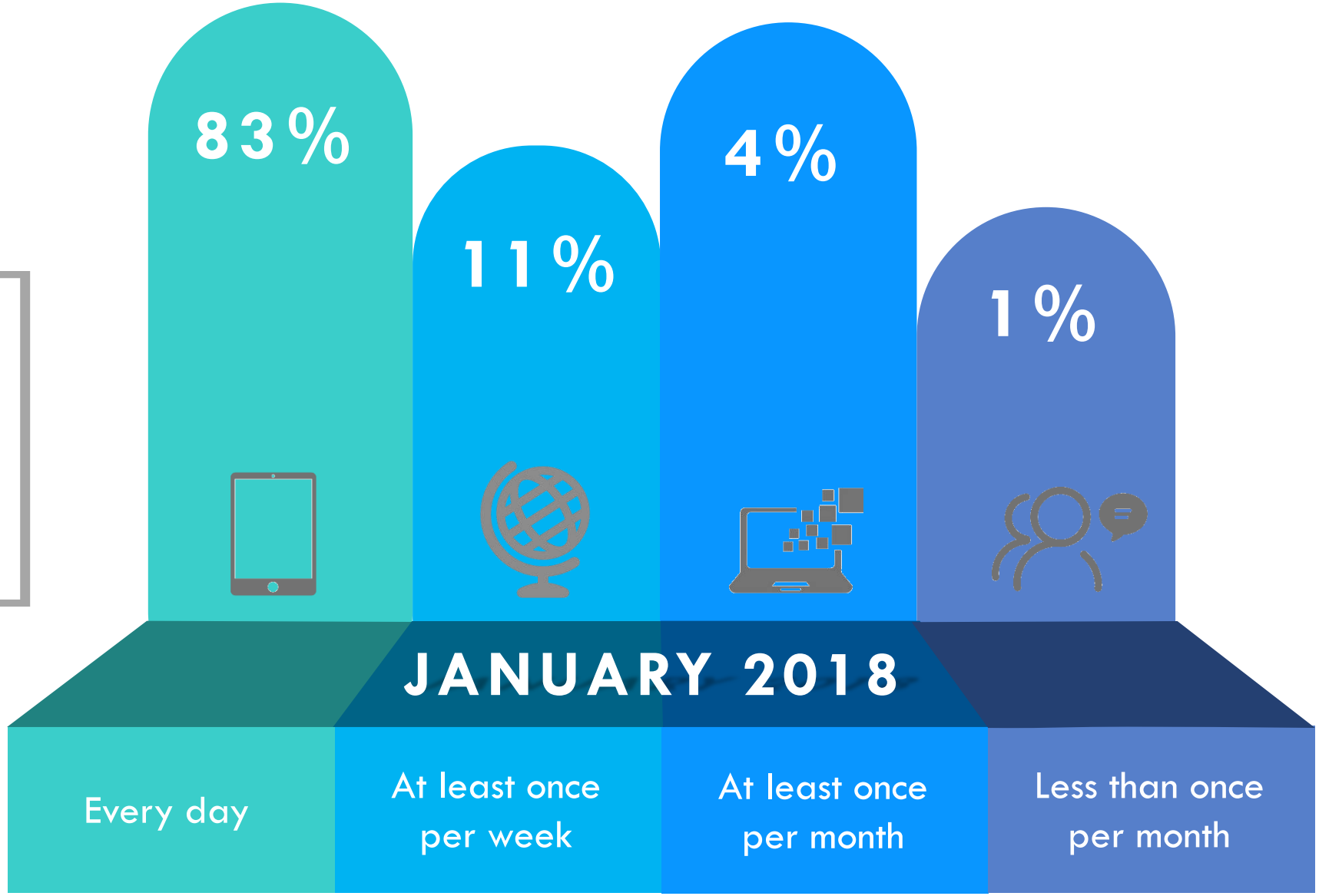
JAN 2018

MOST ACTIVE SOCIAL MEDIA PLATFORM



Sumber: https://www.slideshare.net/wearesocial/digital-in-2018-in-southeast-asia-part-2-southeast-86866464

KEKERAPAN PENGGUNAAN INTERNET



Sumber: https://www.slideshare.net/wearesocial/digital-in-2018-in-southeast-asia-part-2-southeast-86866464

KETAGIHAN INTERNET

14%

Kadar ketagihan internet - Malaysia menduduki tangga ketiga di belakang Filipina dan Hong Kong dengan kadar 14%. Peratusan global 6%.

Sumber: Dr. Kwok Kei Mak, Hong Kong, 2014

78.8%

Pengguna internet, terutama kanak-kanak di negara ini mengalami ketagihan Internet

Sumber: Berita Harian, 22 Oktober 2017

2 dari 7
Remaja Malaysia
GI NET
KETAGIHAN INTERNET

Public Health Malaysia

REMAJA CINA

merupakan golongan tertinggi yang ketagih kepada internet

Majoriti Menggunakan Telefon Pintar

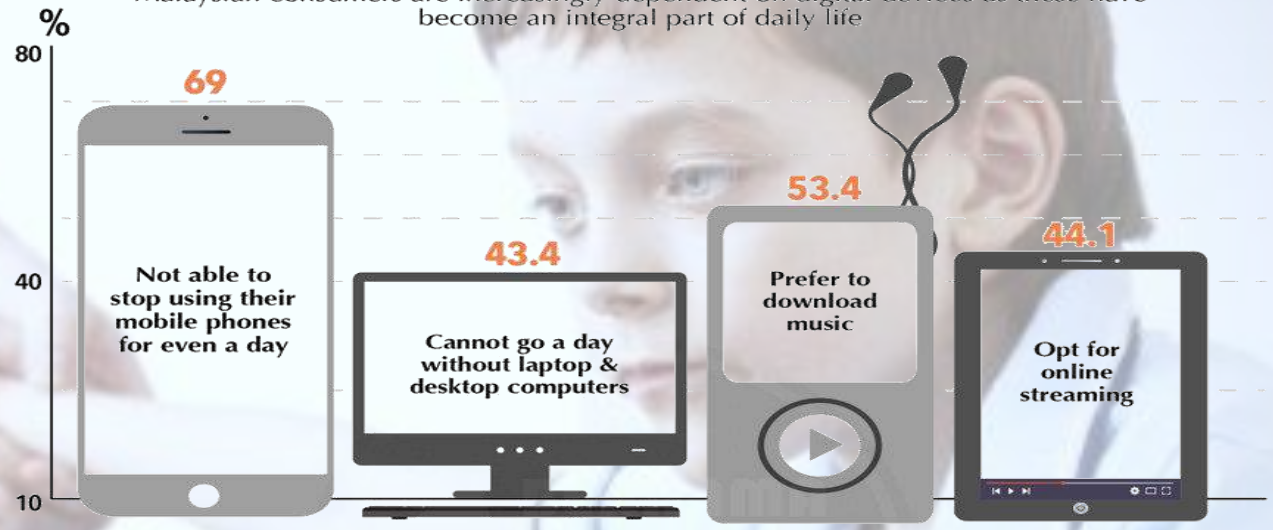
Kesan penggunaan internet berlebihan kepada remaja

- Faktor keselamatan remaja dan data
- Terdedah kepada persekitaran Cyberbully
- Risiko mengunjungi laman porno
- Bermain permainan video secara berlebihan
- Risiko berbelanja berlebihan secara online

Sumber : Adolescent Health Survey,NHMS 2017

MALAYSIAN DIGITAL LIFESTYLE

Malaysian consumers are increasingly dependent on digital devices as these have become an integral part of daily life



- Malaysians are the least likely to pay for digital content alongside Singapore

Music is also the most commonly accessed online content in Malaysia, followed by movies/TV shows and apps

53.4% Opt to download video games

74.7% Prefer digital books

43.5% Prefer playing online games

25.4% Opt for physical copies

The State of Digital Lifestyles Report is based on responses from 5,000 consumers in France, Germany, India, Italy, Japan, Malaysia, Singapore, South Korea, the United Kingdom, and the United States aged 18 and above who had downloaded software or streamed online videos or music in June 2018

..there is enough evidence to show links to anxiety, depression, physical health problems, school disconnection, unemployment, decreased job productivity and social isolation

Sumber: Child Psychologist, Dr. Norharlina Bahar

50.4%

Kanak-kanak di negara ini memiliki telefon pintar pada umur 12 tahun

Sumber: Suruhanjaya Komunikasi dan Multimedia Malaysia

Ketagihan Internet mempunyai kaitan dengan faktor luar - pencemaran udara, kesesakan lalulintas, kepuasan hidup

Sumber: Hong Kong University (HKU) Psychology Department, Associate Dean Prof. Dr Cecelia Cheng

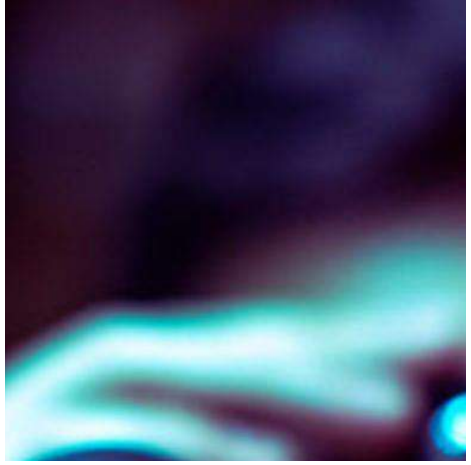
SCREEN ADDICTION

"**2** year old in Malaysia spends **6** hours on screen everyday & **95%** engage two screens at the same time (tv at all times)."

Sumber: Perak Clinical Research Centre 2015 Study, NST 26 Ogos 2018


define: nomophobia
Google
Web
Images
Videos
Nomophobia
[noh-muh-foh-bee-uh]
noun
An abnormal, irrational fear of being without one's mobile device, or of being unable to communicate using one's mobile device.
"as she watched the mobile phone fall into the toilet bowl, her nomophobia caused a bolt of panic to hit her mind"
- DERIVATIVES nomophobe n. nomophobic adj.
Where is it ?
Oh No! I lost it
I found it !
Nomophobia !


ADDICTION RECOVERY CENTER
RECEPTION
1ST. FLOOR
• FACEBOOK
2ND FLOOR
• TWITTER
3RD FLOOR
• INSTAGRAM
ROOFTOP
• TEXTING WHILE WALKING



KESELAMATAN & ANCAMAN SIBER

SERANGAN SIBER KE ATAS INFRASTRUKTUR KRITIKAL

- Grid Bekalan Elektrik
- Infrastruktur Internet
- Sistem Perbankan
- Perkhidmatan Penerbangan

JENAYAH SIBER

- Penipuan Dalam Talian
- *Phishing*
- *Intrusion*

HACKTIVISM

- Bermotifkan isu politik, sosial dan kemanusiaan
- Dendam
- Perhatian

PENGGUNAAN INTERNET OLEH PENGGANAS

- Ideologi
- Pengumpulan Dana
- Merekrut
- Operasi

KETIRISAN MAKLUMAT TERPERINGKAT

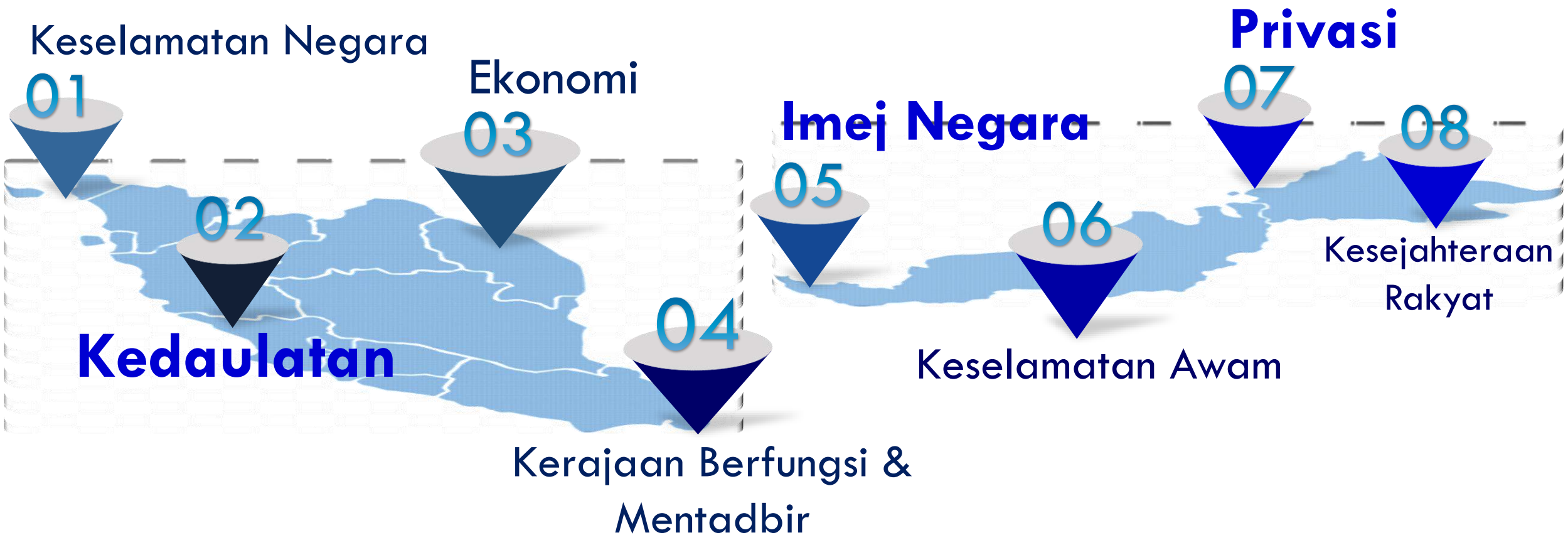
- Maklumat dicuri tanpa disedari
- Maklumat dicuri - terdedah
- Maklumat dicuri – aktiviti jenayah

KERENTANAN TEKNOLOGI (KEBERGANTUNGAN)

- Kebergantungan tinggi kepada Syarikat dan Teknologi – Capaian secara tidak sah kepada Sistem & Maklumat Kritikal

KANDUNGAN INTERNET YANG BERBAHAYA

- Pornografi
- Penderaan Kanak-kanak
- Perjudian Dalam Talian
- Buli Siber



IMPAK ANCAMAN SIBER

SERANGAN SIBER KE ATAS INFRASTRUKTUR KRITIKAL

2017

SERANGAN RANSOMWARE

Wannacry Ransomware

(Mei 2017)

SERANGAN RANSOMWARE

NotPetya Ransomware

(Jun 2017)

SERANGAN DDoS

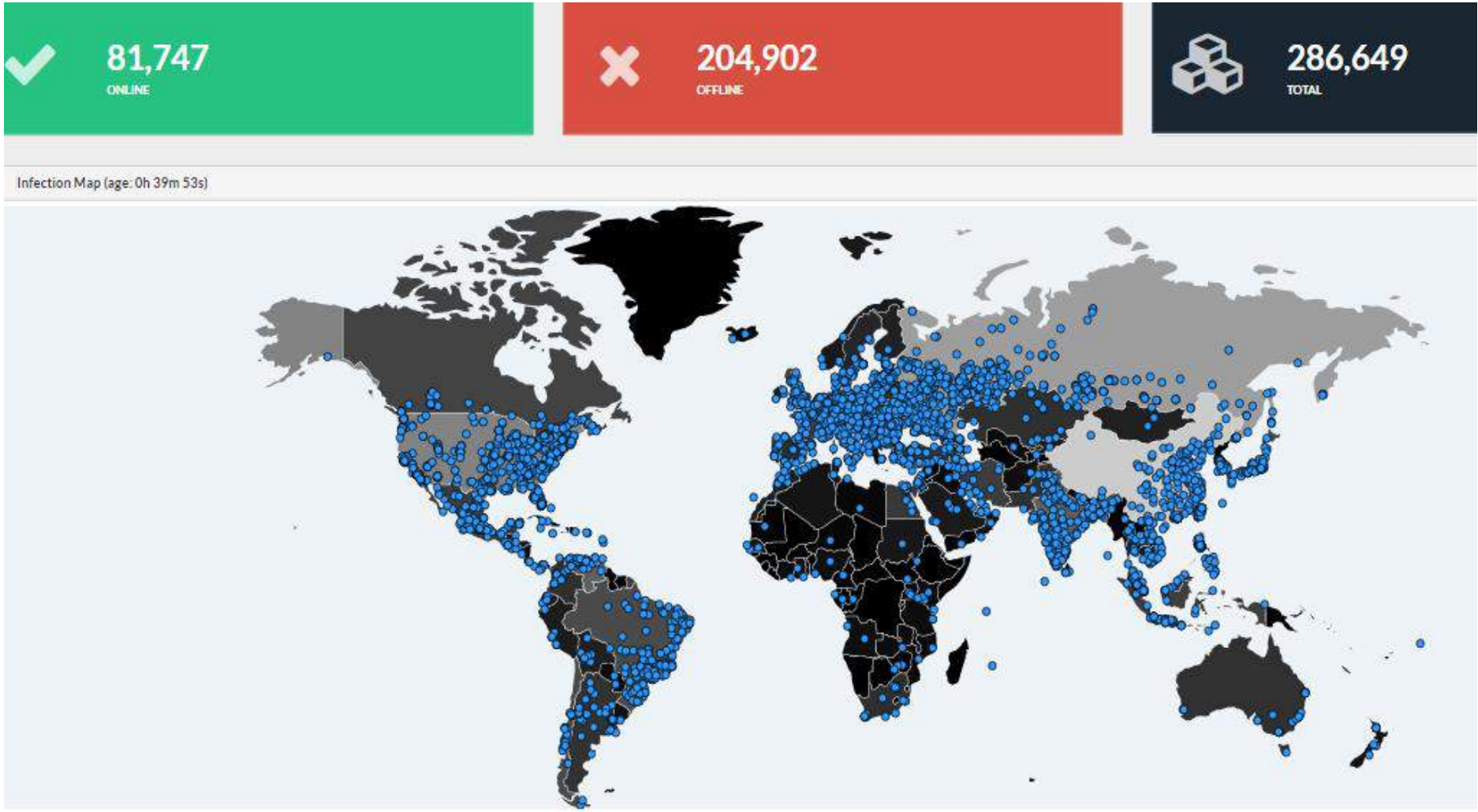
Serangan ke atas Institusi Pelaburan Saham Negara oleh Armada Collective

(Julai 2017)

WANNACRY RANSOMWARE 2017

IMPAK GLOBAL DAN DI MALAYSIA

- Hampir 300,000 komputer dijangkiti di seluruh dunia – 120 IP telah dikesan di Malaysia.
- Sebilangan kecil telah membuat bayaran melalui Bitcoin.
- Walau bagaimanapun, hanya 2 insiden tidak melibatkan data kritikal telah dilaporkan kepada MKN.



Sumber : https://intel.malwaretech.com/botnet/wcrypt/?t=24h&bid=all

RANSOM NOTE


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

2015

Serangan ke atas laman web Malaysia Airlines oleh Lizard Squad - Official Cyber Caliphate (Jan 2015) (Sony PlayStation and Xbox).

2017

Serangan oleh kumpulan penggodam Indonesia ke atas laman-laman web Malaysia berikutan isu bendera Indonesia terbalik dalam Buku Aturcara Majlis Pembukaan Sukan SEA Ke-29 (Ogos 2017)

- Serangan secara *web defacement*.
- Tiga (3) laman web agensi Kerajaan dan 51 laman web syarikat kecil tempatan telah diceroboh.
- 77 maklumat kad kredit rakyat Malaysia telah didedahkan di Internet.

CYBER ATTACKS ON CII - GLOBAL

ESTONIA CYBER ATTACKS 2007

3 Weeks

LOSES USD 1 Billion

Cyber-attack on South Korea

- 20 March 2013
- 48,700 PCs, servers and kiosks at 3 banks and 3 TV stations were hacked
- Business was disrupted
  - Banking: ATM, banking operations, and online banking came to a halt.
  - TV/Media: media contents

3 days

LOSES USD 900 Million

2015

3 hours

LOSES RM2 Million

RUSSIA BEYOND THE HEADLINES

Russia loses $3.3 billion to cyber attacks

April 14, 2016 ANNA KUCHI

Cybercriminals are be
government agencies

Cyber crime cost UK business more than £1bn in the past year

KETIRISAN MAKLUMAT TERPERINGKAT

Serangan APT untuk mendapatkan maklumat beberapa agensi Kerajaan (Feb-Mei 2018)

Data 46 juta pengguna Malaysia terdedah menerusi forum dalam talian dan laman berita *lowyat.net*. Data melibatkan pengguna syarikat telekomunikasi, Persatuan Perubatan Malaysia, jobstreet.my. (Dis 2017)

Data peribadi 220,000 penderma organ dan data peribadi waris menjadikan jumlah keseluruhan 440,000 melalui laman *lowyat.net*. (Jan 2018)

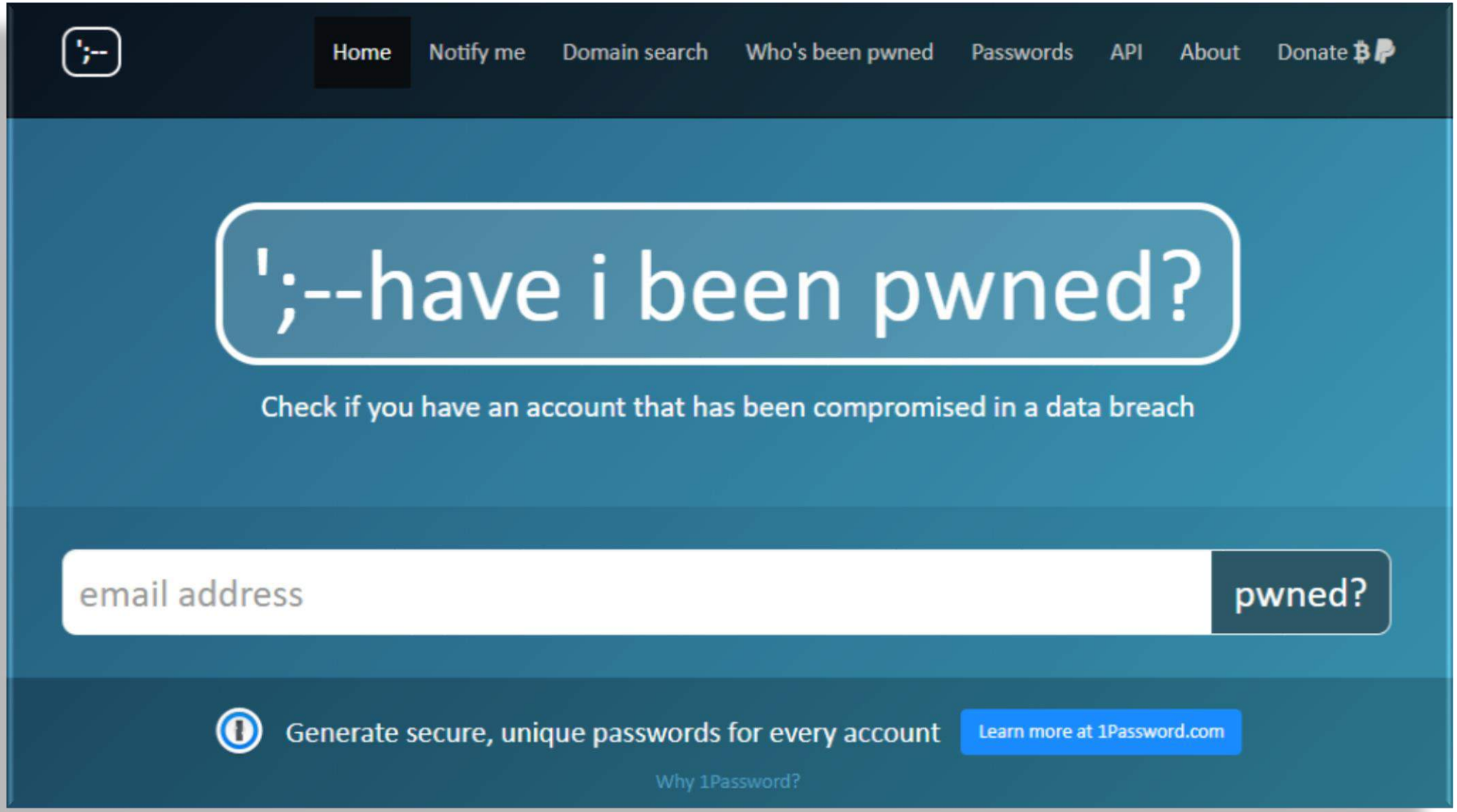
Serangan *spear phishing* berkenaan isu MH370 (Feb-Mei 2018)

Kebocoran maklumat perubahan dalam agensi kerajaan serta syarikat berkaitan kerajaan (GLC) (Julai 2018)

Ali Hamsa @DrAliHamsa · Jul 27

Pegawai forensik @SKMM_MCMC memulakan siasatan terhadap kes kebocoran dokumen-dokumen rahsia kerajaan baru-baru ini.

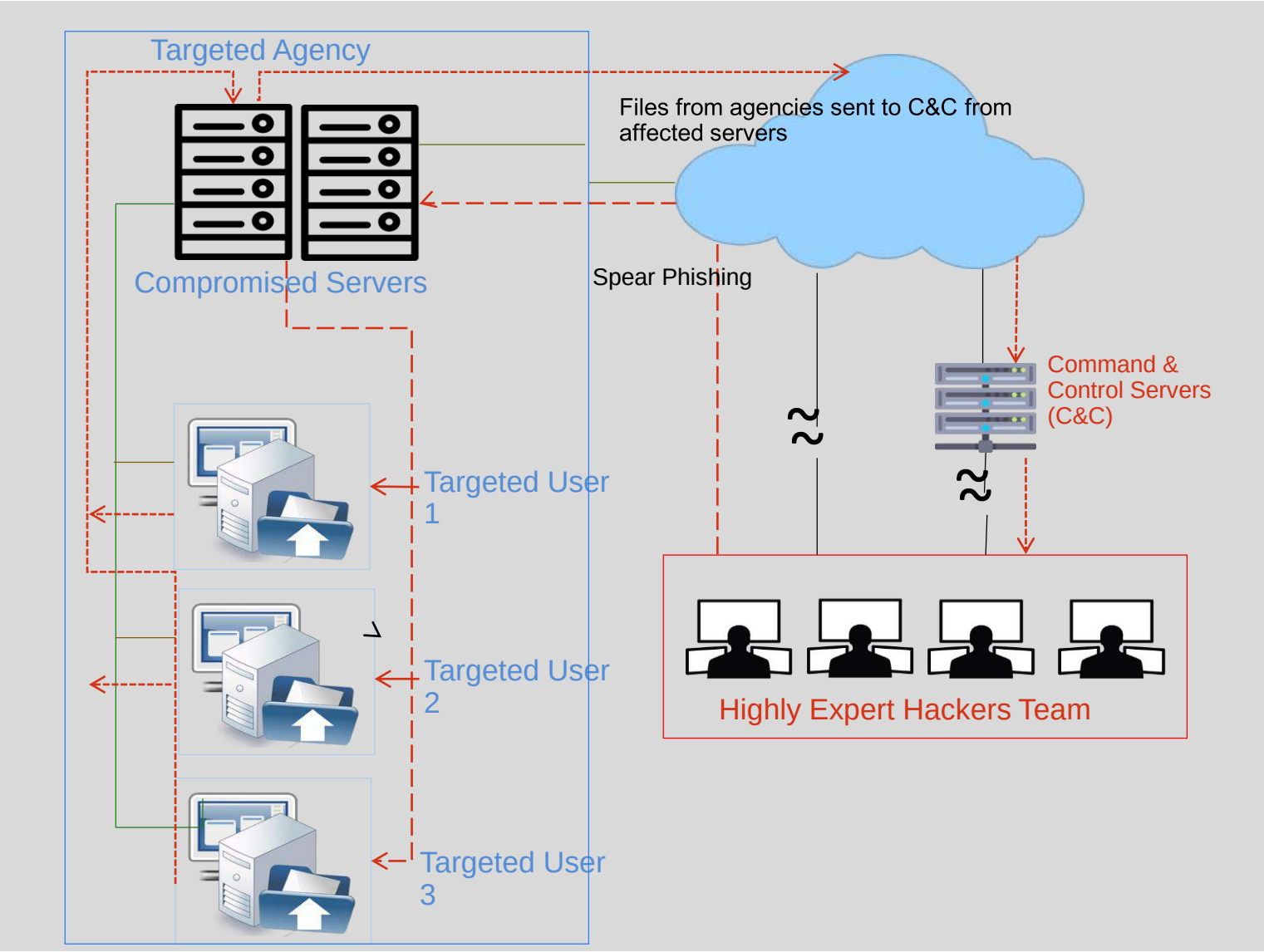
Selain laporan polis, semua KSU dan Ketua Perkhidmatan telah diarah memastikan dokumen terperingkat kerajaan tidak dikompromi.



https://haveibeenpwned.com/

APT AGAINST TARGETED AGENCIES

EMAIL COPIES ARE SENT TO UNAUTHORIZED PARTIES – INFORMATION LEAKAGE



208 agensi-agensi Kerajaan melibatkan 311,532 pengguna

Terdapat 737 e-mel dikepilkan dengan perisian berbahaya

796 pautan URL berbahaya.

Portal Rasmi
KEMENTERIAN PENDIDIKAN MALAYSIA
www.moe.gov.my

Kebocoran 10.5 juta data pengguna Kementerian Pendidikan Malaysia

(450,000 data guru)

https://www.facebook.com/help/securitynotice

JENAYAH SIBER

STATISTIK

JUMLAH KES

2015

8,762 kes

2016

11,012 kes

2017

13,636 kes

RM184,156,177.00

2018

8,313 kes

RM299,557,862.00

(Setakat 3 Okt 2018)

TREND TERKINI JENAYAH SIBER DI MALAYSIA

JENAYAH KOMPUTER "COMPUTER CRIME"

CAPAIAN TANPA KUASA

- ✧Penipuan Telekomunikasi
- ✧Penipuan 419/ Cinta Siber
- ✧Penipuan E-Belian
- ✧Penipuan e-Kewangan
- ✧Pelanggaran Harta Intelek

JENAYAH BERKAITAN KOMPUTER "COMPUTER ASSISTED / RELATED CRIME"

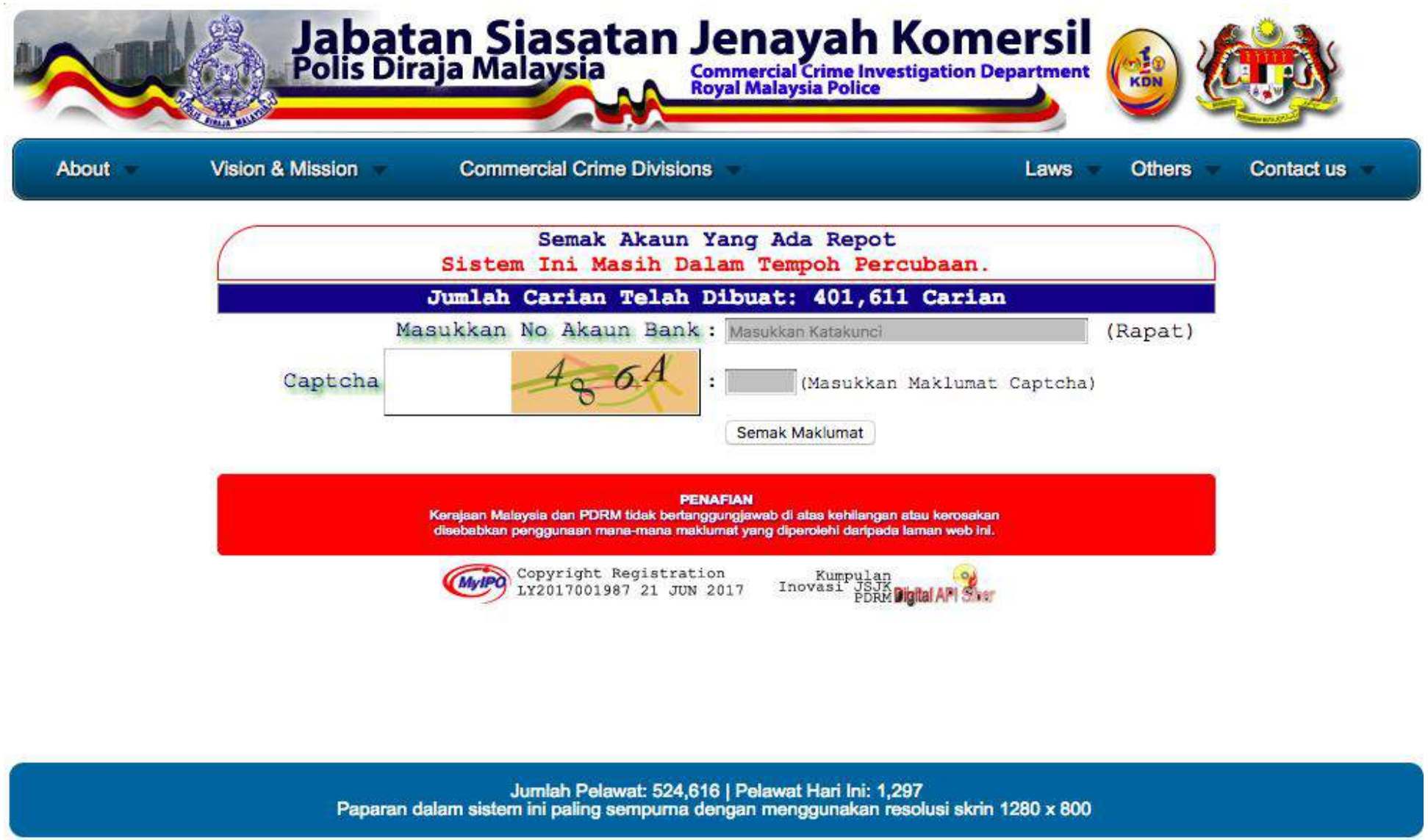
PENIPUAN SIBER

- ✧Penipuan Telekomunikasi
- ✧Penipuan 419/ Cinta siber
- ✧Penipuan E-Belian
- ✧Penipuan e-Kewangan
- ✧Pelanggaran Harta intelek

KESALAHAN KANDUNGAN

- ✧Fitnah
- ✧Lucah
- ✧Hasutan
- ✧Ancaman
- ✧Menjijikkan/menyakitkan hati
- ✧Mengaibkan/menjatuhkan maruah

Sumber: Polis DiRaja Malaysia



http://ccid.rmp.gov.my/semakmule/

Sumber: Polis DiRaja Malaysia

HACKTIVISM

ANONYMOUS ATTACK - 2011

1. Dikesan pada 13 Jun 2011 melalui kenyataan web dan video kumpulan Anonymous. Rancangan untuk menyerang Malaysia melalui "**Operation Malaysia**".
2. Serangan bermula pada 14 – 20 Jun 2011.
3. Ancaman ini adalah berikutan daripada tindakan SKMM yang menyekat akses ke 10 laman perkongsian fail pada 31 Jun2011 yang dianggap sebagai melanggar hak asasi manusia dan kebebasan menggunakan internet.
4. Kebanyakan serangan ini dipercayai dilakukan oleh kumpulan penggodam-penggodam tempatan iaitu *DragonForce* dan *RileksCrew* serta penggodam-penggodam amatur lain.
5. 94 laman web **telah diserang melibatkan** 18 agensi kritikal**. Daripada jumlah ini juga,** 28 **adalah laman web agensi Kerajaan.**

OPS MALAYSIA BY ANONYMOUS HACKERS

2013

1. #OpsFitnah.
2. Serangan dilancarkan atas motif bahawa mereka telah dipergunakan oleh kerajaan susulan daripada isu penyebaran surat palsu berkaitan pengemaskinian maklumat pangkalan data Jabatan Akauntan Negara Malaysia (JANM) yang mengakibatkan sebilangan penjawat awam kehilangan wang gaji dari akaun simpanan.
3. Laman web yang telah dicerobohi melibatkan 4 laman web kerajaan, 4 laman web kolej swasta dan 19 laman web syarikat swasta.
4. Mempunyai agenda tertentu pada 20 Oktober 2013.
5. Tiada insiden pada tarikh tersebut.

2015

1. Dikesan melalui video mengancam untuk melakukan serangan siber pada 29 hingga 30 Ogos 2015 ke atas laman-laman web di Malaysia.
2. Sasaran utama kumpulan penggodam adalah www.1mdb.com.my, www.najibrazak.com, www.sprm.gov.my dan www.rmp.gov.my.
3. Ancaman bermotif politik kerana menggesa YAB Dato' Sri Mohd Najib bin Tun Abdul Razak untuk meletakkan jawatan dalam tempoh 48 jam selepas serangan pertama.
4. Menyatakan sokongan terhadap Bersih 4.0.
5. Ancaman untuk melancarkan serangan ke atas 150 laman web Kerajaan yang lain.
6. Serangan gagal dan dapat dipulihkan dalam tempoh yang singkat.

KANDUNGAN INTERNET

Yang Menjejaskan Identiti &
Nilai Moral Masyarakat

19% kanak-kanak melayari pornografi

7% kanak-kanak mula melayari pornografi sebelum umur 8 tahun (ada bermula 5 tahun)

63% melayari melalui telefon pintar (Ogos 2018)

Sumber: Kajian Heriot Watt University & Suruhanjaya Komunikasi dan Multimedia Malaysia

Malaysia mencatatkan bacaan alamat IP tertinggi di Asia Tenggara dalam memuat naik dan memuat turun gambar serta visual pornografi kanak-kanak.

(PDRM, Jan 18)

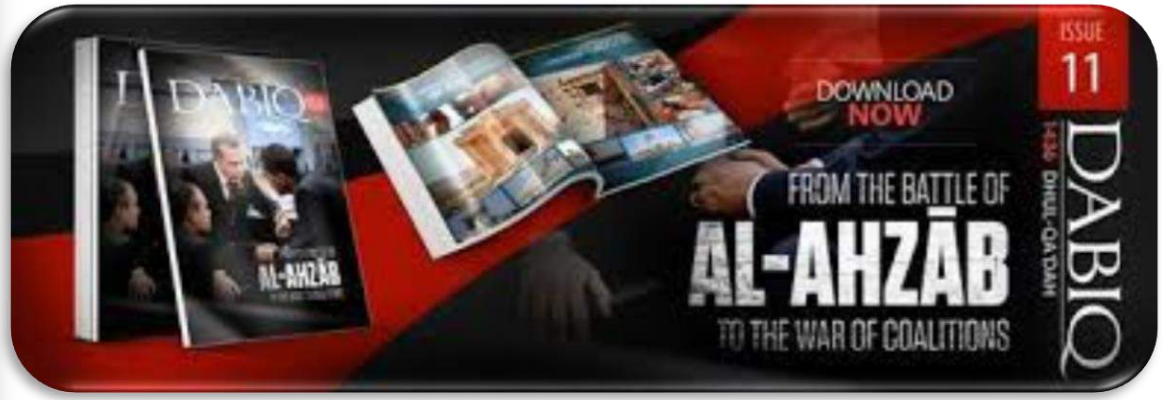
Data menunjukkan hampir 20,000 alamat IP di Malaysia memuat naik dan memuat turun gambar serta visual.

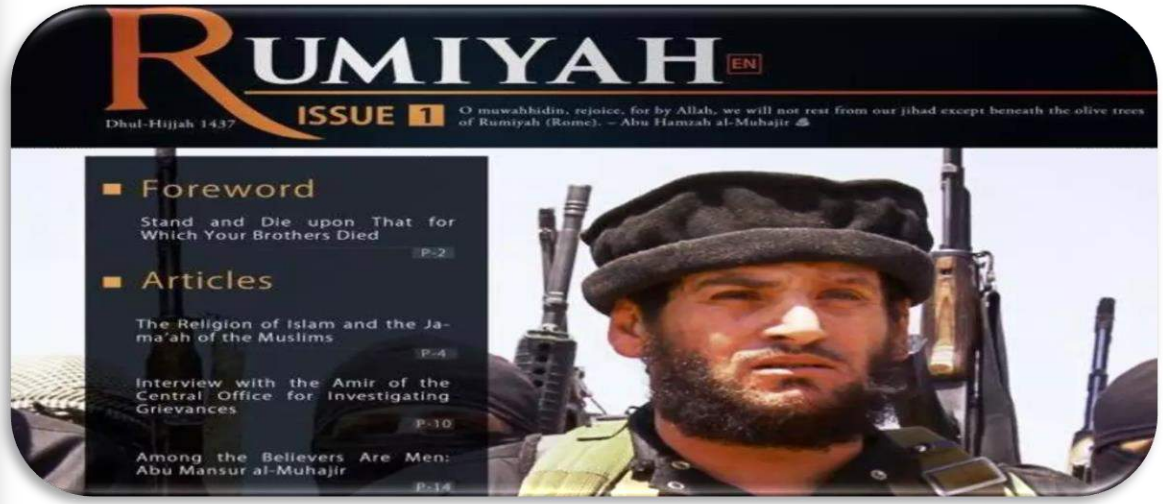
SEBENARNYA.MY

Tidak Pasti Jangan Kongsi

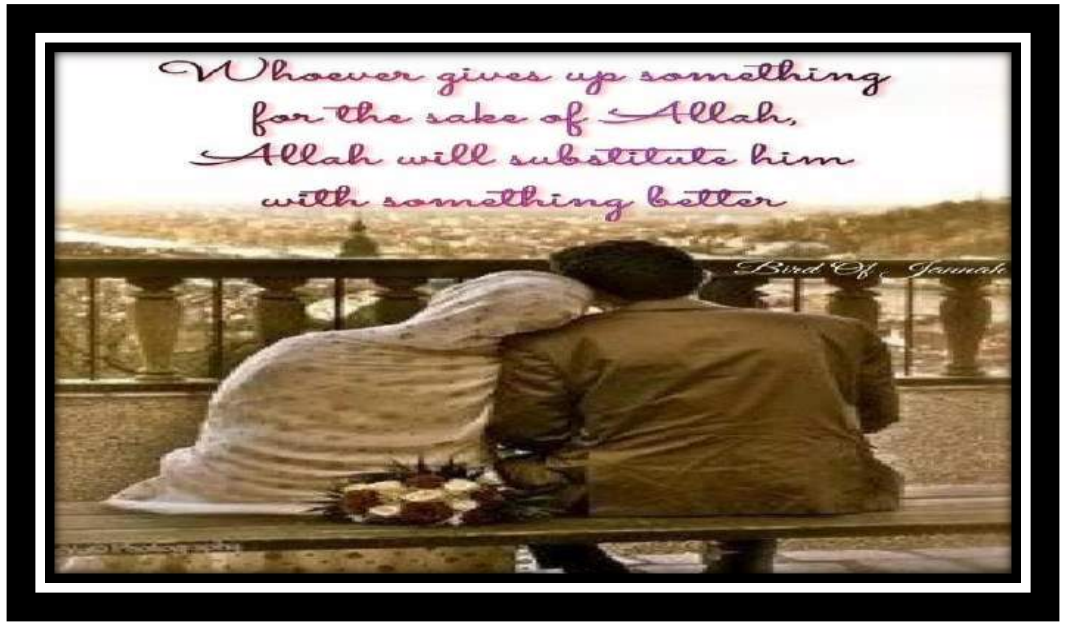
PENGGUNAAN INTERNET OLEH PENGGANAS

1. Al Qaeda, Islamic States/Daesh, Boko Haram.
2. Majalah atas talian dalam pelbagai bahasa – Dabiq, Dar al-Islam, Rumiyah, al-Fatihin (Bahasa Indonesia-mensasarkan rantau Asia Tenggara, Katibah Nusantara)
3. Blog Birds of Jannah – kehidupan seorang isteri pejuang IS.
4. Penggunaan aplikasi media sosial – komunikasi, memberi pengarahan, berbai'ah, merancang aktiviti,





PETIKAN DARIPADA BLOG BIRD OF JANNAH



VIDEO UGUTAN OLEH IS

KESEDARAN KESELAMATAN SIBER SEKTOR AWAM

OBJEKTIF

Meningkatkan tahap kesedaran penjawat awam mengenai keselamatan siber.

Membudayakan pengendalian maklumat digital Kerajaan secara teratur dan selamat.

Memberi **kesedaran** kepada penjawat awam mengenai **implikasi kecuaian** pengendalian maklumat digital Kerajaan.

10 LANGKAH MUDAH KESEDARAN KESELAMATAN SIBER

1

GUNAKAN KATA LALUAN


Wifi
AVAILABLE
HERE
wifi code is,
code =


Username : admin
Password : admin

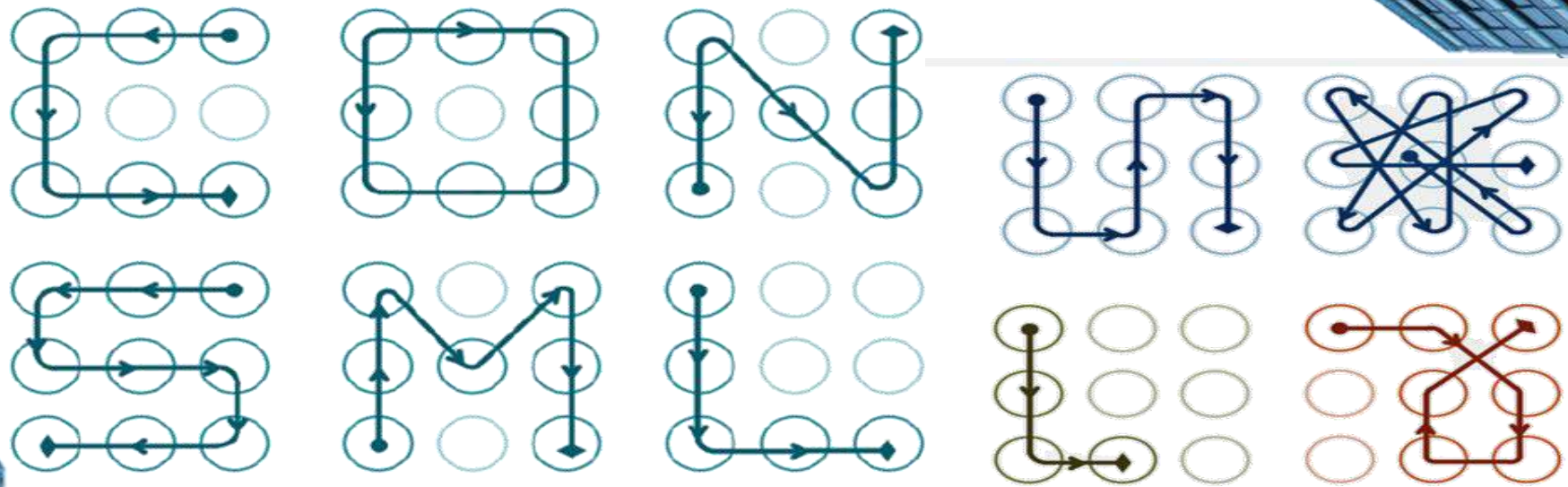

A password is like a toothbrush
Choose a good one
Don't share it with anyone
Change it occasionally

BIZ & IT —

New data uncovers the surprising predictability of Android lock patterns

Like "p@$$w0rd" and "1234567" many Android patterns are easy to guess.

DAN GOODIN - 8/20/2015, 6:15 PM



Marte Løge, a 2015 graduate of the Norwegian University of Science and Technology, recently collected and analyzed almost 4,000 ALPs as part of her master's thesis. She found that a large percentage of them—44 percent—started in the top left-most node of the screen. A full 77 percent of them started in one of the four corners. The average number of nodes was about five, meaning there were fewer than 9,000 possible pattern combinations. A significant percentage of patterns had just four nodes, shrinking the pool of available combinations to 1,624. More often than not, patterns moved from left to right and top to bottom, another factor that makes guessing easier.

Sumber: https://arstechnica.com/information-technology/2015/08/new-data-uncovers-the-surprising-predictability-of-android-lock-patterns/


What's your password?!

2 KEMASKINI PERISIAN KESELAMATAN

Anti virus

Anti spyware

Perisian tulen

Perisian tidak tamat tempoh

3 SIMPAN DAN LINDUNGI MAKLUMAT

- Elakkan daripada memuat naik dokumen rasmi Kerajaan dalam *public cloud*.
- Sentiasa sediakan salinan pendua (back up) maklumat digital secara berkala.
- Elakkan daripada meninggalkan komputer dan gajet tanpa sebarang pengawasan.
- Putuskan sambungan Internet atau wi-fi sekiranya tidak menggunakannya lagi.
- Pastikan meja kerja dikemas dan semua maklumat rasmi (termasuk yang berada di dalam peranti storan) disimpan di tempat yang selamat dan berkunci.

Sentiasa imbas peranti storan sebelum menggunakannya

4 ELAK TERPEDAYA

Elakkan daripada terus mempercayai kandungan laman web, blog dan emel yang diragui atau daripada orang yang tidak dikenali.

Semak dan rujuk kepada sumber-sumber yang sahih.


Elak guna emel dan kata laluan peribadi pada akaun media sosial
Sentiasa *log out* akaun media sosial
Elak kongsi maklumat peribadi & rasmi di media sosial
Elak muat turun aplikasi yang diragui
Elak guna media sosial sewaktu pejabat
5
SOSIAL
INTERNET & MEDIA
MENGGUNAKAN
BERETIKA
Tidak mendedahkan maklumat rasmi
Elak komen berbentuk serangan peribadi
Elak langgar hak cipta atau harta intelek
Elak guna wi-fi umum untuk kerja rasmi
Kenal pasti rakan media sosial anda

6 WASPADA JENAYAH SIBER

Jangan benarkan individu lain menggunakan identiti dan kata laluan akaun emel dan media sosial anda.

Elak layari laman web dan blog lucah, fitnah, hasutan, skim cepat kaya & ideologi keganasan.

Elak sebar kandungan lucah, fitnah, hasutan, skim cepat kaya & ideologi keganasan.

Jangan mudah terpedaya dengan tawaran atau maklumat daripada individu yang tidak dikenali melalui emel atau media sosial.

7 FIKIR SEBELUM KLIK

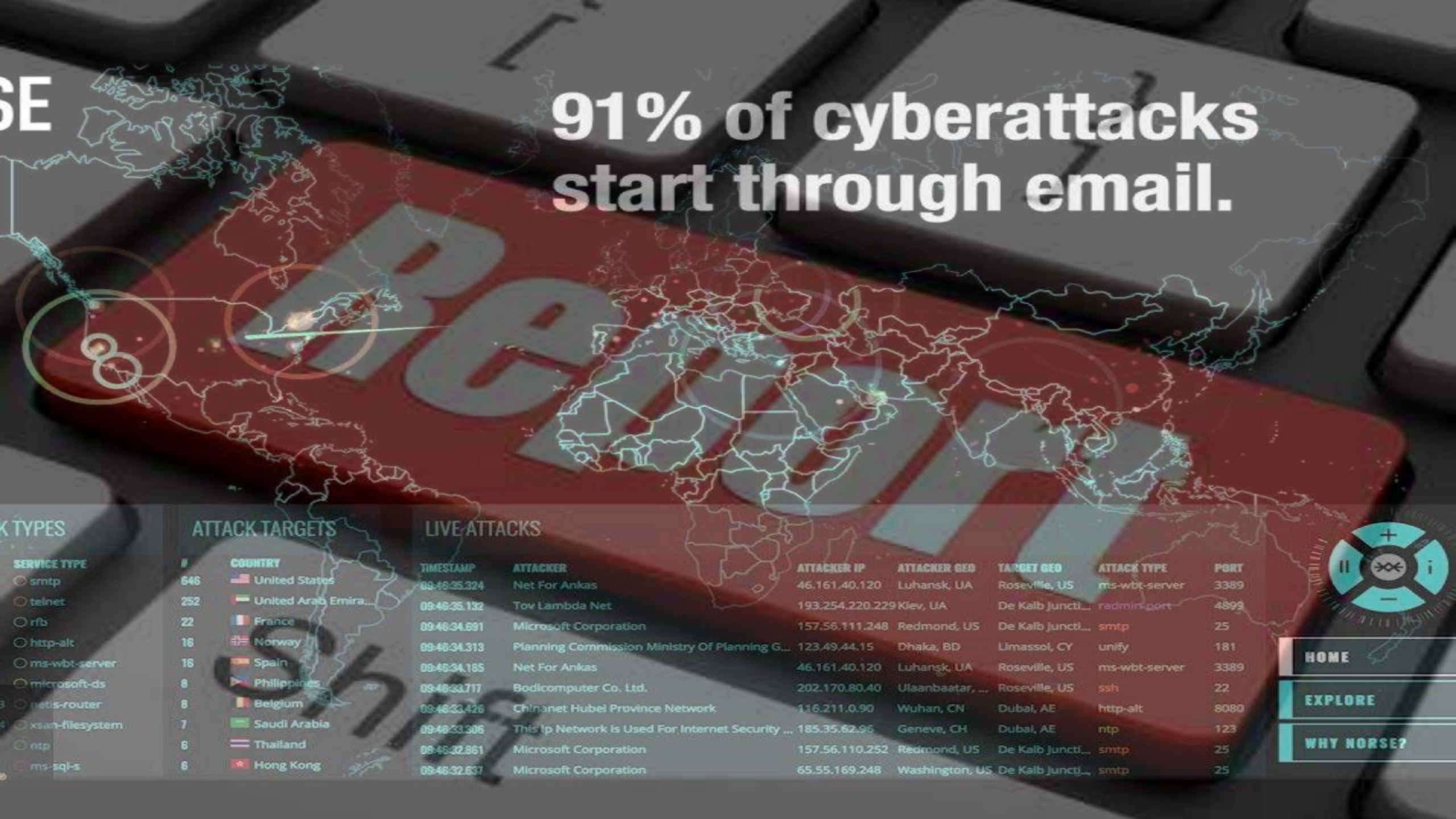
Jangan klik pada e-mel, pautan atau lampiran yang mencurigakan (termasuk dari orang yang tidak dikenali). Padamkan e-mel tersebut.

TABAYYUN

LAPORKAN

8

- ✓ Laporkan sebarang insiden kebocoran maklumat kepada pihak berkaitan.
- ✓ Laporkan dengan segera kehilangan sebarang aset ICT kerajaan (seperti peranti storan, komputer riba, komputer).
- ✓ Laporkan e-mel atau pautan yang mencurigakan atau dari orang yang tidak dikenali kepada Bahagian Teknologi Maklumat.
- ✓ Laporkan kepada pihak berkuasa sekiranya berlaku sebarang insiden jenayah siber seperti penipuan Internet.


91% of cyberattacks
start through email.
K TYPES
SERVICE TYPE
smtp
telnet
rfb
http-alt
ms-wbt-server
microsoft-ds
netis-router
xsan-filesystem
ntp
ms-sql-s
ATTACK TARGETS
COUNTRY
646 United States
252 United Arab Emira...
22 France
16 Norway
16 Spain
8 Philippines
8 Belgium
7 Saudi Arabia
6 Thailand
6 Hong Kong
LIVE ATTACKS
TIMESTAMP ATTACKER ATTACKER IP ATTACKER GEO TARGET GEO ATTACK TYPE PORT
09:46:35.324 Net For Ankas 46.161.40.120 Luhansk, UA Roseville, US ms-wbt-server 3389
09:46:35.132 Tov Lambda Net 193.254.220.229 Kiev, UA De Kalb Juncti... radmin-port 4899
09:46:34.691 Microsoft Corporation 157.56.111.248 Redmond, US De Kalb Juncti... smtp 25
09:46:34.313 Planning Commission Ministry Of Planning G... 123.49.44.15 Dhaka, BD Limassol, CY unify 181
09:46:34.185 Net For Ankas 46.161.40.120 Luhansk, UA Roseville, US ms-wbt-server 3389
09:46:33.717 Bodlcomputer Co. Ltd. 202.170.80.40 Ulaanbaatar, ... Roseville, US ssh 22
09:46:33.426 Chinanet Hubei Province Network 116.211.0.90 Wuhan, CN Dubai, AE http-alt 8080
09:46:33.306 This Ip Network Is Used For Internet Security ... 185.35.62.96 Geneve, CH Dubai, AE ntp 123
09:46:32.861 Microsoft Corporation 157.56.110.252 Redmond, US De Kalb Juncti... smtp 25
09:46:32.637 Microsoft Corporation 65.55.169.248 Washington, US De Kalb Juncti... smtp 25
HOME
EXPLORE
WHY NORSE?

9 AMBIL TAHU

Peka dengan trend ancaman siber terkini.

01

Peka, fahami dan waspada mengenai kesan-kesan negatif akibat penyalahgunaan internet.

02

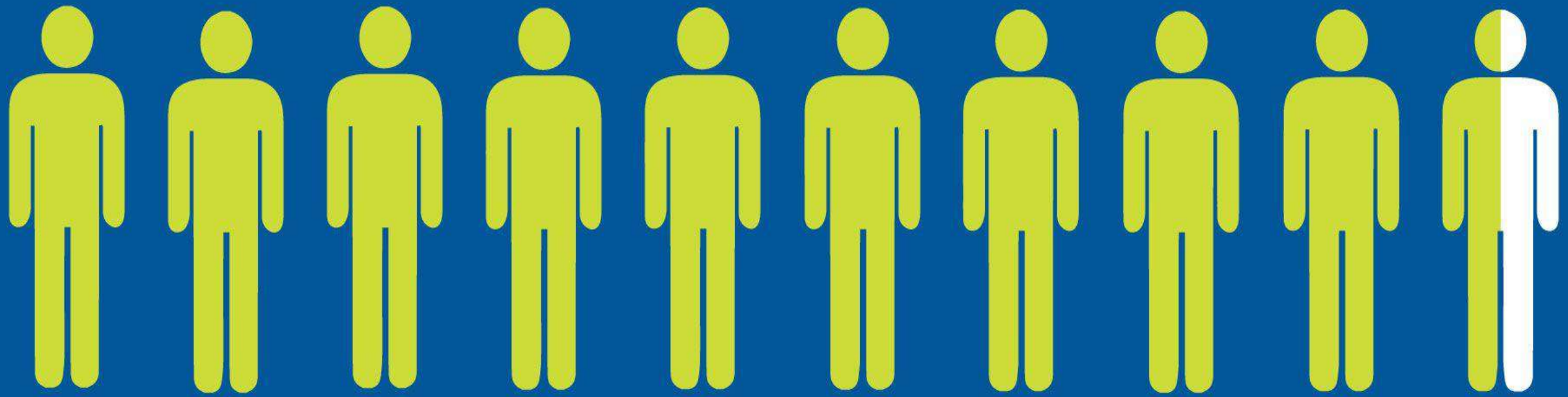
10
PATUHI

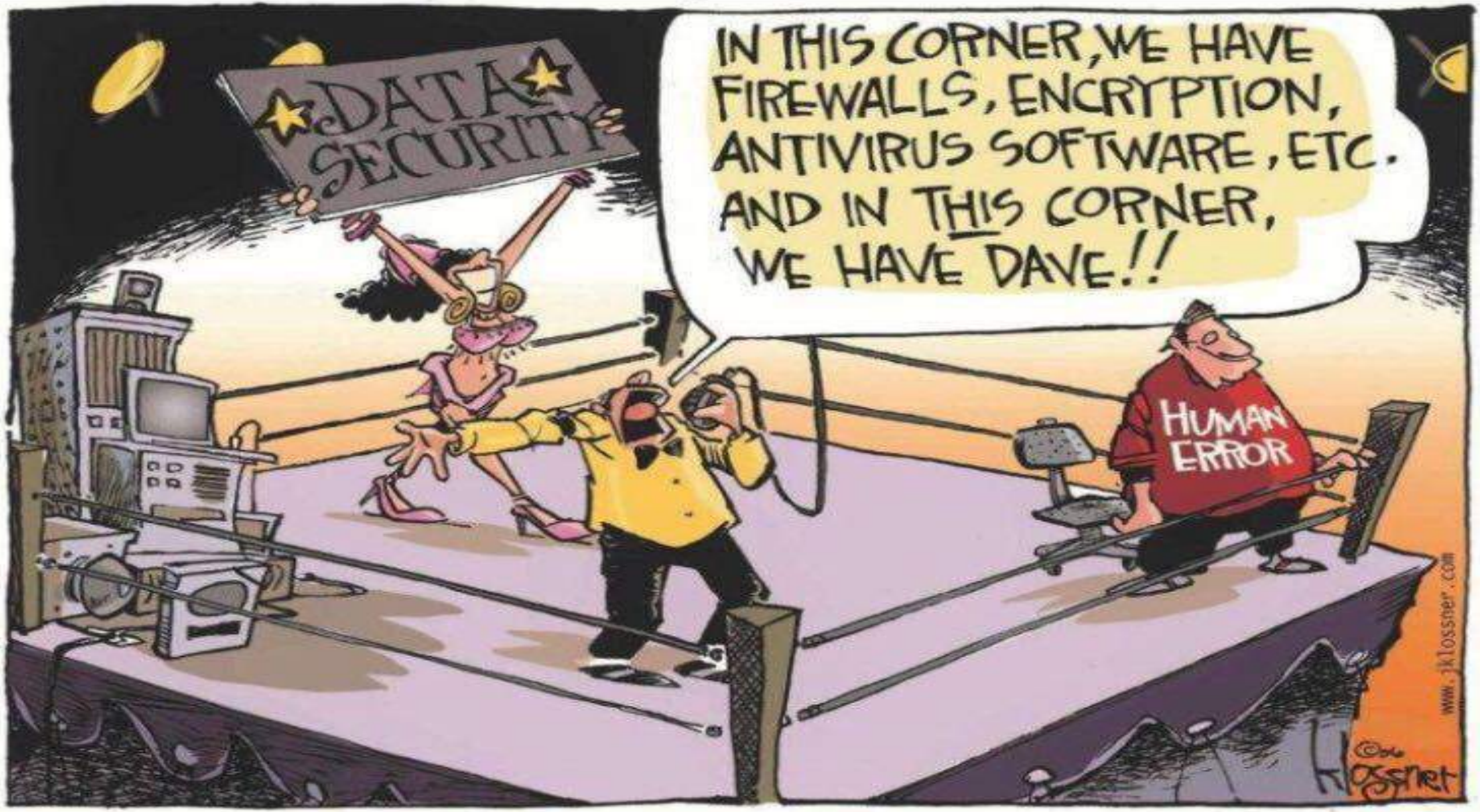
Ketahui dan patuhi polisi, arahan, peraturan, garis panduan dan pekeliling berkaitan keselamatan siber yang dikeluarkan oleh agensi/organisasi anda dan Kerajaan.

95%

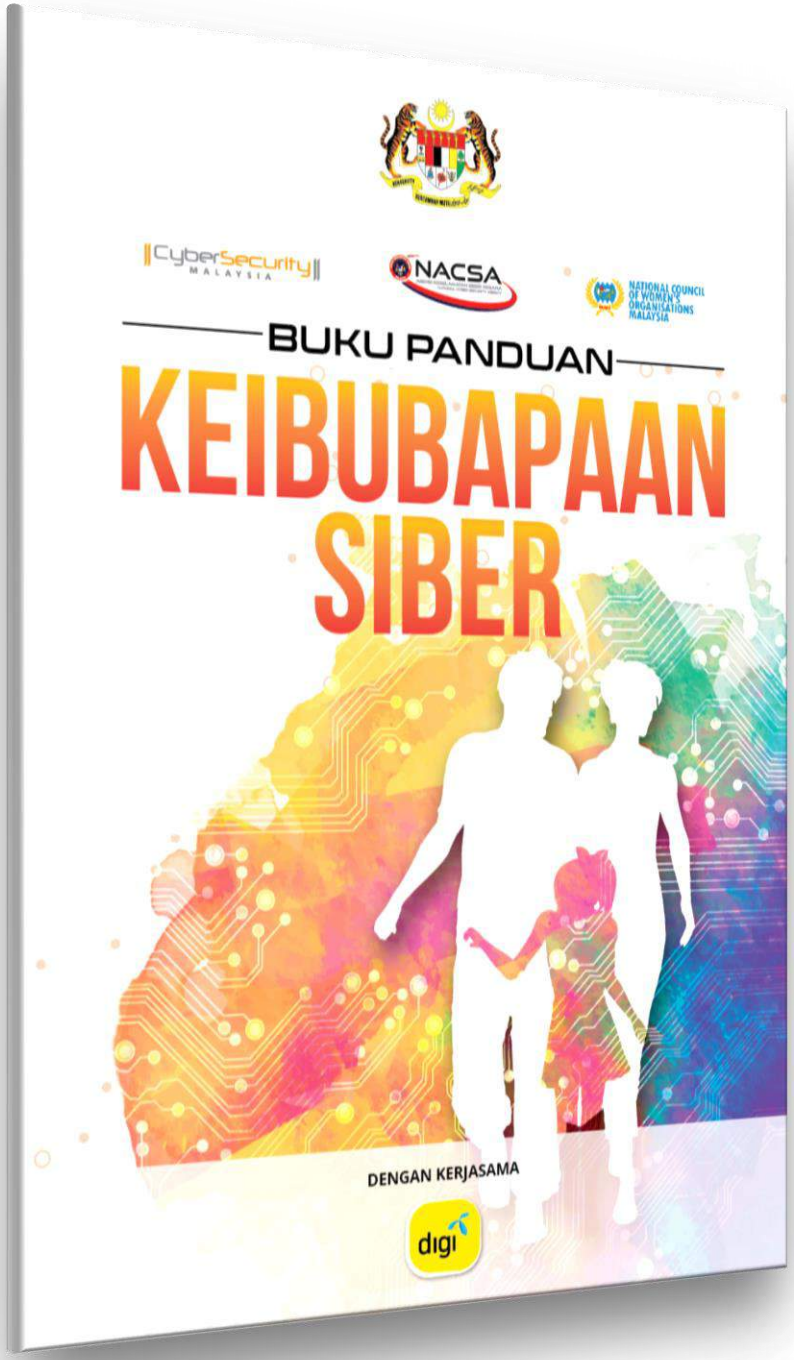
of all successful cyber attacks is caused by human error

Source: IBM Cyber Security Intelligence Index




DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com


S O A L J A W A B



- **Boleh dimuat turun di www.cybersafe.my**

fairuz@mkn.gov.my

03 – 8064 4805

TERIMA KASIH

NACSA
AGENSI KESELAMATAN SIBER NEGARA
NATIONAL CYBER SECURITY AGENCY

AGENSI KESELAMATAN SIBER NEGARA
MAJLIS KESELAMATAN NEGARA
JABATAN PERDANA MENTERI
ARAS G & LG, BLOK BARAT
BANGUNAN PERDANA PUTRA
62502 PUTRAJAYA
TEL: 03-8064 4843
FAKS: 03-8064 4848