CYBER SECURITY

Kamaruddin Mahad
Certified Secure Computer User (CSCU) Certified
Certified Ethical Hacker (CEH)
Ec-Council Certified Security Specialist (ECSS)

Bahagian Keselamatan ICT

TAHUKAH ANDA?

59.5% = 4.66 billions

Penduduk dunia terhubung dengan internet.

Sumber: https://www.statista.com (7 April 2021)

31.79 millions

Pengguna internet di MALAYSIA.

Sumber: https://www.statista.com (7 April 2021)

APAKAH ITU 'KESELAMATAN SIBER'?

Keselamatan Siber adalah keupayaan untuk melindungi atau mempertahankan penggunaan ruang siber dari serangan siber .

Sumber: National Institute of Standards and Technology (NIST)

What is Cyber Security ?

CYBER
(technology)

SECURITY
(protection)

User

System

Device

Network

Programs

Data

APAKAH 'SERANGAN SIBER'?

Serangan yang bertujuan untuk mengganggu, melumpuhkan, memusnahkan atau menganiaya suatu persekitaran infrastruktur pengkomputeran atau memusnahkan integriti data atau mencuri maklumat terkawal.

TAHUKAH ANDA?

Penggodam menyerang setiap 39 saat, purata 2,244 kali sehari.

Sumber: University of Maryland

Purata 30,000 laman web baru digodam Setiap hari.

Sumber: Forbes

TAHUKAH ANDA?

Penggodam mencuri 75 rekod setiap saat

Sumber: Breach Level Index

73% penggodam topi hitam mengatakan keselamatan firewall tradisional dan antivirus Tidak relevan atau usang.

Sumber: Thycotic.com

TAHUKAH ANDA?

Penggodam membuat 300,000 perisian *malware* baru setiap hari.

Sumber: McAfee

SIAPA MANGSA SERANGAN SIBER?

- Agensi Kerajaan
- Syarikat Swasta
- Perbankan & Kewangan
- Syarikat Tenaga
- Institusi Pendidikan
- Media
- ANDA

Cyber criminals don't attack your computer. They attack YOU!

Why Cyber Security is Important

The rise of cybercrime

Damage to companies

The barrier to entry is low

Cyber attack comes with low risk

Bad actors are constantly innovating

Cyber crime offers high rewards

Utusan Malaysia | 11 Oktober 2020 | Page: 12 & 13

MUKADIMAH

Yang bijak pun boleh kena tipu

"Mana ada, tiada siapa yang kaya. Tauke dia saja kaya. Skim cepat kaya, pelaburan tak wujud, sering diuar-uarkan."

"Macam *Macau Scam* sekarang. Kita tengok, mangsa ditipu dan wang disalur masuk ke akaun lain. Kalau kita tak ambil tindakan, AMLA tak bertindak pantas, duit itu akan lesap."

RM126 juta hasil Macau Scam, penipuan online disita

Oleh MALINDA ABDUL MALIK

KUALA LUMPUR – Bahagian Siasatan Jenayah Pengubahan Wang Haram (BSJPWH) Bukit Aman menyita lebih RM126 juta hasil kegiatan Macau Scam, jenayah terancang (Sosma), penipuan dan judi online dalam tempoh 11 bulan tahun ini.

Daripada jumlah itu, lebih RM93 juta sitaan membabitkan wang di dalam akaun bank dan diikuti hartanah (RM17,875,000), pelbagai kenderaan (RM9,022,725), wang tunai (RM3,616,144), cek bernilai RM20,429 dan 116,549,185 unit saham.

Pengarah Jabatan Siasatan Jenayah Komersial (JSJK) Bukit Aman, Datuk Zainuddin Yaacob mendedahkan, sebanyak 158 kertas siasatan dibuka dalam tempoh 11 bulan tahun ini berkaitan kes berskala besar termasuk Macau Scam, jenayah terancang (Sosma), Ops Khazanah, penipuan dan judi online.

Katanya, 124 kertas siasatan dibuka oleh JSJK manakala Jabatan Siasatan Jenayah (33) dan Jabatan Siasatan Jenayah Narkotik (1).

"Sepanjang tahun 2019 kita buka 138 kertas siasatan, namun tahun ini menunjukkan peningkatan sebanyak 20 kes walaupun berbaki sebulan sebelum akhir tahun.

"Walaupun kertas siasatan bagi tahun 2019 dibuka sedikit berbanding 11 bulan tahun ini, namun jumlah sitaan tahun lepas mencecah RM1.2 bilion susulan kes 1Malaysia Development Berhad (1MDB)," katanya dalam wawancara khas bersama media di Menara KPJ, Jalan Tun Razak baru-baru ini.

ZAINUDDIN

ZAINUDDIN (kiri) menunjukkan antara pelbagai jenis kereta mewah yang dirampas sepanjang tahun ini.

Mengulas mengenai pembekuan dan pelucuthakan harta, Zainuddin berkata, sesuatu harta yang disyaki hasil daripada aktiviti haram akan dibekukan untuk menghalang penjenayah melakukan apa-apa transaksi berkaitan harta tersebut mengikut Seksyen 44 Akta Pencegahan Pengubahan Wang Haram dan Pencegahan Pembiayaan Keganasan 2001 (AMLATFA).

Jelas beliau, tempoh pembekuan itu akan berkuat kuasa selama 90 hari dari tarikh perintah pembekuan dikeluarkan sebelum tindakan penyitaan dilakukan.

"Tindakan penyitaan harta diambil mengikut Seksyen 45, 50 dan 51 AMLATFPUAA 2001 mengikut jenis harta dan penyitaan bermula selepas tempoh pembekuan tamat. Tempoh penyitaan pula, akan berkuat kuasa selama 12 bulan dari tarikh perintah penyitaan.

"Setelah selesai siasatan, tindakan lanjut yang boleh dikenakan adalah mendakwa penjenayah atas kesalahan pengubahan wang haram termasuk melucutkan harta tersebut kepada kerajaan atau pelepasan semula kepada pihak ketiga, namun tindakan itu mesti menerusi proses perbicaraan di mahkamah," ujarnya.

Tambah beliau, dalam tempoh 11 bulan tahun ini lebih RM25 juta pelucuthakan harta berjaya dilakukan.

"Sebanyak 20 kenderaan pelbagai model dilucut hak dan daripada jumlah itu tiga buah kenderaan diserahkan untuk kegunaan JSJK, tiga buah lagi diserahkan kepada Polis Kontinjen Johor serta Kontinjen Kuala Lumpur untuk kegunaan rasmi dan penugasan kepolisan.

"Selain itu, lebih RM18 juta pelepasan harta diberikan bagi tahun 2020 kepada pihak ketiga iaitu pihak yang membuat tuntutan ke atas harta serta wang yang disita," katanya.

Sindiket 'parcel scam' lumpuh

MUHAMAD AFHAM RAMLI

KLANG - Sindiket 'parcel scam' yang aktif membabitkan penipuan jual beli barangan di sekitar daerah Klang lumpuh dengan tertangkapnya sembilan individu warga asing dalam dua serbuan berasingan di Taman Sentosa, di sini, awal pagi, semalam.

Ketua Polis Daerah Klang Selatan, Asisten Komisioner Kamarul Zaman Mamat berkata, serbuan pertama pada jam 1 pagi di sebuah pangsapuri berjaya menahan tiga lelaki warga Nigeria dan dua wanita warga Filipina serta Thailand.

Menurutnya, hasil soal siasat, dua lagi lelaki warga Nigeria ditahan di sebuah pangsapuri lain di kawasan yang sama.

"Dalam serbuan tersebut, kita telah merampas beberapa peralatan seperti komputer riba pelbagai jenama, tablet, telefon bimbit, kad visa, dan beg yang mengandungi pelbagai dokumen," katanya.

Beliau turut mendedahkan sindiket yang aktif sejak tahun lalu itu akan menghantar bungkusan mengandungi barangan bernilai kepada mangsanya yang terdiri daripada wanita.

Menurutnya, sindiket itu akan menyamar dan berhubung dengan mangsa melalui laman sosial dan khidmat pesanan ringkas (SMS).

"Mereka mengarahkan mangsa untuk membuat bayaran melalui akaun bank milik warga tempatan jika ingin membuat tuntutan barangan tersebut.

"Mangsa yang terpedaya kemudian membuat bayaran dengan harapan memperoleh bungkusan tersebut," katanya.

Kamarul Zaman berkata, mangsa menyedari dirinya tertipu setelah pemeriksaan dengan pihak kastam mendapati barang yang dihantar tidak wujud.

Justeru, beliau menasihatkan orang awam supaya lebih berhati-hati dengan modus operandi membabitkan penghantaran bungkusan.

"Kesemua warga asing berusia 25 hingga 44 tahun direman 14 hari dan kes disiasat mengikut Seksyen 420 Kanun Keseksaan," katanya.

Antara lelaki warga Nigeria yang ditahan

Part 1: Cyber Security Threats

Cyber Security Threats

Is an **ACT** or **POSSIBLE ACT** which intends **to steal data** (personal or otherwise), **harm data**, or **cause some sort of digital harm**

Cyber Security Attack

A cyber attack is **an ASSAULT launched by cybercriminals** using one or more computers **against** a single or multiple computers or networks.

Types of Cyber Attack

Fraud

HACKING

COMPUTER VIRUSES

Ransomware

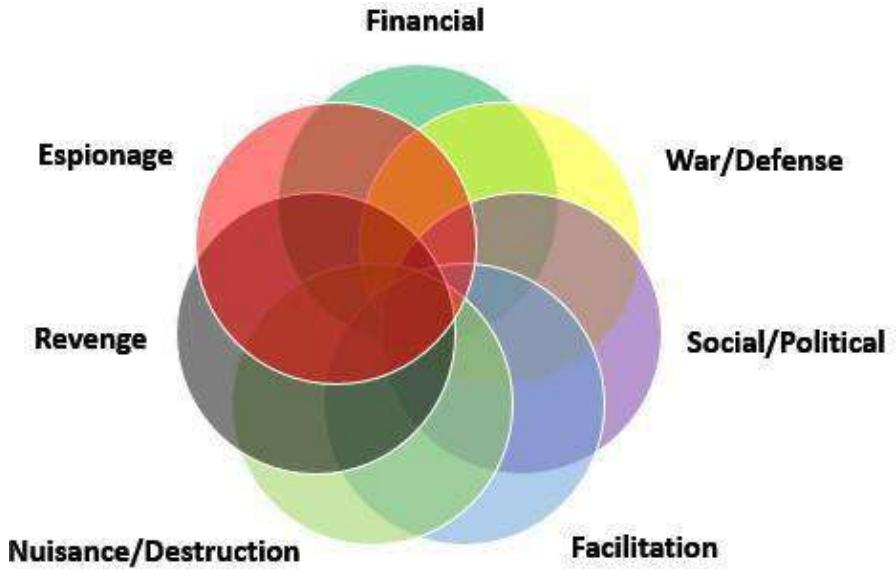
DDoS Attack

Botnets

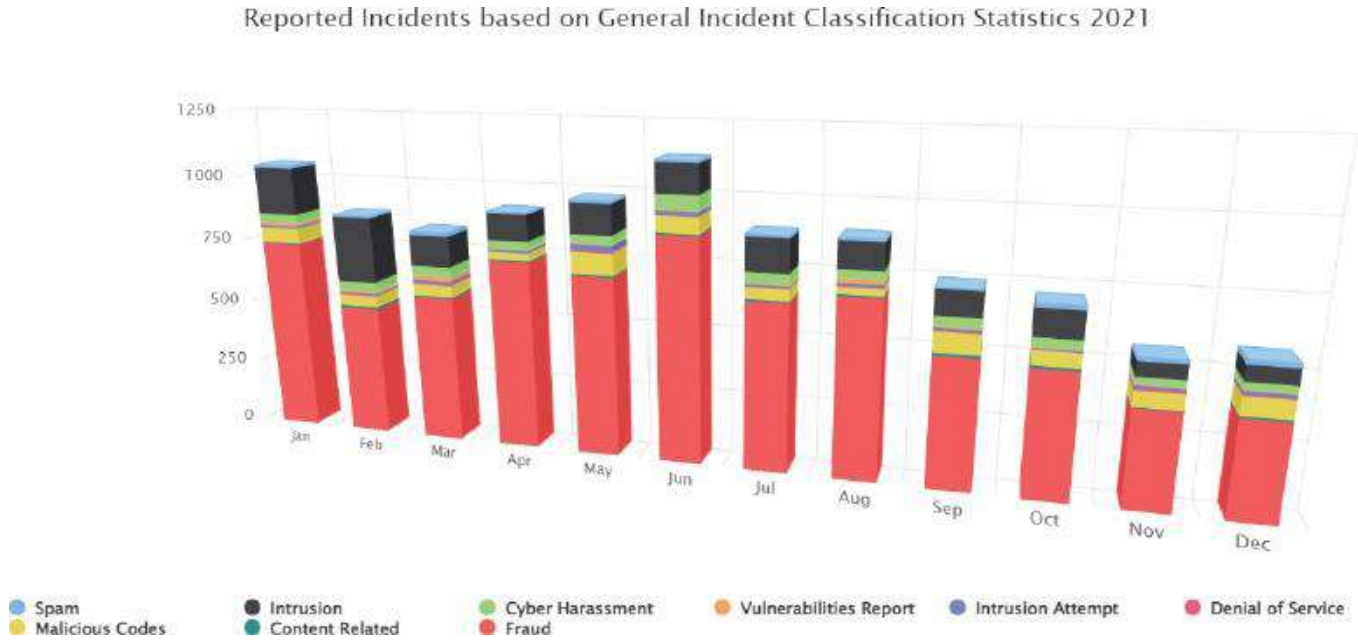
SCAMMING

Identity Theft

Motives of Cyber Security Threats



MyCert Incident 2021



MyCert Incident 2021

#	JAN	FEB	MAC	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Spam	10	4	11	5	8	4	7	6	6	14	13	14	102
Intrusion	178	252	119	100	116	112	126	101	94	102	54	56	1,410
Vulnerabilities Report	8	5	12	4	6	3	3	13	3	4	3	5	69
Intrusion Attempt	11	10	16	12	24	18	9	12	12	8	12	15	159
Denial of Service	1	2	3	1	3	0	1	2	3	0	4	2	22
Malicious Codes	58	44	42	29	83	64	44	25	76	53	60	70	648
Content Related	2	11	10	6	9	5	8	7	12	12	3	6	91
Fraud	746	502	566	726	689	861	639	680	490	473	365	361	7,098
	1,049	867	819	912	968	1,122	878	880	731	696	539	555	10,016

Threats During Movement Control Order (MCO)

- Throughout the Movement Restriction Order (MCO), MyCERT observed an increase in various cyber security attacks capitalizing the COVID 19 Pandemic.
- The threats that are using COVID 19 as theme uncovered during the MCO period are:
  - **COVID 19 Phishing emails/websites**
  - **COVID 19 Scam Domains**
  - **COVID 19 based malware**
  - **COVID 19 Android Malware**
  - **COVID 19 Vulnerable Sectors and Infrastructures (Health Sector)**

50 YEARS OF SHAPING THE NATION TOGETHER

TheStar

StarPlus | News | Asean+ | Business | Sport | Metro | Lifestyle | Food | Tech | Education

TOPICS | Euro Mania 2020 | Sabah & Sarawak | The New Normal | In 500 Words | Covid-19 Watch

Cybersecurity cases rise by 82.5%

THE EDGE MARKETS
MAKE BETTER DECISIONS

Home | Corporate | Sections | The Edge TV | Others | Frankly Speaking | EdgeProp.my

TRENDING NOW | SC Annual Report 2020 | Economic Recovery Plan | The Edge Covid-19 funds

MALAYSIA | TECHNOLOGY | MANAGEMENT | CORPORATE | TOP STORIES

Tech (Updated)

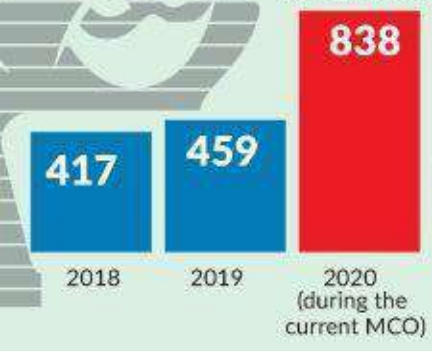
Digital transformation, rise of cyber threats on CEOs' concerns list — PwC survey

Syahirah Syed Jaafar / theedgemarkets.com
March 12, 2021 13:48 pm +08

Beware of cyberattacks!

Total number of incidents

> Cybersecurity cases increased by 82.5% during the MCO 2020 (March 18 to April 7) compared to the same period in 2019.



Tips to stay safe online

Working from home

> Update all systems including Virtual Private Networks (VPN) and devices with the latest security patches
> Alert employees about phishing attempts.
> Avoid logging in to your work environment using public Internet Wi-Fi. Connect through your home or mobile network data.
> Enable Multi Factor Authentication.

Covid-19 scams

> Always verify information from emails, text messages and social media posts about Covid-19.
> Do not share personal or financial information in emails
> Do not click on suspicious links provided to you on Covid-19, verify with the sender or agencies that can help.
> Use legitimate, government websites for up-to-date, fact-based information

Video teleconferencing apps

> Use the latest version of apps and security software
> Only download software from its official website or app store.
> Never share confidential information during a meeting
> Enable non-recordable videos and audio, and limit file sharing.
> If something is suspicious, log out.
> If you lose your computer or mobile phone, log out from all clients immediately and change your login password.
> Do not share or publish the confer
> Log out from the app after a meeting.

Source: CyberSecurity Malaysia

Risk and Cyber Threat: From Home

Virus, Malware, Ransomware

Social Engineering and Phishing Scheme, Online Fraud

Possibility of confidential and sensitive information leakage

Social Media Exposure

Unsecured network
Personal device connect to office remotely

Social Engineering

A combination of social, psychological and information gathering techniques that are used to manipulate people for nefarious purposes

- ✓ Phishing: tactics include deceptive emails, websites, and text messages to steal information.
- ✓ Spear Phishing: email is used to carry out targeted attacks against individuals or businesses.
- ✓ Baiting: an online and physical social engineering attack that promises the victim a reward.
- ✓ Malware: victims are tricked into believing that malware is installed on their computer and that if they pay, the malware will be removed.
- ✓ Pretexting: uses false identity to trick victims into giving up information.

Type of Online Fraud

Phishing

FAKE

LHDN
MALAYSIA

After a review of your previous tax year payments, we are determined that you are eligible to receive a tax refund due to over payments in tax.

In order to claim your tax refund, please complete our tax refund form online by clicking below.

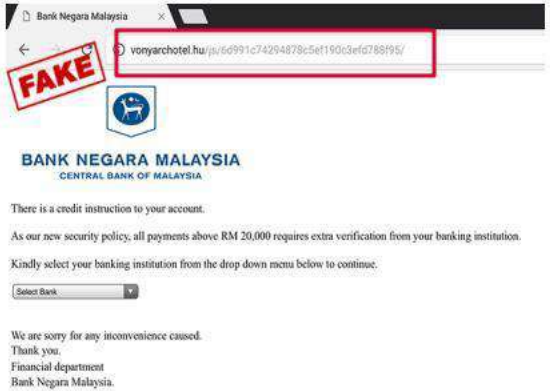
Get Started Now

Completed return amounts take 1 to 2 days to appear on your account.

Thank you,

Inland Revenue Board of Malaysia

Beware!
The hyperlink will re-direct you to a phishing (fake) website.



Last Reminder: Your package could not be delivered on 19.01.2021

POS MALAYSIA

Hello

Last Reminder: This Email informs you that your shipment is still pending.

Your package could not be delivered on 19.01.2021 because no customs duty was paid (MYR 6.66)

Pay To : POS Malaysia Berhad
Payment of Order: 20210115-54605
Net Charges : MYR 6.66
Delivery scheduled between : 20.01.2021 - 21.01.2021

- To confirm the shipment of your package Click here .

You will receive an email or SMS when you arrive in your home address. You will have 8 days, from the date of availability, to withdraw the package. Upon withdrawal, you will be asked for ID.

- For more services, find the follow-up of your shipment by Clicking here .

Thank you for your trust,

MACAU SCAM

PENYAMARAN MELALUI TELEFON

Menyamar sebagai pegawai Bank / Polis / Mahkamah / SPRM dll ...

Ugut mangsa bahawa mangsa terlibat dalam aktiviti DADAH, PENGGUBALAN WANG HARAM, tunggakan KAD KREDIT dll.

Mangsa tidak dibenarkan memberitahu pasangan / keluarga / kenalan dengan alasan siasatan adalah sulit.

Saspek meminta maklumat semua akaun bank mangsa. Saspek meminta mangsa memindahkan wang ke akaun lain untuk tujuan siasatan.

SASARAN MANGSA

Warga emas/ golongan pencen

Orang kaya/ berharta

Golongan yang mudah cemas.

SCAM ALERT

#beSmart

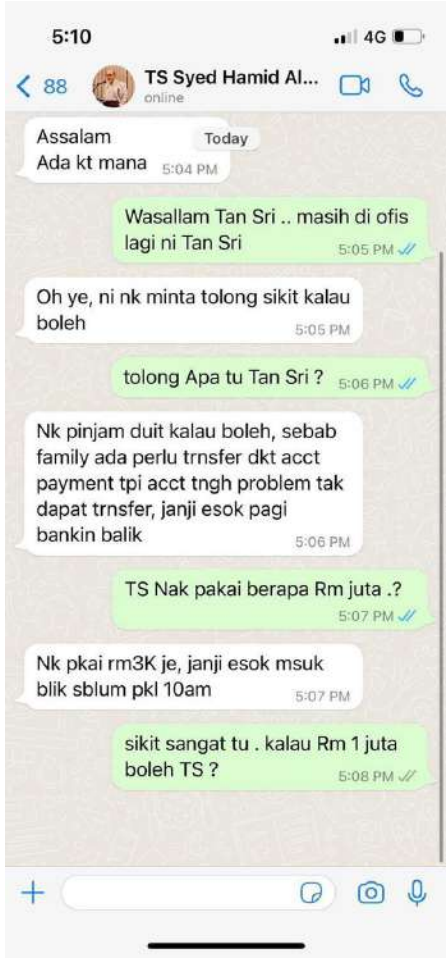
Astro AWANI
23 h ·

Mangsa berusia 52 tahun itu telah dihubungi seorang lelaki yang memperkenalkan diri sebagai pegawai mahkamah pada 4 Okt tahun lepas.

#AWANInews #AWANI745

ASTRO AWANI

Penjawat awam rugi lebih RM700,000 ditipu sindiket Macau Scam



MODUS OPERANDI LOVE SCAM

SCAM ALERT

#beSmart

HATI-HATI !!

sesiapa sahaja boleh menyamar melalui media sosial

Berkenalan melalui media sosial (FB, Wechat dll..) beberapa minggu / bulan.

Saspek menyamar tinggal di luar negara, ingin berniaga di Malaysia atau bekerja di syarikat minyak di Malaysia dll.

Saspek kemudian beritahu akan hantar hadiah dan wang tunai yang banyak kepada mangsa melalui courier.

Mangsa akan dihubungi oleh pihak courier atau kastam.

Mangsa kemudian diminta membuat beberapa bayaran cukai, insurans dll.

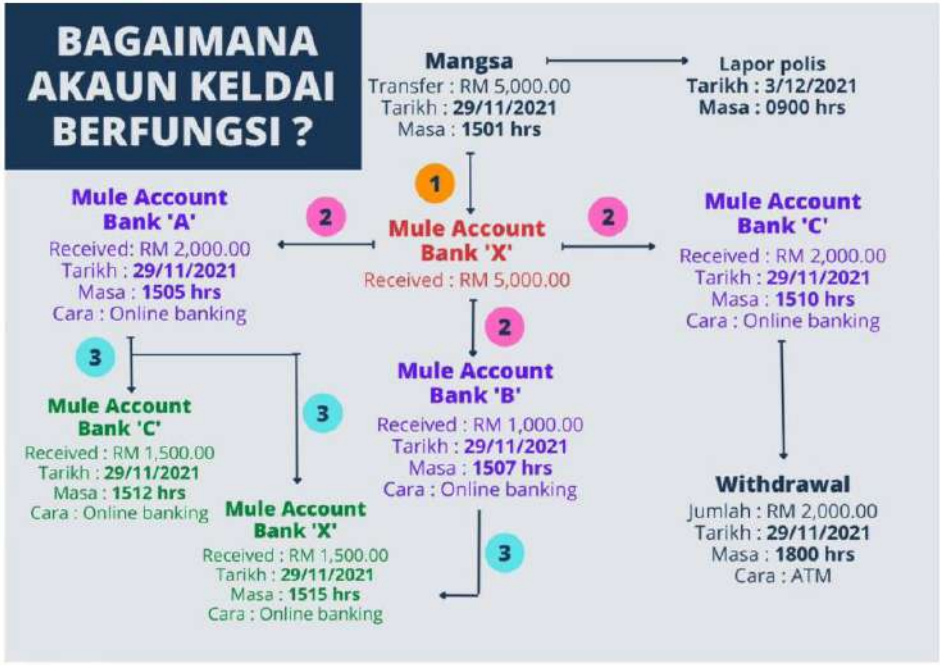
Mangsa membuat bayaran ke beberapa akaun keldai dengan niat ingin membantu kekasih media sosialnya.

CIRI – CIRI MANGSA "LOVE SCAM"

- Mudah 'diayat' dengan kata – kata manis.
- Teringin kaya dalam sekelip mata.
- Punya kecenderungan untuk berkahwin dengan warganegara luar.
- Kesunyian.
- Suka melayan walaupun hanya sekadar sembang (chatting) di media sosial.
- Pernah gagal atau mempunyai masalah dalam perhubungan cinta atau perkahwinan.
- Boleh berkomunikasi menggunakan Bahasa Inggeris.

BE SM@RT


! BAHAYA !
KELDAI AKAUN
Pernah menyerahkan kad ATM anda kepada orang lain ??
Anda menerima bayaran dari urusan tersebut ??
Anda adalah KELDAI AKAUN!
Akaun anda mungkin digunakan untuk tujuan JENAYAH!
Anda boleh disabitkan dengan kesalahan di bawah Kanun Keseksaan !!
Semak nombor akaun terlibat dengan kes jenayah di :-
http://ccid.rmp.gov.my/semakmule
JABATAN SIASATAN JENAYAH KOMERSIL
POLIS DIRAJA MALAYSIA
http://ccid.rmp.gov.my
BE SM@RT


BAGAIMANA AKAUN KELDAI BERFUNGSI ?
Mangsa
Transfer : RM 5,000.00
Tarikh : 29/11/2021
Masa : 1501 hrs
Lapor polis
Tarikh : 3/12/2021
Masa : 0900 hrs
1
Mule Account Bank 'A'
Received: RM 2,000.00
Tarikh : 29/11/2021
Masa : 1505 hrs
Cara : Online banking
2
Mule Account Bank 'X'
Received : RM 5,000.00
2
Mule Account Bank 'C'
Received : RM 2,000.00
Tarikh : 29/11/2021
Masa : 1510 hrs
Cara : Online banking
3
Mule Account Bank 'C'
Received : RM 1,500.00
Tarikh : 29/11/2021
Masa : 1512 hrs
Cara : Online banking
3
Mule Account Bank 'X'
Received : RM 1,500.00
Tarikh : 29/11/2021
Masa : 1515 hrs
Cara : Online banking
2
Mule Account Bank 'B'
Received : RM 1,000.00
Tarikh : 29/11/2021
Masa : 1507 hrs
Cara : Online banking
3
Withdrawal
Jumlah : RM 2,000.00
Tarikh : 29/11/2021
Masa : 1800 hrs
Cara : ATM

Not secure | ccid.rmp.gov.my/semakmule/#

Jabatan Siasatan Jenayah Komersil
Polis Diraja Malaysia

Commercial Crime Investigation Department
Royal Malaysia Police

About | Vision & Mission | Commercial Crime Divisions | Laws | Others | Contact us

Semak Akaun Yang Ada Repot

Carian Telah Dibuat: 916,344 Carian [BSS 27]

Masukkan No Telefon : Masukkan Katakunci (Rapat)

Kategori : Nombor Telefon

Captcha : (Masukkan Maklumat Captcha)

Borang Soal Selidik | Semak Maklumat

Maklumat	AMARAN **0163088432** Ada **2 Repot** Telah Dibuat. *Untuk Maklumat Lanjut Sila Behubung Mana-mana Balai Polis Berhampiran.*

Jumlah Pelawat: 1,873,088 | Pelawat Hari Ini: 3,510
Paparan dalam sistem ini paling sempurna dengan menggunakan resolusi skrin 1280 x 800


PENYAMARAN PANGGILAN TELEFON
POS MALAYSIA
DHL
Mangsa terima panggilan dari saspek yang mengaku dari syarikat penghantaran (DHL, Pos Malaysia dll)
Saspek memberitahu bahawa terdapat bungkusan yang mengandungi sejumlah kad pengenalan, dadah dan barang salah yang lain yang dihantar ke alamat mangsa.
POLICE
Panggilan kemudian disambungkan kepada pihak Polis. Mangsa ditakutkan bahawa terlibat dengan jenayah berat.
Mangsa diminta untuk memindahkan wang ke akaun yang tidak dikenali dengan alasan untuk tujuan siasatan.
DITIPU !!
http://ecid.rmp.gov.my
BE SM@RT


PHONE SCAM
Fraudster will impersonate authorities asking victims' information and money for investigation purposes!
You're involve in illegal activities!
Transfer your money for investigation!
DO NOT BELIEVE !
if someone ...
notifies you via phone call that you're engaged in illegal activities.
asks you to transfer money to individual bank account.
tells you by a phone call that you will be arrested.
warn you not to tell anyone about your criminal offense.
IGNORE OR JUST HANG UP !

INFORMATION LEAKAGE

What information did Facebook leak?
Phone numbers, full names, locations, some email addresses, and other details from user profiles were posted to an amateur hacking forum on Saturday, Business Insider reported last week. The leaked data includes **personal information from 533 million Facebook users in 106 countries** -9 April 2021


Addiction
Child Trafficking
Child Porno
TMI
Social Media Exposure

Part 2: Cyber Security Vulnerabilities

Cyber Security Vulnerabilities

In cyber security, a vulnerability is a weakness which can be exploited by a cyber attack to gain unauthorized access to or perform unauthorized actions on a computer system.

Vulnerabilities can allow attackers to run code, access a system's memory, install malware, and steal, destroy or modify sensitive data.

Case Study: KLIA Incidents 2019 not a cyber attack?

WHAT HAPPENED?

1. System Disruption At KLIA International Airport Occurred On 21st August2019
2. Flights Were Delayed Up to 20 flights per Day
3. Disruption Continued For Four Days costing Loss of RM1.2 M

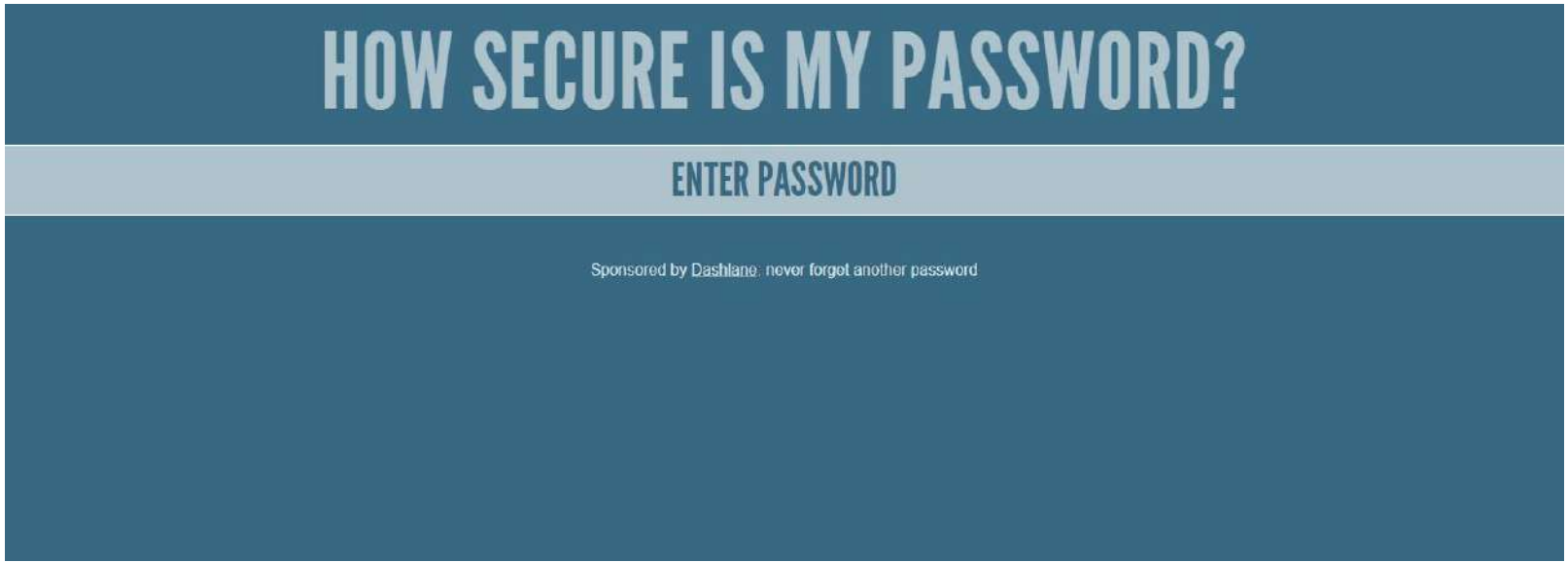
MAIN CAUSE:

1. Lack of server Maintenance since 1998
2. Unavailable Disaster Recovery Centre
3. Lack of ICT expertise

Top 5 Cyber Security Vulnerabilities

- Poor endpoint security defenses – **hardware/ software**
- Poor data backup and recovery - **data**
- Poor network segmentation and monitoring – **network hardware/ software**
- Weak authentication and credential management - **people**
- Poor security awareness - **people**

How Secure Is My Password?



Part 3: Awareness

Awareness: Inisiatif Kerajaan

CyberSecurity

CyberSAFE™ MALAYSIA

NACSA
AGENSI KESELAMATAN SIBER NEGARA
NATIONAL CYBER SECURITY AGENCY

LANGKAH MUDAH
KESEDARAN KESELAMATAN SIBER

NACSA

10 LANGKAH MUDAH
KESEDARAN KESELAMATAN SIBER

1. GUNAKAN **KATA LALUAN**

2. **KEMASKINI** PERISIAN KESELAMATAN

3. **SIMPAN** DAN **LINDUNGI** MAKLUMAT

4. **ELAK** TERPEDAYA

5. **BERETIKA** MENGGUNAKAN INTERNET DAN MEDIA SOSIAL

6. **WASPADA** JENAYAH SIBER

7. **FIKIR** SEBELUM KLIK

8. **LAPORKAN**

9. **AMBIL TAHU**

10. **PATUHI**

Sumber: https://www.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/10-Langkah-Mudah-KKS_compressed.pdf

Awareness:Emel jabatan

Semak Cyber Crime Alert dari PDRM

https://www.facebook.com/CyberCrimeAlertRMP

CyberSecurity MALAYSIA

MyCERT

Malaysia Computer Emergency Response Team

Cyber999

Phone Call

1300-88-2999 24x7

Emergency: **+6019-266 5850**

Walk in to

Menara Cyber Axis, Cyberjaya

SMS

Format: Cyber999 Report send to **15888**

cyber999 [at]cybersecurity.my

Cyber999 Mobile Apps

ANDROID APP ON Google play

DOWNLOAD ON THE App Store

Download the form and fax to

03 – 8008 7000

More info: https://www.mycert.org.my


Prevention Methods to Overcome
Cyber Security Attacks

General Prevention Tips

Social Network Security

Don’t Link Accounts

Status update to specific people

Keep Birthdate Hidden

Don’t Accept Strangers (esp fine looking one)

Don’t Reveal Location

Have Private Profile

Change Setting from Public to Friends only

Review Friends lists

INFORMATION LEAKAGE

Clean Desk and Clear Screen Policy

Lock up all Confidential Documents

Always use privacy screen

Use password

Device Protection (location)

Paperless culture (no printout, no sticky note)

Clear up your thrash

Always google your name

Prevention Based on Threats

MALICIOUS CODES

- Install Anti-Virus/Malware Software.
- Keep Your Anti-Virus Software Up to Date.
- Run Regularly Scheduled Scans with Your Anti-Virus Software.
- Think Before You Click.
- Keep Your Personal Information Safe.
- Don’t Use Open Wi-Fi.

Prevention Based on Threats

- Download software from authorized websites
- Do not click on random email attachments
- Scan all types of hard drives before running
- Abstain from keeping easy passwords
- Never store or share your login information
- Importance of an Anti-hacking Software

HACKING

Prevention Based on Threats

- Keep Informed About Phishing Techniques
- Think Before You Click!
- Verify a Site's Security
- Check Your Online Accounts Regularly
- Keep Your Browser Up to Date
- Install an Anti-Phishing Toolbar
- Be Wary of Pop-Ups

Prevention Based on Threats

S PA M

Try to avoid opening spam emails and clicking on links in spam messages

Avoid ‘unsubscribe’ options

Don’t buy anything from a spammer

Use a disposable email address

Don’t be tempted to reply

Be wary about giving out your main email address

Munging – eg. (john@abc.com)
Written as John at abc dot com

Prevention Based on Threats

Secure Your Personal Records

Safeguard Your Personal Information Online

Limit What You Carry

Guard Against Tele-Theft

Protect Your Social Security Number

Use Passwords and Change Them Regularly

Be Vigilant When Travelling

Find Out If Your Records Were Affected After a Data Breach

IDENTITY THEFT

Two Factor Authentication – 2FA

PEMBERITAHUAN

AKTIFKAN PENYAHIHAN DUA-FAKTOR BAGI MENINGKATKAN TAHAP KESELAMATAN AKAUN MEDIA SOSIAL DAN APLIKASI PEMESEJAN ANDA

CYBERJAYA, 10 Februari 2022 --- Suruhanjaya Komunikasi dan Multimedia Malaysia (MCMC) ingin menasihatkan orang ramai supaya mengaktifkan penyahihan dua-faktor *('two-factor authentication'-2FA)* sebagai ciri keselamatan yang membantu melindungi akaun media sosial dan platform pemesejan segera anda selain daripada kata laluan anda.

Statistik trend aduan awam yang diterima oleh MCMC menunjukkan, jumlah aduan berkaitan penggodaman dan kehilangan akses telah meningkat sebanyak 55 peratus, iaitu 1,599 aduan pada tahun 2020 dan 2,483 aduan pada tahun 2021. Rata-rata pengadu memohon bantuan dan nasihat bagi mendapatkan kembali akses kepada akaun dan halaman milik atau kendalian mereka.

Risiko keselamatan sebegini menjadikan penggunaan 2FA lebih mendesak, kerana risiko penggodaman atau pengambilalihan akaun bukan sahaja boleh mengakibatkan kecurian identiti malah boleh membawa kepada penipuan melibatkan kerugian ribuan ringgit.

Lapisan keselamatan pertama secara umumnya adalah gabungan bersama nama pengguna *('username')* dan kata laluan *('password')*, yang telah digunakan sejak awal lagi. Namun, penggunaan kata laluan sebagai satu-satunya langkah keselamatan di alam maya adalah lemah dan terdedah kepada risiko penggodaman atau pengambilalihan akses.

Melalui 2FA, anda akan diminta untuk memasukkan kod log masuk atau kunci keselamatan khas bagi mengakses akaun. Anda juga boleh mendapatkan amaran *('alert')* apabila terdapat percubaan log masuk daripada pelayar atau peranti mudah alih yang tidak dikenali dan diminta mengesahkan percubaan log masuk anda setiap kali terdapat cubaan dibuat.

Sehubungan itu, aktifkan penyahihan dua-faktor bagi akaun anda sekarang. Maklumat lanjut berhubung pengaktifan penyahihan dua-faktor adalah seperti berikut:

1. **Facebook - Login alert and two-factor authentication:** www.facebook.com/help/148233965247823/
2. **Twitter – How to use two-factor authentication:** https://help.twitter.com/en/managing-your-account/two-factor-authentication
3. **Google 2-step verification:** https://www.google.com/landing/2step/
4. **Instagram two-factor authentication:** https://help.instagram.com/566810106808145
5. **TikTok – Keep your account secure:** https://www.tiktok.com/safety/youth-portal/keep-your-account-secure
6. **Whatsapp two-step verification:** https://faq.whatsapp.com/general/verification/how-to-manage-two-step-verification-settings
7. **Telegram – Active Sessions and Two-step verification:** https://telegram.org/blog/sessions-and-2-step-verification
8. **Signal PIN:** https://support.signal.org/hc/en-us/articles/360007059792-Signal-PIN

Orang ramai juga diminta untuk tidak klik kepada pautan-pautan mencurigakan yang diterima melalui e-mel serta sentiasa berwaspada dan berhati-hati dengan sebarang panggilan telefon atau mesej daripada mana-mana individu (sama ada yang dikenali atau tidak dikenali) yang meminta anda berkongsi kod khas seperti kod keselamatan *('Security Code')* kepada akaun media sosial serta aplikasi pemesejan anda. Perkongsian kod khas tersebut hanya akan memberi peluang mudah kepada pihak tidak bertanggungjawab bagi mengambil alih akaun media sosial atau aplikasi pemesejan anda.

JABATAN KOMUNIKASI KORPORAT MCMC

www.mcmc.gov.my

Sistem Pengurusan Keselamatan Maklumat
Information Security Management System (ISMS)

ISO/IEC 27001:2013

Wan Noor Asiah Bt Wan Mohamad Nawi
Perunding Latihan
Unit Keselamatan dan Privasi
INTAN Bukit Kiara
4-7 April 2017

LATAR BELAKANG

- Kerajaan Malaysia telah membuat pelaburan yang banyak ke atas aset Teknologi Maklumat dan Komunikasi (ICT): Infrastruktur, Teknologi, Aplikasi dan Proses.

- Demi memastikan bahawa **aset ICT Kerajaan digunakan dengan optimum dalam keadaan selamat untuk menyokong penyampaian perkhidmatan yang berkesan kepada pelanggan,** maka perlu digerakkan inisiatif ke arah jaminan kualiti sistem pengurusan keselamatan aset ICT Kerajaan.

LATAR BELAKANG

- Walaupun pelaksanaan program ICT di agensi agak memberangsangkan, namun banyak usaha yang perlu dilaksanakan termasuk **memperkukuh dan memastikan keselamatan aset ICT**.

- Dalam hal ini, Kerajaan harus mengambil initiatif untuk **mengamalkan sistem pengurusan keselamatan ICT yang berlandaskan kepada standard antarabangsa**.

PUNCA KUASA

Mesyuarat Jemaah Menteri pada 24 Februari 2010 telah bersetuju supaya agensi awam yang terlibat dalam sektor prasarana maklumat kritikal negara (CNII) mendapat pensijilan **ISMS ISO/IEC 27001:2007** dalam tempoh 3 tahun.

Ketua Pengarah MAMPU telah mengeluarkan **Surat Arahan: Pelaksanaan Pensijilan ISO/IEC 27001 dalam Sektor Awam** bertarikh 24 November 2010.

PANDUAN PELAKSANAAN ISO/IEC 27001 DALAM SEKTOR AWAM

- Panduan ini menjelaskan tindakan yang perlu diambil oleh semua kementerian, jabatan dan agensi Kerajaan Malaysia supaya mencapai taraf **ISO/IEC 27001 Sistem Pengurusan Keselamatan Maklumat**.

- Panduan ini mengandungi dua (2) bahagian:
  - ✓ Panduan Keperluan dan Persediaan Pelaksanaan Pensijilan ISMS ISO/IEC 27001 Sektor Awam; dan
  - ✓ Panduan Pelaksanaan Audit Dalam ISMS ISO/IEC 27001 Sektor Awam.

MANFAAT PENSIJILAN ISMS ISO/IEC 27001

- **Menjamin kesinambungan perniagaan** - melindungi maklumat yang menjadi aset kritikal perniagaan dari segi kerahsiaan, integriti dan ketersediaan. Perlindungan ini dilakukan dengan memastikan individu, proses, prosedur dan teknologi yang sesuai disediakan untuk melindungi aset maklumat

- Melindungi perniagaan anda, memberikan **keyakinan kepada pelanggan, pembekal dan pihak berkepentingan**

- **Menjimatkan sumber kewangan** bagi insiden keselamatan kerana kos bagi mencegah insiden keselamatan adalah lebih kecil berbanding kos mengendalikan tindakan pembetulan selepas insiden berlaku

MANFAAT PENSIJILAN ISMS ISO/IEC 27001

- Menggalakkan **penambahbaikan berterusan** yang akan memberikan kelebihan kepada perniagaan anda untuk bersaing dalam pasaran, menjadi lebih berjaya dan berdaya tahan

- Menitikberatkan **keperluan sumber manusia** yang seterusnya akan turut meningkatkan moral dan komitmen kakitangan dalam melindungi maklumat penting perniagaan

- **Mematuhi standard** memberikan anda pengiktirafan untuk kelebihan bersaing

- **Meningkatkan keberuntungan dan jaminan perniagaan**

EXAMPLE OF STANDARD

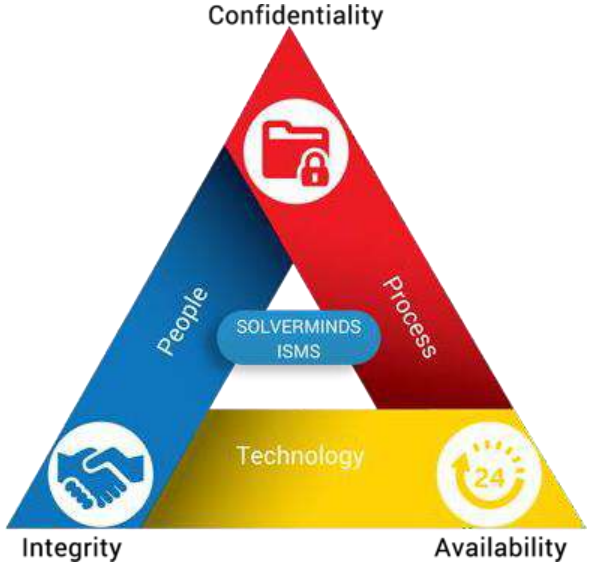
- ISO 9001: 2015 – Sistem Pengurusan Kualiti (QMS)
- ISO 14001:2015 - Sistem Pengurusan Alam Sekitar (EMS)
- 1722:2011 & OHSAS 18001:2007 - Sistem Pengurusan Kesihatan dan Keselamatan Pekerjaan (OSHMS)
- MS ISO 22000: 2012 - Sistem Pengurusan Keselamatan Makanan (FSMS)
- ISO/IEC 27001: 2013 - Sistem Pengurusan Keselamatan Maklumat (ISMS)
- ISO 50001:2011 - Sistem Pengurusan Tenaga (EnMS)

What is Information Security Management System (ISMS)

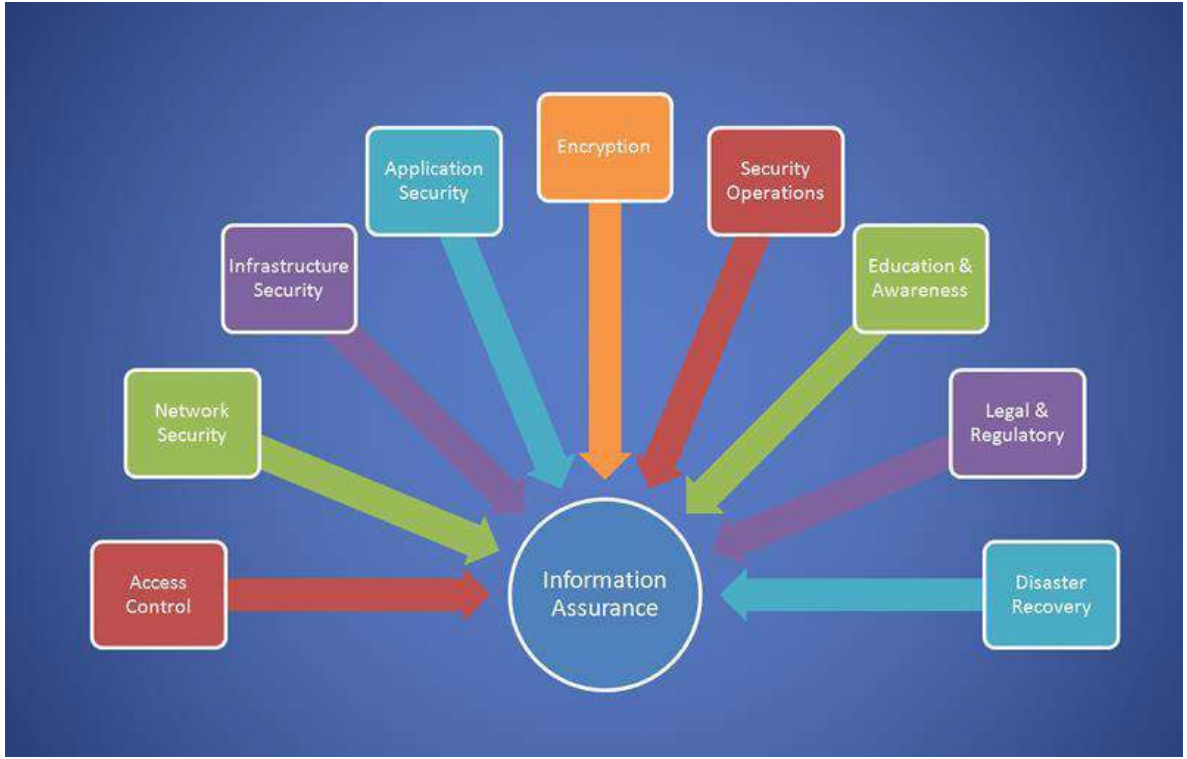
An information security management system (ISMS) is a set of policies concerned with information security management or IT related risks.

https://en.wikipedia.org/wiki/Information_security_management_system

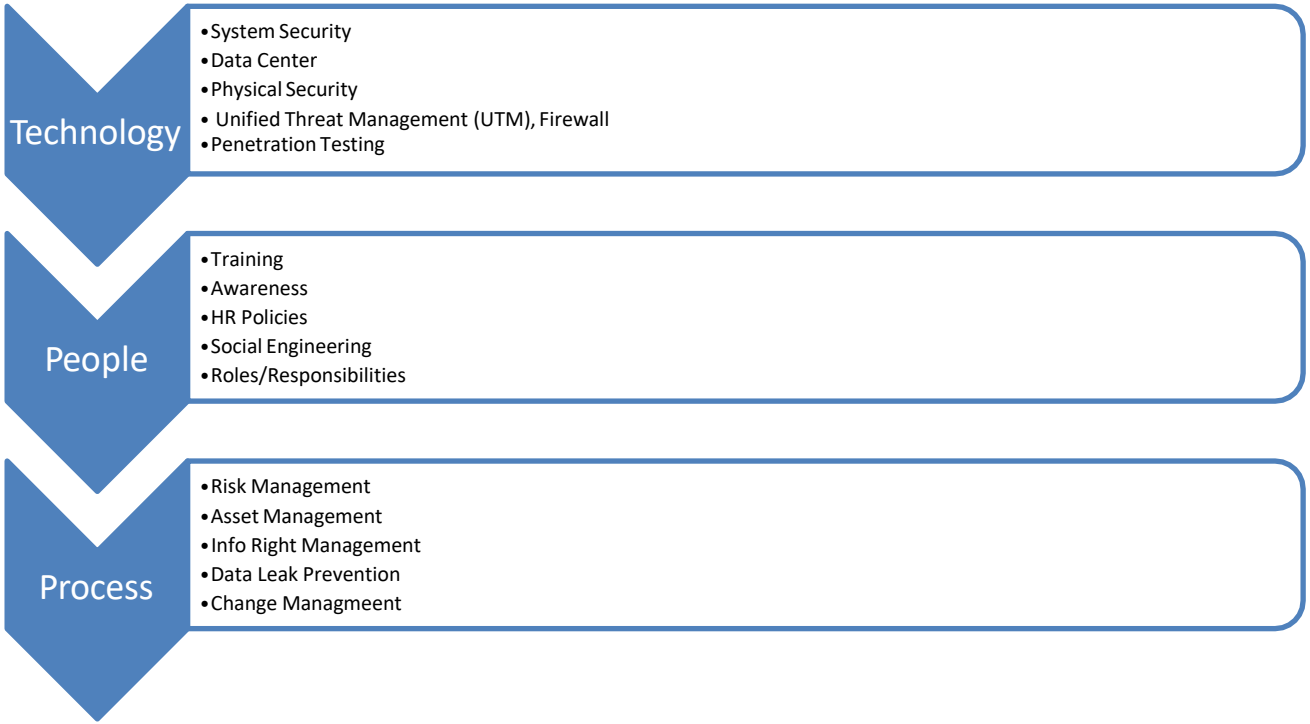
ISMS Initiative



ISMS Initiative



Some of the Controls Recommended by the Standard



ISO 27001 Family

The Family of ISO 27000 provides best practice recommendations on information security management, risks and controls within the context of an overall information security management system (ISMS), Alignment to management systems for quality assurance ISO 9000 Family

ISO 27000: Vocabulary

ISO 27001: Information Security Management System Requirements

ISO 27002: Code of Practices

ISO 27003: Information technology – Security techniques – Information security management system implementation guidance – Published 2010

ISO 27004: Information technology – Security techniques – Information security management – Measurement – Published 2009

ISO 27005: Information technology -- Security techniques -- Information security risk management – Published 2011

ISO 27006: Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems – Published 2011

ISO 27007-ISO 27008: Information technology -- Security techniques -- Guidelines for auditors on information security controls – Published 2011

ISO 27011: Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 – Published 2008

ISO 27799: Health informatics -- Information security management in health using ISO/IEC 27002 Published 2008


INTERNATIONAL STANDARD
ISO/IEC 27000
Third edition
2014-01-15
Information technology — Security techniques — Information security management systems — Overview and vocabulary
Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire

Benefits of ISO 27001

ISO/IEC 27001:2013 Implementation, Certification from a certification body demonstrates that the security of organization information has been addressed, valuable data and information assets properly controlled.

Also there is List of benefits By achieving certification to ISO/IEC 27001:2013 organization will be able to acquire numerous benefits including:


SEC_RITY
is not complete without U!


thank
you