Pelatihan "Security Awareness"

Lembaga Amil Zakat, Infaq, dan Shadaqah Muhammadiyah (LAZSIMU) D.I Yogyakarta

Yogyakarta, 4 Januari 2020

Program Pemberdayaan Umat (PRODAMAT) MTI UAD

lazismu
Daerah Istimewa Yogyakarta

Outline sesi 1

- Pengertian ***Information Security***
- Isu **Keamanan** dan **Ancaman**
- Keamanan **Lingkungan Kerja**
- **Kebijakan** *Information Security*

Kesalahan Konsep Umum

Data saya
tidak penting

Kami tidak pernah
mengalami insiden

Kami sudah **aman**

Pengertian Information Security

Pengamanan pada Confidentiality (C) Kerahasiaan informasi, Integrity (I) data tidak berubah dari aslinya dan Availability (A) memastikan sumber daya yang ada siap diakses kapanpun oleh user, application, sistem yang membutuhkannya

Aset digital paling berharga adalah Data dan Informasi

Isu Keamanan

1. **Berbagi** penulisan password
2. **Password** mudah ditebak
3. **Password** dikirim dalam bentuk plaintext
4. Tidak kejalasan **policy dan prosedur**

Ancaman yang akan terjadi

- Menggunakan dan menyalahgunakan resource
- Denial of Service (DOS)
- Penghapusan Data
- Penyebarluasan Data
- Pengrusakan Data
- Kegagalan Komponen

Proteksi informasi menggunakan laptop

1. Jaga agar notebook berada dalam pengawasan kita.
2. Jika berpergian usahakan tidak diletakkan di bagasi.
3. Gunakan security lock.
4. Backup data secara periodik.

Bagaimana dengan keamanan lingkungan kerja?

Berikut beberapa hal yang perlu dilakukan dalam lingkungan kerja

Keamanan di Lingkungan Kerja

1. Hindari penyebaran informasi penting/sensitif
2. Jangan meninggalkan dokumen sembarangan di meja kerja
3. Gunakan metoda pemusnahan dokumen yang benar.
4. Jangan biarkan dokumen tertinggal di mesin fotocopy atau fax

MTI-UAD

Keamanan di Lingkungan Kerja

5. Kunci layar komputer dengan menggunakan password.
6. Jangan menyimpan informasi penting di dalam USB.
7. Jangan meminjamkan USB flash disk sembarangan.
8. Jaga agar pintu masuk kantor senantiasa tertutup.

MTI-UAD

Keamanan di Lingkungan Kerja

Jangan biasakan meminjamkan ID Card

Kebijakan Information Security

Information Security Policy

Bank Mega Information Security, Policy Third party access policy, Security Training and Awareness Policy, Desktop Management, Policy Password Policy.

Information Security Procedure

information Classification & Handling Procedure, User Account Management Procedure, End User Computing Procedure, Information Security Incident Response Procedure, Router hardening Procedure

Outline sesi 2

- Pengamanan **Password**
- Pengamanan **Social Engineering**
- Pengamanan **Virus dan Spyware**
- Pengamanan **Mobile**
- Pengamanan **Penggunaan Email**

Pengamanan Password

Password seperti kunci untuk membuka pintu rumah

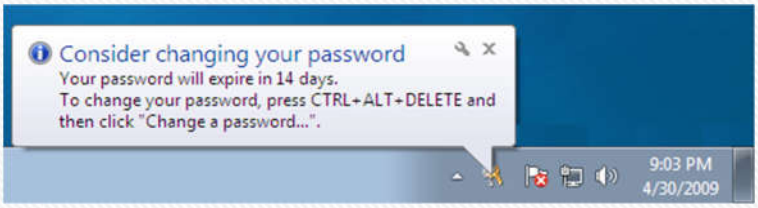
Easy to remember but hard to guess

Hindari dalam pembuatan password

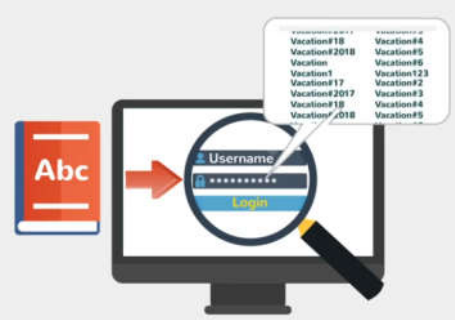
1. **Nama** : nama pribadi, anak, keluarga, lembaga, daerah, hobi, komunitas
2. Kata-kata yang terdapat dalam **kamus**
3. **Tanggal dan tahun :** kelahiran, berdirinya perusahaan

Tips Pengamanan Password

- Jangan menepel user dan password di area publik
- 8 karakter atau lebih
- Kombinasi angka, huruf besar, huruf kecil, karakter
- Klasifikasi penggunaan password (Bedakan password lembaga dengan password pribadi)
- Ubahlah password setiap 6 bulan (1 tahun 2x)



Strong Password



Buatlah strong password dengan kombinasi huruf kecil, besar, angka dan karakter minimal 8 karakter

Buatlah hint password tersebut

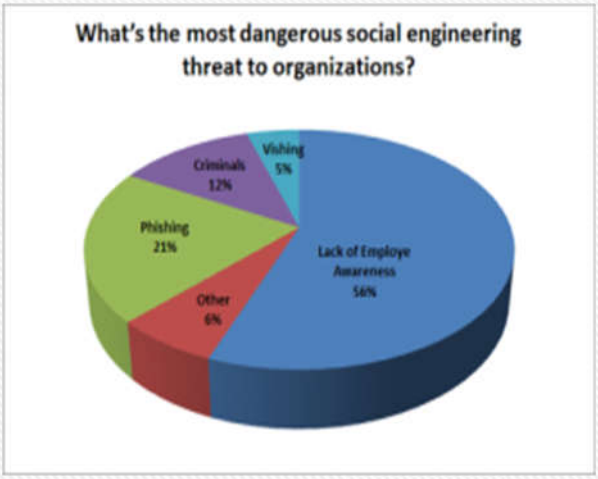
Membuat Password

Contoh :
b15m1ll4h@ll@hu@kb@r99

hint : mulai membaca takbir dan asmaul husna

Pengertian Social Engineering

Social engineering adalah kegiatan untuk mendapatkan informasi rahasia/penting dengan cara menipu pemilik informasi tersebut (targeted) umumnya dilakukan melalui telepon dan Internet dengan pendekatan yang manusiawi melalui mekanisme interaksi sosial.



Tips menghindar ancaman social engineering

1. Tanyakan **nama dan identitas** (verifikasi)
2. Tanyakan mengapa memerlukan **informasi**
3. Tanyakan siapa yang **mengautorisasi** permintaan informasi

Sifat dasar manusia dalam social engineering

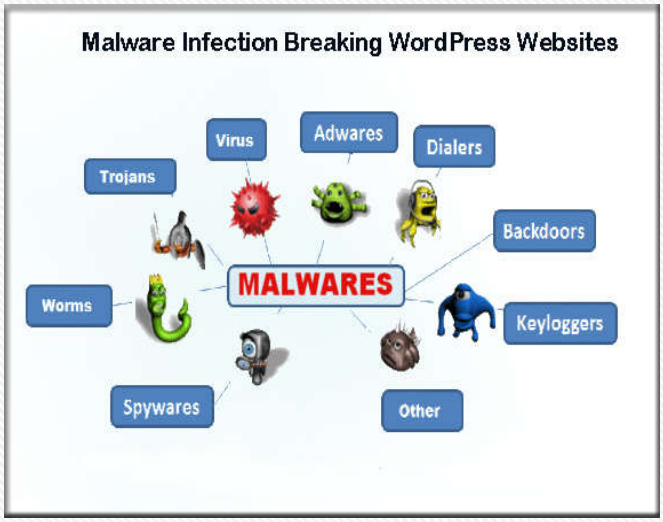
1. Keinginan untuk **menolong** orang lain
2. Kecenderungan untuk **mempercayai** orang lain
3. Rasa **takut dan khawatir** akan memperoleh kesulitan/masalah

Target social engineering

Serangan Social Engineering

Pengertian Virus & Spyware

- Virus dan spyware adalah salah satu dari Malware (Malicious software) Sesuai Namanya yang berarti **software jahat**/ kode jahat, program ini merupakan software yang diciptakan oleh seseorang dengan tujuan untuk merugikan orang lain

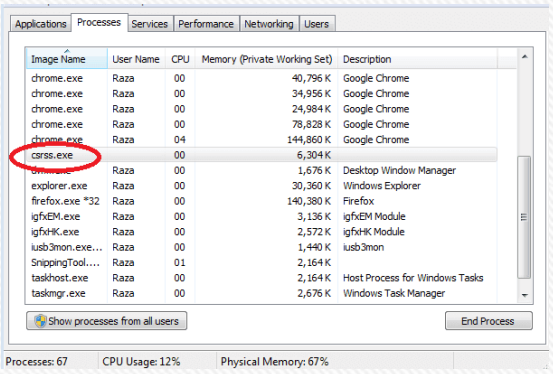


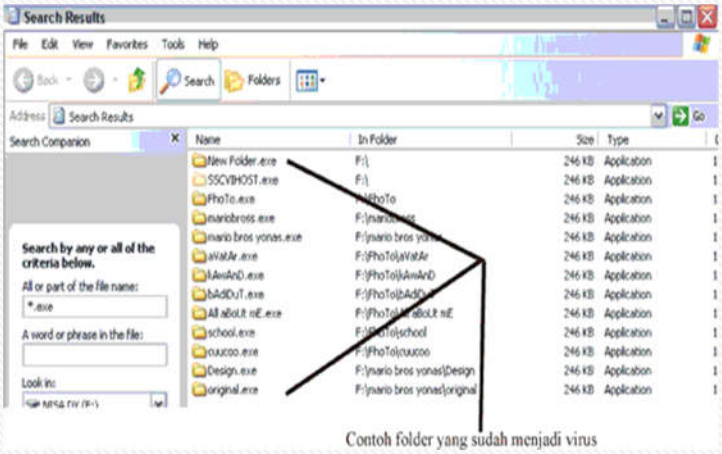
Virus Vs Spyware

1. Virus adalah Malware yang menginfeksi sebuah komputer dengan **bantuan pihak ketiga** untuk mengaktifkan/ menjalankan dirinya – biasanya pemilik komputer itu sendiri.

2. Spyware adalah malware memang diciptakan untuk memata-matai (spy) profil pribadi pemilik komputer. Kegiatan ini dilakukan dengan **menampilkan iklan-iklan** yang sekiranya diminati oleh pengguna komputer

Serangan Virus dan Spyware





Contoh folder yang sudah menjadi virus

Ancaman yang akan terjadi

- Komputer terasa lemot, bahkan saat tidak menjalankan aplikasi apapun.
- Selalu muncul iklan pop-up ketika terkoneksi ke internet.
- Settingan berubah pada browser padahal user tidak merasa mengubah settingan.
- Ada aplikasi yang terinstall sendiri tanpa diketahui.
- Spyware bisa mengirimkan data kepada pengguna computer lain ketika computer target terhubung keinternet.

Tips Pencegahan

- Waspada terhadap proses sistem operasi diluar normal Selalu muncul iklan pop-up ketika terkoneksi ke internet.
- Jika terinfeksi virus, hentikan pekerjaan cari bantuan IT Admin
- Pastikan antivirus terupdate dengan baik
- Jangan klik iklan di internet yang tidak jelas
- Hindari instal aplikasi freeware (crack dll)
- Klik next dan next ketika install tanpa cek agreement

Keamanan Penggunaan internet-browsing

Phising adalah jenis serangan yang biasanya menggunakan e-mail dan website palsu yang didesain persis untuk mengelabui orang lain.

Tujuan phising : mengambil data penting (kartu kredit, username dan password) dengan cara illegal

Bank Niaga and Bank Bukopin Phishing Update 2008

Fraud Phishing Security

Recently one of the biggest private bank in Indonesia, Bank Niaga -part of CIMB Group, and one of biggest state bank in Indonesia, Bank Bukopin, attacked by phishing for their internet banking service. Here is the detail of what happened:

1. Bank Niaga and Bank Bukopin cooperate with bank2home (pacomnet) to outsource its internet banking services.
2. There are some hacker who perform a social engineering process by redirecting the link using fake link as below:

http://secure.bank2home.com.cn/ib-niaga/Login.html
http://secure.bank2home.com.cn/appbukopin/

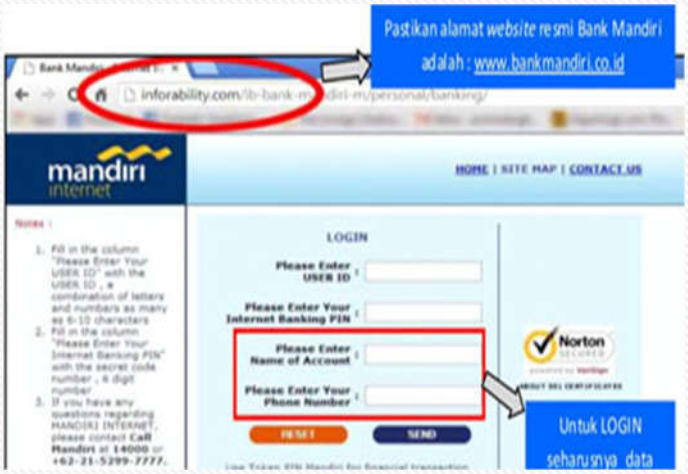
Compare to the original link that using https and no addition for .cn domain.
https://secure.bank2home.com/ib-niaga/Login.html
https://secure.bank2home.com/appbukopin/login.jsp

Do you have any opinion? about security in online banking?

Serangan phising

Tips Pencegahan Phising

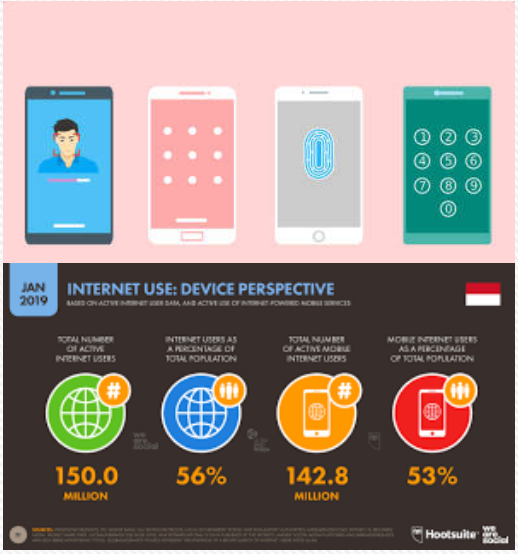
- Waspada terhadap link internet yang menggiurkan
- Cek alamat situs sebelum input password
- Pastikan alamat situs HTPPS
- Jangan memasukkan data penting dan no kartu kredit



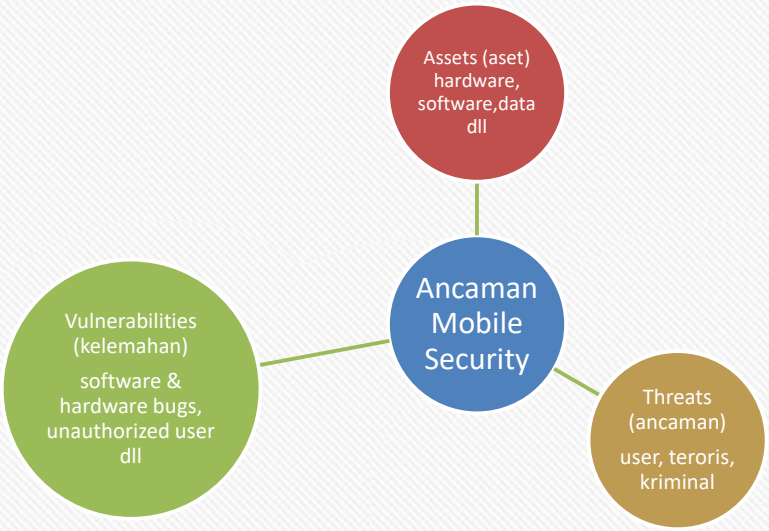
Keamanan Mobile

Keamanan Mobile adalah sebuah sistem yang di gunakan untuk mengamankan sebuah smartphone atau mobilephone dari segala gangguan dan ancaman yang tidak di inginkan (keamanan data, informasi dan hardware)

Saat ini Smartphone terintegrasi akun **email** (ANDROID > GMAIL) untuk kebutuhan aplikasi informasi dan transaksi

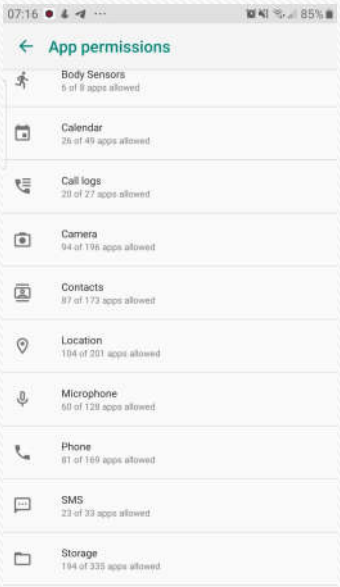


Ancaman Mobile



Tips Keamanan Mobile

- Gunakan aplikasi yang resmi dari playstore
- Hati-hati dengan wifi public
- Hindari penggunaan VPN unsecure (gratisan)
- Selalu backup data
- Saat install jangan next dan next perhatikan permission yang diminta
- Aktifkan password (pattern, pin, password, fingerprint)
- Aktifkan find my device
- Aktifkan remote wipe

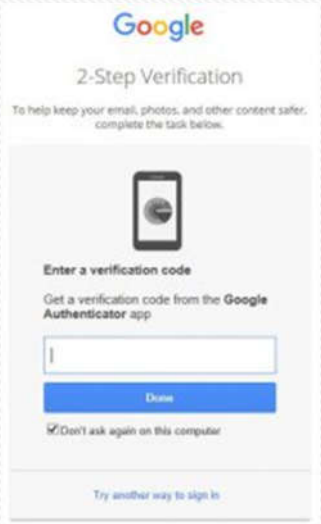


Keamanan Email

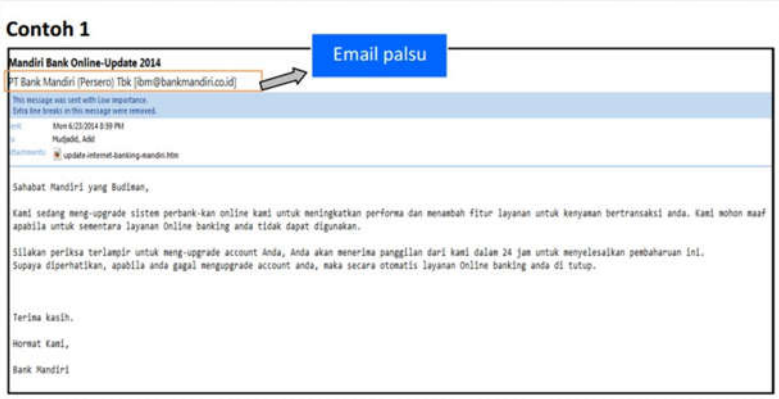
Email atau surat elektronik sangat memudahkan kita untuk mengirimkan pesan. Saat ini banyak layanan email gratis seperti gmail, yahoo, microsoft)

Tips pengamanan email

- Aktifkan verifikasi 2 langkah
- Update browser dengan versi terbaru
- Gunakan password yang bervariasi dan sering menggantinya
- Tidak mengklik link yang diberikan sebelum dicek kebenaran link-nya
- Tidak mengisi form pribadi pada link email yang tidak diminta
- Cek alamat pengirim (nama & domain)
- Tidak melakukan download terhadap file attachment



Serangan email



Alamat Email Tidak Resmi – Email dikirimkan dari email yang menyerupai email resmi untuk menipu. Pada contoh Bank Mandiri di atas, email dikirimkan melalui ibm@mandiri.co.id sedangkan email asli Bank Mandiri adalah mandiricare@bankmandiri.co.id.


Safety start with awareness,
Awareness start with YOU
Terimakasih ☺