Strategi Mencegah Kebocoran Data

Webinar SANDIKAMIMANIA Series 20
31 Januari 2022

Digit Oktavianto
@digitoktav
https://medium.com/@digit.oktavianto

About Me

- Infosec Consulting Manager at Mitra Integrasi Informatika
- Co-Founder BlueTeam.ID (https://blueteam.id)
- Born to be DFIR Team
- Community Lead @ Cyber Defense Community Indonesia
- Member of Indonesia Honeynet Project
- Opreker and Researcher
- {GCIH | GMON | GCFE | GICSP | CEH | CSA | ECSA | ECIH | CHFI | CTIA | ECSS} Certifications Holder

Agenda

- Kebocoran Data
- Tren Keamanan Tahun 2022
- Tips Aman Bekerja di Jaringan Komputer

Data Breach di Indonesia

KOMPAS.com NEWS TREN HEALTH FOOD EDUKASI INSPIRASLI MONEY TEKNO LIFESTYLE HOMEY PROPERTI BOLA TRAVEL

BAGIKAN: Penjelasan KreditPlus Soal Kebocoran Data Nasabah

Iklan oleh Google

Kirim masukan

Mengapa iklan ini?

Home / Money / Whats New

Penjelasan KreditPlus Soal Kebocoran Data Nasabah

Kompas.com - 05/08/2020, 14:35 WIB

BAGIKAN:

Komentar

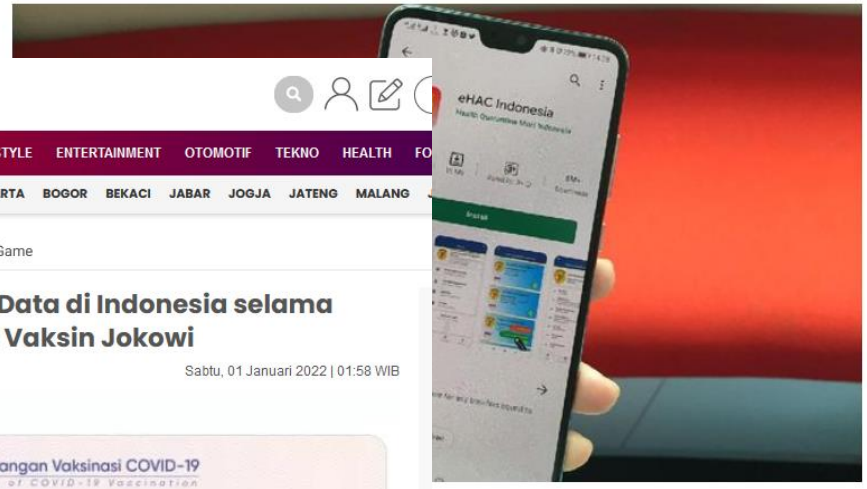
CNN Indonesia Home Nasional Internasional Ekonomi Olahraga Teknologi Hiburan Gaya Hidup CNN TV

Home > Teknologi > Teknologi Informasi

Deretan Kasus Bocor Data Penduduk RI dari Server Pemerintah

CNN Indonesia | Rabu, 01/09/2021 15:50 WIB

Bagikan :



CNN Indonesia Home Nasional Internasional Ekonomi Olahraga Teknologi Hiburan Gaya Hidup CNN TV

Home > Teknologi > Teknologi Informasi

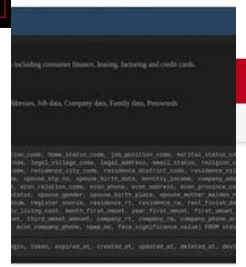
Kebocoran Data Pribadi yang Tak Berujung di RI

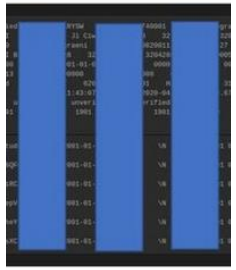
M. Ikhsan | CNN Indonesia

Kamis, 13 Jan 2022 06:48 WIB

Bagikan :

Data pribadi yang bocor dijual di Raid Forum atau sebuah forum jual beli data. (Foto: dok. Screenshot Raid Forums)





ternet. (Cyble Inc)

suara.com

NEWS BISNIS BOLA SPORT LIFESTYLE ENTERTAINMENT OTOMOTIF TEKNO HEALTH FO

yOursay.id Cek Fakta Infografis JAKARTA BOGOR BEKACI JABAR JOGJA JATENG MALANG

TEKNO / Internet / Gadget / Tekno / Sains / Game

Daftar Kasus Kebocoran Data di Indonesia selama 2021, Termasuk Sertifikat Vaksin Jokowi

Liberty Jemadu | Dicky Prastya

Sabtu, 01 Januari 2022 | 01:58 WIB

Ada beberapa kasus kebocoran data di Indonesia selama 2021. Salah satu yang paling ramai adalah tersebarnya sertifikat vaksin Jokowi. Foto: Tangkapan layar sertifikat vaksin dengan nama Presiden Jokowi di PeduliLindungi. (Twitter)

ta pribadi pada aplikasi ementerian Kesehatan ().

bocoran data lain yang k Indonesia dari KPU dan


YOU GET A DATA BREACH, AND YOU GET A DATA BREACH....
EVERYONE GETS A DATA BREACH!!!!
memegenerator.net

Trend Era (Cyber) Criminal As A Service

Dalam 10 tahun terakhir, dunia underground security telah berevolusi dengan cepat, dari group hacking yang masih dalam circle yang sempit, mulai dari having fun seperti phreaking, deface, **menjadi sebuah industry cyber criminal yang telah mengakibatkan kerugian secara global dalam dunia ekonomi** berkisar USD 300 Juta dalam 1 tahun[1]

Kita akan membahas dalam sharing session ini, bagaimana :

- Threat Actor melakukan shifting dari cara kerja dalam melakukan aktivitas cyber criminal untuk mendapatkan uang lebih banyak,
- Bagaimana kita semua cepat atau lambat suatu saat akan menjadi korban mereka
- Bagaimana kita menghadapi situasi tersebut, dan menghindari agar kita tidak menjadi korban

[1] http://www.mcafee.com/nl/resources/reports/rp-economic-impact-cybercrime.pdf

Uang Yang Terlibat Dalam Aktivitas Cyber Criminal

Putting Malicious Cyber Activity in Context			
CRIMINAL ACTION	ESTIMATED COST	PERCENT OF GDP	SOURCE
GLOBAL			
Piracy	$1 billion to $16 billion	0.008% to 0.02%	IMB
Drug Trafficking	$600 billion	5%	UNODC
Global cyber activity	$300 billion to $1 trillion	0.4% to 1.4%	Various
US ONLY			
Car Crashes	$99 billion to $168 billion	0.7% to 1.2%	CDC, AAA
Pilferage	$70 billion to $280 billion	0.5% to 2%	NRF
US- cyber activity	$24 billion to $120 billion	0.2% to 0.8%	Various

https://www.bbc.com/news/technology-59998925

REvil ransomware gang arrested in Russia

14 January

The FSB has released video footage of the arrests

Authorities in Russia say they have dismantled the ransomware crime group REvil and charged several of its members.

The United States had offered a reward of up to $10m (£7.3m) for information leading to the gang members, following ransomware attacks.

Russia's intelligence bureau FSB said the group had "ceased to exist".

However, it does not appear that any Russian members of the gang will be extradited to the United States.

The agency said it had acted after being provided with information about the REvil gang by the US.

According to the Russian state news service Tass, REvil "developed malicious software" and "organised the theft of money from the bank accounts of foreign citizens".

The FSB said it had seized more than 426 million rubles (£4m), including about £440,000 worth of crypto-currency.

https://www.reuters.com/technology/ukrainian-police-arrest-hacker-who-caused-150-million-damage-global-firms-2021-10-04/

October 4, 2021
9:37 PM GMT+7
Last Updated 4 months ago

Technology

Ukrainian police arrest hacker who caused $150 million damage to global firms

Reuters

https://www.thejakartapost.com/news/2021/04/16/indonesian-hackers-arrested-over-60-million-us-covid-19-scam-.html

INDONESIA BUSINESS WORLD OPINION CULTURE TRAVEL MULTIMEDIA SPORTS FRONT ROW TODAY'S PAPER MORE

Indonesian hackers arrested over $60 million US COVID-19 scam

This picture taken on April 15, 2021 shows police parading two hackers arrested over an international scam that saw the theft of about USD 60 million in Covid-19 aid intended for US citizens left jobless by the pandemic, at a press conference in Surabaya. (AFP /STR)

Share this article

Whatsapp

Facebook

News Desk (Agence France-Presse)

Surabaya • Fri, April 16, 2021

Two Indonesian hackers have been arrested over an international scam in which $60 million was stolen from a COVID-19 aid program helping Americans left jobless by the pandemic, authorities said.

Most Viewed

01 Yohana Yembise: Portrait of a true Papuan lady

02 Indonesia launches G20 forum on recovery, innovation

03 Indonesia imposes mandatory domestic sales on palm oil

04 COVID-19 third wave takes hold in Jakarta

05 Sealed off: Inside the 'closed loop'

Intro Data Breach / Data Leakage

- **Definisi Data Breach / Data Leakage :** Kebocoran data adalah aktivitas yang meng-ekspos confidential, sensitive, atau informasi yang terlindungi dari individu maupun organisasi. File, dokumen, informasi yang terlibat dalam data breach di lihat serta disebarluaskan tanpa izin dari pemiliknya.
- Siapa saja dapat menjadi korban dari risiko adanya data breach ini, baik individu, organisasi pemerintahan, high-level enterprise, dan banyak organisasi lainnya.
- In general, data breaches data breach ini terjadi karena terdapat kelemahan / kerentanan pada :
  - ❖Technology
  - ❖User Behaviour

Top 10 Biggest Breach Incident Reported

Company/Organization	Number of Records Stolen	Date of Breach
Yahoo	3 billion	August 2013
Equifax	145.5 million	July 2017
eBay	145 million	May 2014
Heartland Payment Systems	134 million	March 2008
Target	110 million	December 2013
TJX Companies	94 million	December 2006
JP Morgan & Chase	83 million (76 million households and 7 million small businesses)	July 2014
Uber	57 million	November 2017
U.S. Office of Personnel Management (OPM)	22 million	Between 2012 and 2014
Timehop	21 million	July 2018

https://www.trendmicro.com/vinfo/it/security/news/cyber-attacks/data-breach-101

Bagaimana Data Breach / Data Leakage Terjadi?

- **An Accidental Insider.** Sebagai contoh seorang staff yang menggunakan PC / Laptop milik temannya, dan tidak sengaja membaca / melihat informasiatau data pribadi milik rekannya tsb tanpa izin.
- **An Insider Threat / Disgruntle Employee.** Individu yang dengan sengaja mengakses dan/atau membagikan data milik organisasi dengan maksud untuk merugikan individu atau perusahaan. **Ancaman orang dalam** ini mungkin memiliki otorisasi yang sah untuk menggunakan data tersebut, tetapi tujuannya adalah untuk menggunakan informasi tersebut dengan cara yang tidak baik / mencuri data dan informasi tsb
- **Lost or Stolen Devices.** Laptop, Mobile Device, atau hard drive eksternal yang tidak terenkripsi atau tidak terkunci, dan di dalamnya terdapat data yang berisi informasi sensitive yang dicuri, atau hilang.
- **Malicious Outside Criminals.** Ini adalah merupakan hacker yang menggunakan berbagai vektor serangan untuk mengumpulkan informasi dari jaringan atau individu.

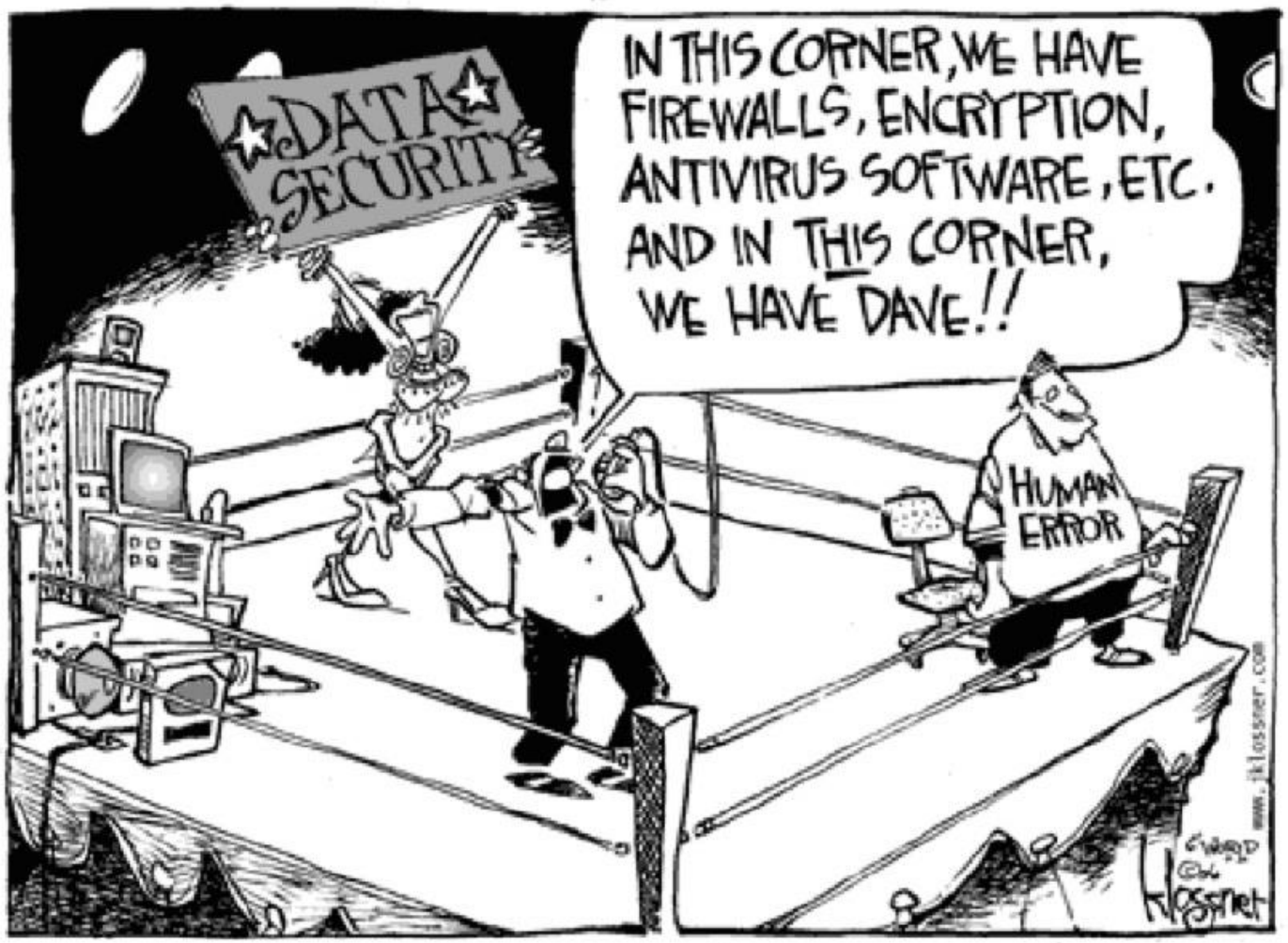
(Human = Social Beings) + Internet = Vulnerability

- Facebook
- Twitter
- Google+
- Linkedin
- Tumblr
- Filckr
- Blog
- Etc.

Information Leakage

The KEY to

Information Gathering !


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

Trend Cyber Criminal as A Service

Over the past few decades the digital underground has evolved and matured from a few small groups hacking and phreaking for fun and prestige, to a thriving criminal industry that costs global economies an estimated USD 300+ billion per year[1].

The most common 'positions' or specializations according to the FBI are:

1. **Programmers.** Who develop the exploits and malware used to commit cyber-crimes.
2. **Distributors.** Who trade and sell stolen data and act as vouchers for the goods provided by other specialists.
3. **Tech experts.** Who maintain the criminal enterprise's IT infrastructure, including servers, encryption technologies, databases, and the like.
4. **Hackers.** Who search for and exploit applications, systems and network vulnerabilities.
5. **Fraudsters.** Who create and deploy various social engineering schemes, such as phishing and spam.
6. **Hosted systems providers.** Who offer safe hosting of illicit content servers and sites.
7. **Cashiers.** Who control drop accounts and provide names and accounts to other criminals for a fee.
8. **Money mules.** Who complete wire transfers between bank accounts. The money mules may use student and work visas to travel to the U.S. to open bank accounts.
9. **Tellers.** Who are charged with transferring and laundering illicitly gained proceeds through digital currency services and different world currencies.
10. **Organization Leaders.** Often "people persons" without technical skills. The leaders assemble the team and choose the targets.

[1] **http://www.mcafee.com/nl/resources/reports/rp-economic-impact-cybercrime.pdf**

FBI: The 10 Criminal Cyber Crime Professions (knowbe4.com)

Cara Umum Kebocoran Data Terjadi

Berikut ini Cara / Vektor Umum Penyebab Kebocoran Data dapat terjadi :

- Phishing
- Malware
- Brute Force Attacks
- Exploit the Application or Infrastructure from Organization

Mengapa Ini Bisa Terjadi?

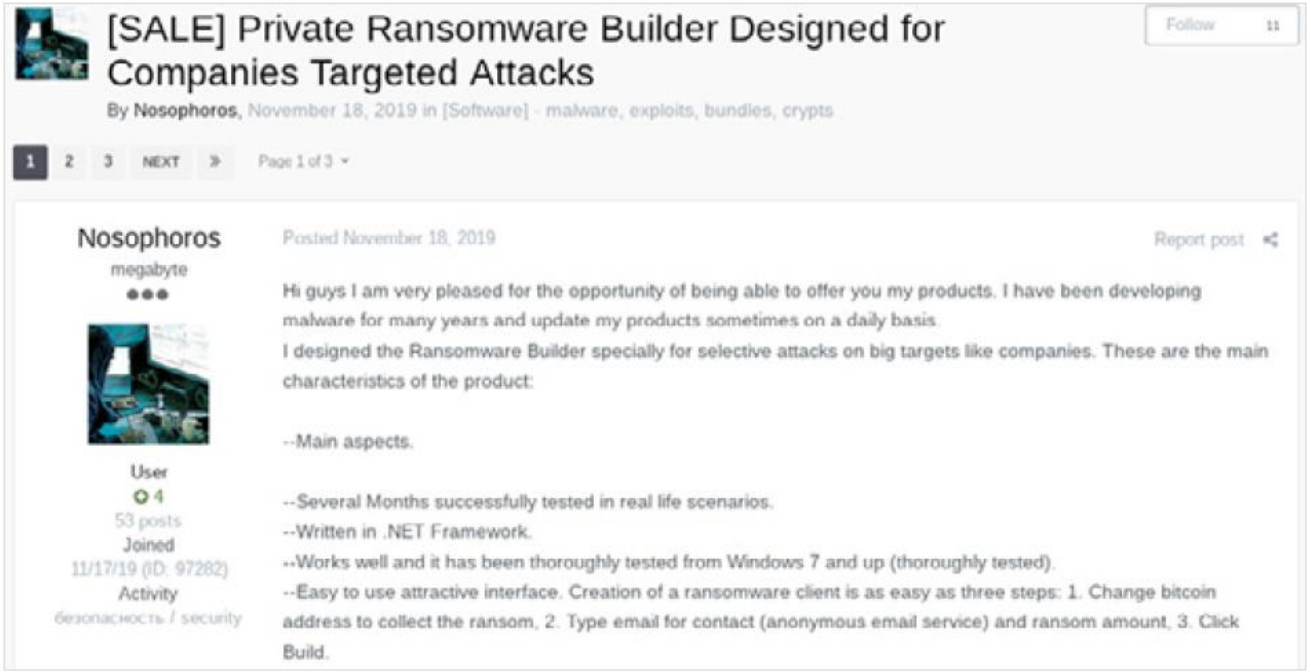
1. **Lack of** Security Awareness from Users
2. **Weak** or Stolen **Credentials**
3. **Unpatched** Security Vulnerabilities
4. **Holes** in Application
5. **Konfigurasi Sistem yang tidak proper** / tidak baik pada Application, Server, Infrastructure Network, database, dll
6. **Lack of** Security Monitoring and Detection from Organization

Cyber Security Prediction 2022

- Serangan Ransomware Akan terus meningkat. Peningkatan dari RaaS (Ransomware as a Service) dan ransomware yang dioperasikan manusia(Human Operated Ransomware).
- Serangan yang disasarkan ke institusi finansial termasuk ATM, ATM Switch, SWIFT Server, by some APT Group such as Lazarus
- Bisnis Email Compromise meningkat signifikan
- Supply Chain Attack : Studi kasus solar wind
- Kebocoran informasi PSE (Penyelenggara Sistem Elektronik)
- Serangan di prediksikan menyasar pekerja / end user yang bekerja secara remote

Ransomware as a Service

- Ransomware menjadi salah satu komoditas yang digunakan oleh pelaku ancaman di tahun 2020
- RaaS bermaksud untuk membuat ransomware Anda sendiri, kapabilitas, dan membuat pesan khas dan file ekstensi Anda sendiri
- Ransomware Builder dijual di pasar gelap dan mudah diperoleh



Serangan terarah pada lembaga keuangan

- Beberapa Bank di Indonesia menjadi incaran APT Group, terutama menyerang Server SWIFT
- ATM Switching Attack juga meningkat dalam 2 tahun terakhir.
- Serangan yang ditargetkan Mesin ATM. Banyak grup (Cobalt, MoneyTaker, Silence, Lazarus) memiliki ATM Trojans. Malware ATM digunakan dalam serangan yang ditargetkan ini untuk meminta aplikasi melakukan serangan ATM jackpotting

Business Email Compromise

- Business Email Compromise (BEC) adalah jenis perusahaan yang menargetkan penipuan yang melakukan transfer kawat dan memiliki pemasok di luar negeri. Akun email eksekutif perusahaan atau yang tersedia untuk umum atau karyawan tingkat tinggi yang terkait dengan keuangan atau terlibat dengan pembayaran transfer kawat baik palsu atau disusupi melalui keylogger atau serangan phishing untuk melakukan transfer curang.
- Beberapa contoh pesan email memiliki subjek yang berisi kata-kata seperti permintaan, pembayaran, transfer, dan mendesak, antara lain.
- Karena penipuan ini tidak memiliki tautan atau lampiran berbahaya, mereka dapat menghindari solusi tradisional. Pelatihan dan kesadaran karyawan dapat membantu perusahaan menemukan jenis penipuan ini.

Business Email Compromise (Lanjutan)

Berdasarkan FBI, terdapat 5 tipe dari BEC scams:

- **Skema Faktur / Invoice Palsu.** Perusahaan dengan pemasok asing sering menjadi sasaran taktik ini, di mana penyerang berpura-pura menjadi pemasok yang meminta transfer dana untuk pembayaran ke rekening milik penipu.
- **CEO Fraud.** Hacker berpura-pura / menyamar sebagai CEO perusahaan atau eksekutif mana pun dan mengirim email ke karyawan bagian keuangan, meminta mereka untuk mentransfer uang ke akun yang mereka kontrol.
- **Kompromi Akun-Akun email eksekutif atau karyawan** diretas dan digunakan untuk meminta pembayaran faktur ke vendor yang tercantum di kontak email mereka. Pembayaran kemudian dikirim ke rekening bank palsu.
- **Peniruan Lembaga Firma Hukum / Pengacara.** Penyerang berpura-pura menjadi pengacara atau seseorang dari firma hukum yang seharusnya bertanggung jawab atas masalah penting dan rahasia. Biasanya, permintaan palsu tersebut dilakukan melalui email atau telepon, dan selama akhir hari kerja.
- **Pencurian Data.** Karyawan di bawah HR dan pembukuan ditargetkan untuk mendapatkan informasi identitas pribadi (PII) atau laporan pajak karyawan dan eksekutif. Data tersebut dapat digunakan untuk serangan di masa mendatang.

Supply Chain Attack

- Serangan Supply chain melibatkan penargetan organisasi dengan mengeksploitasi tautan lemah di jaringan pasokan.
- Karena meningkatnya upaya dalam memperkuat postur keamanan siber organisasi, diyakini bahwa pelaku ancaman semakin sering melakukan serangan rantai pasokan karena semakin sulit untuk menyusup langsung ke organisasi.
- Serangan ini mungkin sulit dideteksi karena aktivitas ancaman terkait sering dilakukan di luar batas jaringan organisasi.
- Selain itu, sulit untuk mengamankan jaringan pasokan karena organisasi sering kali mengandalkan banyak pemasok untuk solusi dan layanan. Dengan kata lain, rantai pasokan pasti memperluas permukaan serangan organisasi.

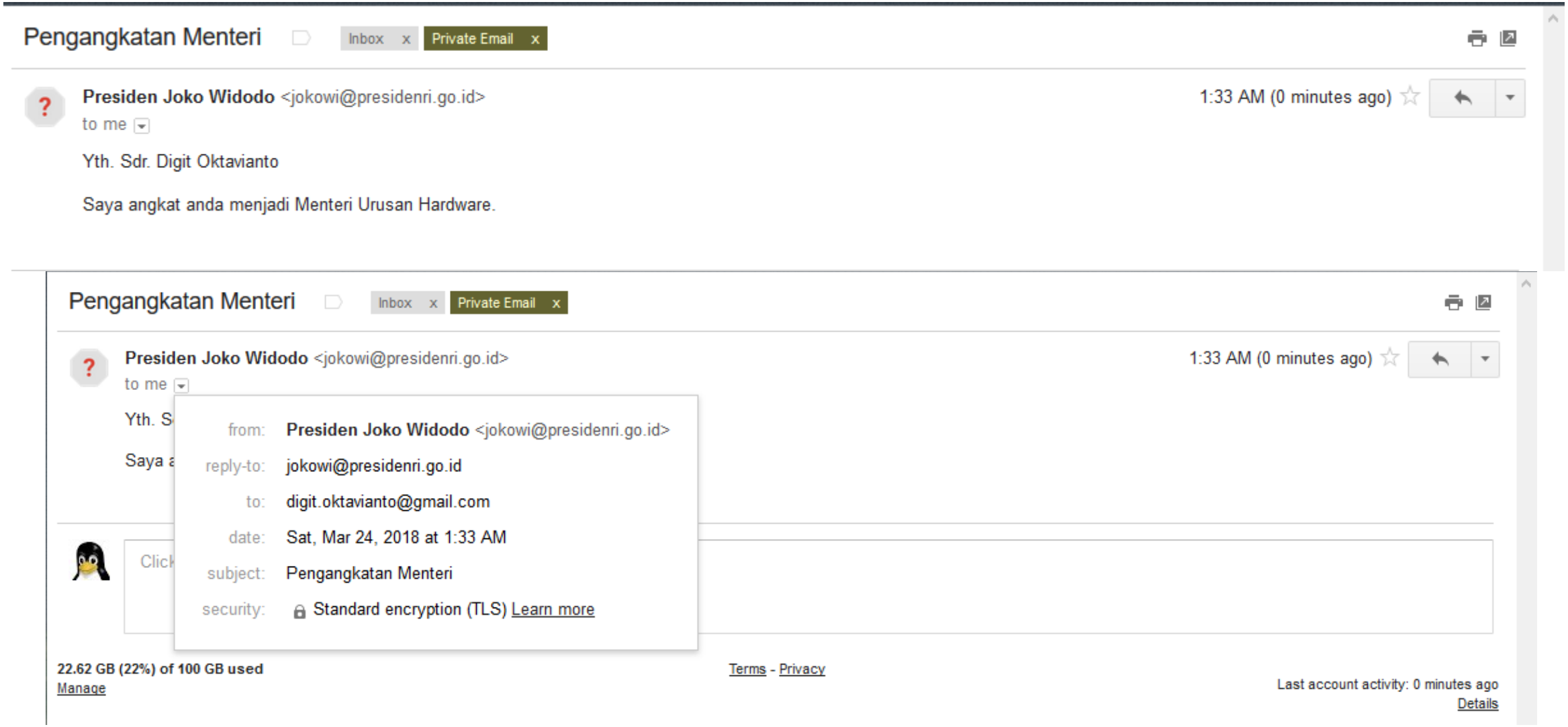

BUDGET BEFORE DATA BREACH
BUDGET AFTER DATA BREACH
imgflip.com

Jenis-Jenis Ancaman Umum yang Menjadi Penyebab Kebocoran Data Serta Bagaimana Menghindarinya

Phishing

- Deceptive emails / Email Tipuan yang membuat user untuk melakukan hal :
  - Memberikan sensitive information
  - Install Malicious Software
  - Download dan Open Malicious Documents
- Email yang sangat mirip dengan email yang legitimate :
  - Customer Service dari Bank
  - Email dari E-Commerce
  - Blast Email dari Perusahaan
- Variants
  - Vishing – Phishing media melalui Voice (Telepon)
    - Menjebak untuk memberikan informasi sensitive
    - Menakut-nakuti dengan tujuan mendapatkan keuntungan (Uang, dsb)
  - Text messages / Whatsapp / Instant Messnger

Demo - Email phishing



Demo - Email phishing

```
Delivered-To: digit.oktavianto@gmail.com
Received: by 2002:a9d:1445:0:0:0:0:0 with SMTP id h63-v6csp825627oth;
        Fri, 23 Mar 2018 11:33:44 -0700 (PDT)
X-Google-Smtp-Source: AG47ELsaqNQvaBhSeVaBsSFlvs9LTB84tJe9Hbk6fsHU42UWQR8JdZGucsGQv21XNgbTG20QkCpm
X-Received: by 10.223.165.3 with SMTP id i3mr26140091wrb.283.1521830024599;
        Fri, 23 Mar 2018 11:33:44 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1521830024; cv=none;
        d=google.com; s=arc-20160816;
        b=WVv47FH4vQ9RVnSZXLl+pOreAyCBySne912IW7oFJi2TU5tpvHKBZ/V0LtdpIfKI0E
         uJeYEFI2g+eP0LmIT0SzQXVgGscpof2F+fQIu4oZFyXCFSP/D/lWwXU7bdj1Smw6Gctm
         u17fQ8MDG0eR/V3+vBuvdKhTD0l+T+6ihQ/4cSJTLJR5ANQJec7jthkL/O9JzBWrb7tk
         18FmIajdvAKG0pbLAvLpb0bdMOysLaoZSiSkZlGacM0JDwZk20E/yPD/boI0pHtr49g5
         o3eL13uYCK2rFNkrAlh6aRykvgu6uFnYCmtOKMSoMo/xLQ8W33t6CV4BKbcDVNVveFKG
         fHfw==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=date:message-id:reply-to:errors-to:importance:from:subject:to
         :arc-authentication-results;
        bh=wfsCTb909L0nveDriGPIVi6ptCx8GYPkQgLD/7/rrSM=;
        b=heU97HIzRHjHLM1nwB2TTGRmdf+kWlSdM0y/AT3gBml8sVxQ9SEVpDAE5FV/cHRGHF
         vBw0+8NtqH31bBlcZluOdFcwNEXfEQ2csXsyfC2pbJq0/tXHamDF3yACm8xBwrFKfYm/
         oPppNY1ONEKlID6w2HJd8/Iexufz4/Ckhgo2gSSXSPopJSLVeY7JDr+u2p/upccXxMNe
         kpmf7D49QumMvEgS5RRV9Mn5u6k2UjXxkCNP73gT+TpUdpmUwzeF6mpeDMtTZJdYL4YV
         b7+2UxJHPkXiACiUC8hM+KrBmVNMc/fHDtKCJKO2EwQGM7i/hadOmWFfSleJ5OiEBeD4
         HHbA==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=neutral (google.com: 46.167.245.205 is neither permitted nor denied by best guess record for domain of
jokowi@presidenri.go.id) smtp.mailfrom=jokowi@presidenri.go.id
Return-Path: <jokowi@presidenri.go.id>
Received: from emkei.cz (emkei.cz. [46.167.245.205])
        by mx.google.com with ESMTPS id f1si5884497wre.74.2018.03.23.11.33.43
        for <digit.oktavianto@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Fri, 23 Mar 2018 11:33:43 -0700 (PDT)
Received-SPF: neutral (google.com: 46.167.245.205 is neither permitted nor denied by best guess record for domain of
jokowi@presidenri.go.id) client-ip=46.167.245.205;
Authentication-Results: mx.google.com;
```


I.T. CONGRATULATING ME FOR
NOT FALLING FOR THE PHISHING TEST
ME WHO
DOESN'T
READ EMAILS
imgflip.com

Passwords

- Authentication merupakan first line of defense terhadap bad guys
  - Logins user dan passwords memberikan anda authentikasi terhadap sistem yang anda ingin akses
- Jangan pernah memberikan password anda kepada orang lain
  - Jika seseorang melakukan sesuatu menggunakan akun ana, maka analah yang akan di minta pertanggungjawaban
- Gunakan password yang unik dan strong. Gunakan kombinasi dari beberapa frasa kata untuk mempermudah mengingat
- Strong passwords memiliki beberapa komponen :
  - Panjang karakter minimal 8 karakter
  - Termasuk angka, symbols, Huruf besar dan Huruf kecil
  - Tidak terdapat informasi pribadi anad seperti tanggal lahir, alamat, nama binatang peliharaan, nama anak, pasangan, alamat rumah, kota asal, dll

Auto ga liat pas diliat balik

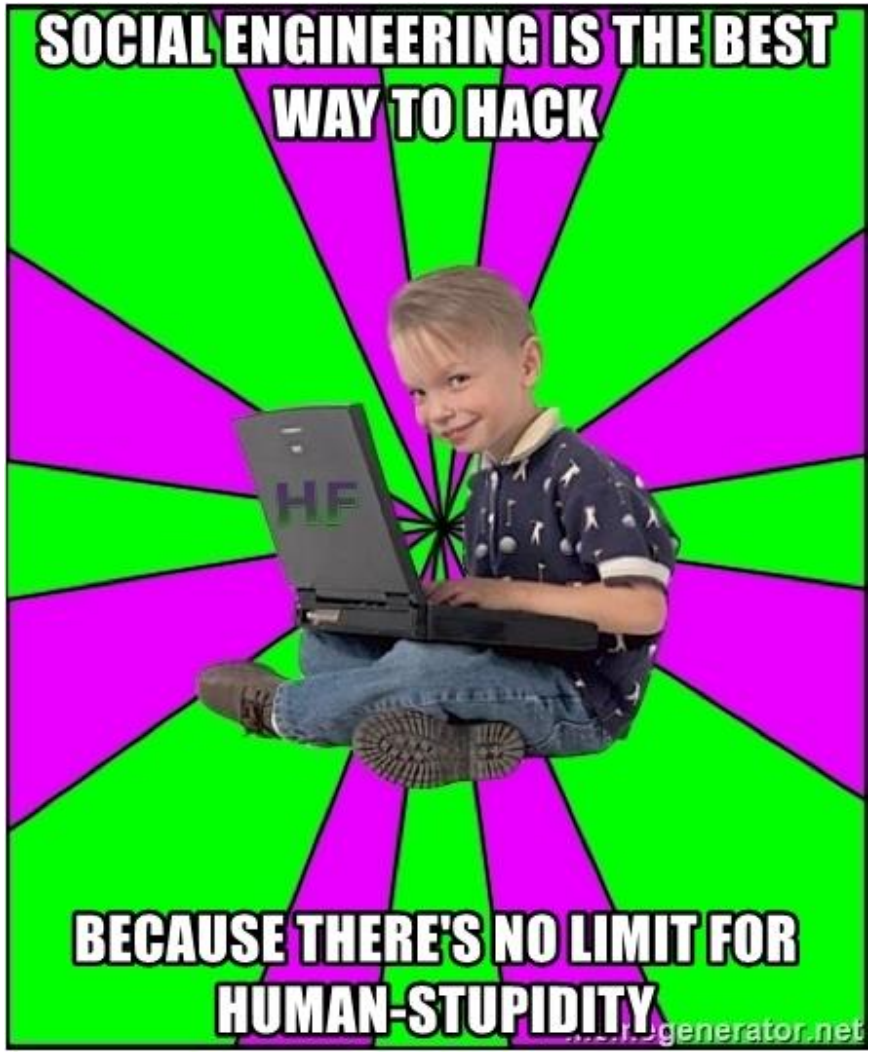
Social Engineering

- Manusia mrupakan rantai terlemah
  - **Segala sesuatu technical control yang sudah di implementasikan akan percuma jika tidak ada kesadaran dari masing-masing individu dalam organisasi**
- Percobaan target serangan social engineering
  - Confidential information atau credential
  - Akses terhadap sensitive area, atau dokumen
- Social Engineering dapat berbentuk banyak cara :
  - Human
  - Email
  - Phone
  - Text Message


SO, WHAT'S YOUR FAVORITE BOOK?
"CALL OF THE WILD" - IT REMINDS ME OF MY OLD DOG
AWW, WHAT'S YOUR DOG'S NAME?
"ROSIE" - ALL THE KIDS IN OUR NEIGHBORHOOD LOVED HER
SPEAKING OF - WHAT STREET DID YOU GROW UP ON?
MAPLE ROAD - WHY DO YOU ASK?
SECURITY QUESTIONS ANSWERED
WELCOME, AMANDA
DOGMO COMICS
@DOGMODOG

Face-to-Face Social Engineering

- Social engineering bisa juga berbentuk aktifitas yang complex
  - Custom costume, props, barang, logo, kendaraan,
  - Cerita yang di rekayasa
- Melibatkan rencana yang sudah matang
  - Informasi terhadap target, informasi terhadap prosedur yang berlaku
  - Informasi mengenai lokasi and jam operasional yang berlaku
- Melibatkan tools / device yang membantu supporting dalam aksinya
  - RFID Cloner
  - Lockpicking Tools


SOCIAL ENGINEERING IS THE BEST WAY TO HACK
BECAUSE THERE'S NO LIMIT FOR HUMAN-STUPIDITY

Social Engineering: Protect Yourself

- Verifikasi setiap kunjungan yang datang
  - Meyakinkan bahwa setiap kunjungan / tamu sudah membuat janji sebelumnya dan sudah diketahui oleh orang yang dituju
- Selalu tanyakan mengenai identitas diri dan asal
- Melakukan monitor terhadap vendor dan visitor yang berkunjung
  - Jangan pernah tinggalkan visitor berada sendiri di area yang sensitive
  - Visitor harus selalu ditemani setiap saat
- Never trust suspicious emails
  - Jangan pernah selalu percaya begitu saja terhadap setiap email yang masuk. Selalu lakukan pengecekan dan validasi

Wireless

- Attack yang banyak dilakukan
  - WEP/WPA/WPS Cracking
  - Sniffing
  - Fake Access Points
    - Beware of the WiFi Pineapple!

- Best Practices
  - WPA/WPA2
  - VPN

Fake USB Flash Drive

- Common Attacks
  - Bad USB (USB HID) -> USB Rubber Du
  - USB Killer (37 USD in Aliexpress)

- Best Practices
  - Always Lock Screen Your Laptop
  - Never Plug In Untrusted USB Devi
  - Disable Autorun USB Drive

Dumpster Diving

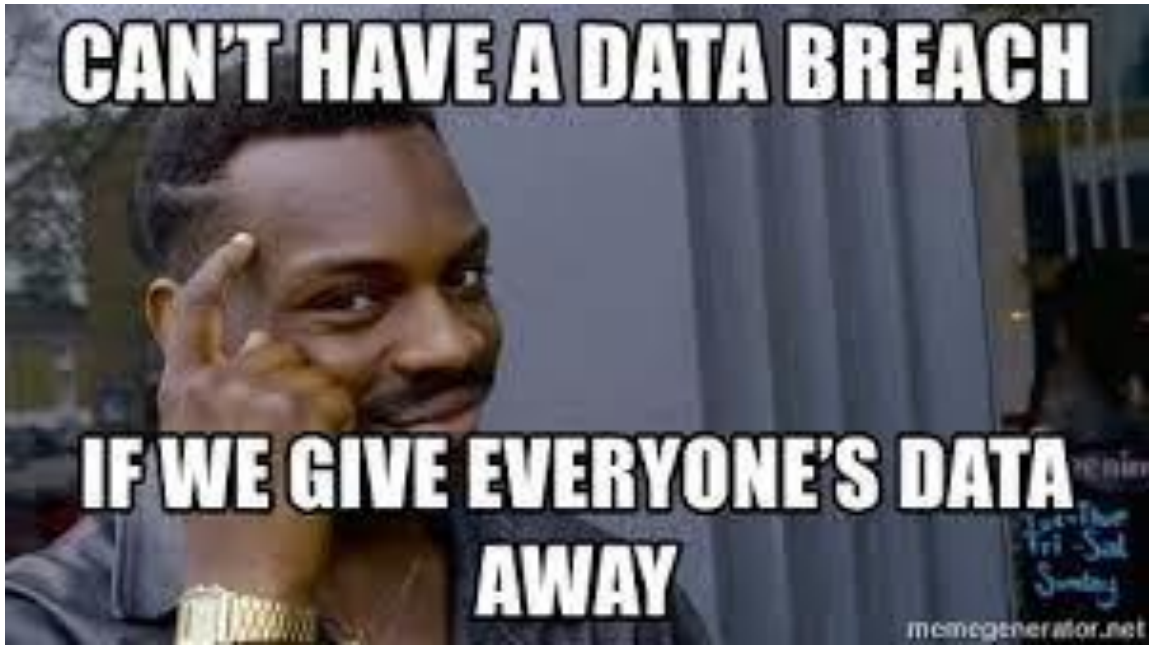
- **Dumpster diving** adalah salah satu aktivitas yang mengambil keuntungan dari sampah atau dokumen yang sudah di buang.
  - Customer information
  - Internal records
  - Applications
  - Informasi Medis
- Informasi yang kadang ditemukan :
  - Credit cards
  - Technical documentation
  - Backup tapes
  - Loan applications
  - Floor plans/schematics
  - Copies of identification

- Selalu gunakan Document Shredder sebelum membuang dokumen yang sensitive

Laptop / Workstation / Cubicle

- Bad Guys yang mempunyai akses terhadap laptop anda, workstation meja kerja / cubicle anda bisa mendapatkan informasi berikut ini :
  - Personal data
  - Email
  - Sensitive Document (Payslip, Transactioin Info)
- Lock Laptop / PC anda Ketika anda meninggalkan meja, bahkan jika hanya dalam waktu 1 menit.
  - Critical Data / Information bisa di ambil hanya dalam hitungan detik saja

  Windows Key + L untuk lock computer anda
- Jangan tinggalkan dokumen sensitive di meja kerja (bill, invoice belanja, sticky notes yang berisi informasi pribadi)


CAN'T HAVE A DATA BREACH
IF WE GIVE EVERYONE'S DATA AWAY
memegenerator.net


I NOTICED YOU LEAVE YOUR COMPUTER UNLOCKED WHILE YOU GET A COFFEE
I TOO LIKE TO LIVE DANGEROUSLY
quickmeme.com

Tips Bekerja Dengan Aman

Tips Bekerja Dengan Aman

- ✓**Berhati-hati saat bekerja dari jarak jauh, terutama Ketika anda sedang mengakses informasi milik organisasi / perusahaan yang sensitive.**
  - ✓Saat bekerja dari jarak jauh dari rumah atau saat dalam perjalanan, penting untuk mengambil tindakan pencegahan sebelum Anda mengakses data kepemilikan dan sensitif dari organisasi Anda. Koneksi internet Anda mungkin tidak seaman di kantor, sehingga memberikan peluang bagi peretas untuk mencuri data. Gunakan koneksi VPN yang aman atau ikuti petunjuk yang diberikan oleh organisasi Anda.
- ✓**Ketika menggunakan WI-Fi public, pastikan anda terkoneksi di Wi-Fi yang benar**
  - ✓Hati-hati saat menggunakan koneksi Wi-Fi milik public, pastikan Wi-Fi itu adalah Wi-Fi yang benar, karena bisa saja anda terkoneksi ke Fake Wi-Fi yang di buat oleh Hacker.

Tips Bekerja Dengan Aman

- ✓**Ketika menggunakan akses Wi-Fi milik public, tambahkan pengamanan pada koneksi anda**
  - ✓Pastikan Ketika anda mengakses layanan elektronik seperti bank, ecommerce, web transaksi lainnya, anda mengakses website yang benar. Tambahkan lapisan pengamanan seperti VPN Ketika anda sedang menggunakan Wi-Fi public.
- ✓**Jaga Mobile Device dan Laptop anda Ketika bekerja dari jarak jauh**
  - ✓Jangan tinggalkan laptop dan mobile device anda Ketika bekerja jarak jauh. Risiko akan pencurian data, hilangnya device anda, bisa terjadi pada anda Ketika anda lengah dari perhatian dan saat tidak dalam jangkauan laptop ataupun device lainnya

Tips Bekerja Dengan Aman

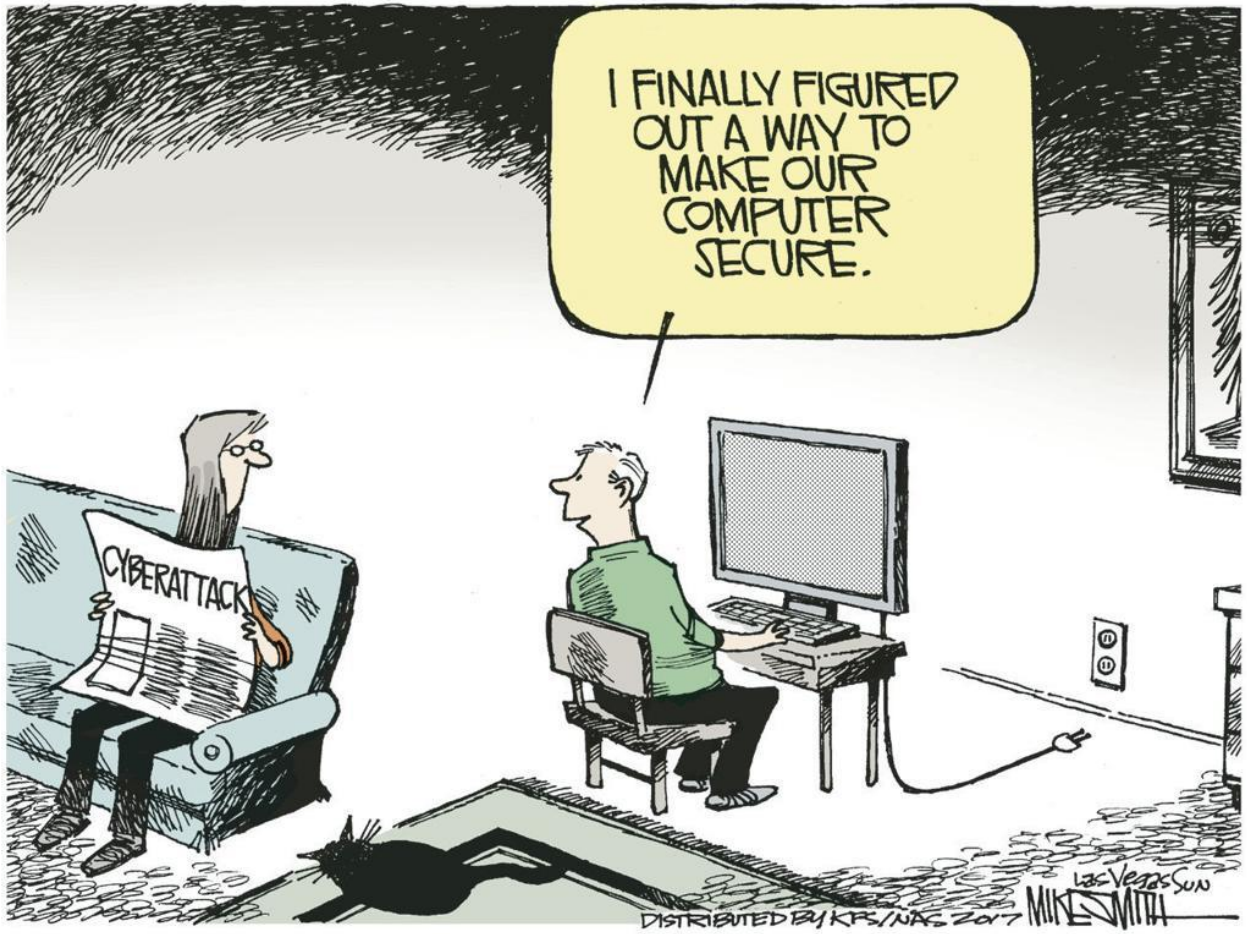
- ✓**Update Sistem Operasi dan Aplikasi Secara Berkala**
  - ✓Pastikan Sistem Operasi dan Aplikasi yang anda gunakan di update secara berkala. Hal ini untuk mengurangi risiko adanya kerentanana pada system operasi maupun aplikasi anda.
- ✓**Gunakan perlindungan pada device anda seperti Firewall dan Antivirus**
  - ✓Pastikan anda mengaktifkan Firewall, serta meng-install Anti Virus pada device anda. Pastikan juga Antivirus anda di update secara berkala.

Tips Bekerja Dengan Aman

- ✓**Backup Device Anda Secara Rutin**
  - ✓Akan selalu ada risiko akan kehilangan data anda, baik itu karena terjadi peretasan, malware, ataupun karena masalah pada perangkat anda. Selalu backup secara rutin data-data anda.
- ✓**Berhati-hati Ketika membuka Email**
  - ✓Selalu teliti dan waspada Ketika mendapatkan email, terutama sesuatu yang anda curigai ataupun ada file attachment, atau URL yang tidak anda kenal. Selalu ingat pepatah : “***If it is too good to be true then it is not true***”
- ✓**Gunakan Kombinasi Password Dengan Baik**
  - ✓Selalu menggunakan kombinasi password dengan baik. Tidak menggunakan Password yang sama di banyak aplikasi / system lainnya. Serta rutin mengganti Password dalam Periode waktu tertentu

Tips Bekerja Dengan Aman

- ✓**Tambahkan Pengamanan Multi Factor Authentication**
  - ✓Tambahkan MFA pada account-account penting anda, seperti email, social media, ecommerce, transaksi di perbankan, untuk mencegah terjadinya pencurian credential
- ✓**Ikuti Program Training dan Security Awareness yang di berikan oleh Organisasi Anda**
  - ✓Ikuti program training dan pembelajaran terkait cyber security awareness untuk mengetahui modus serangan dalam dunia cyber serta Langkah-Langkah pengamanannya.


I FINALLY FIGURED OUT A WAY TO MAKE OUR COMPUTER SECURE.
CYBERATTACK
DISTRIBUTED BY KFS/NAS 2017
LAS VEGAS SUN
MIKE SMITH

Summary and Key Takeaways

- In today's world, cyber security is a crucial part of any business.
- Cyber Crime and threat become more **Advanced, Sophisticated, and Targeted. Be careful, you may become the next target**
- **Technology** alone **can't solve all** your cyber security problem
- Data protection is not only about technology, but also in people and process
- Lack of security awareness is one of major problem from end user perspective from data breach case
- Prepare for the worst if data breach happen in your organization

Thank you. Q and A.

THANK YOU
Q & A