twenty-four CONSULTING

KEMENTERIAN SUMBER ASLI DAN KELESTARIAN ALAM

Keselamatan Siber, Tiada Jurang, Tiada Ancaman

Program Hari Digital, Kementerian Sumber Asli dan Kelestarian Alam (NRES)

Ali Reza Azmi
Trainer

Hello! I'm Ali Reza

Ali Reza has honed his mastery of technology over two decades. A sought-after Microsoft Certified Trainer, Google Cloud Authorized Trainer, and holder of numerous certifications, he's skillfully guided thousands of Malaysian professionals toward digital fluency. Ali understands that true power lies in sharing knowledge and empowering others to unlock their potential.

20+
Years of experience.

5000+
Participants trained.

2001
Certified since then.

10+
Certified Credentials.

Company Overview

Mengenai Twenty-Four Consulting PLT

Ditubuhkan pada Februari 2024, Twenty-Four Consulting PLT ialah sebuah syarikat latihan dan perundingan yang membantu organisasi dan pasukan berkembang dalam era digital yang pesat berubah.

Dengan lebih 20 tahun pengalaman dalam industri teknologi, kami mereka bentuk program latihan bersifat praktikal dan diperibadikan serta perkhidmatan perundingan yang disesuaikan mengikut keperluan dan matlamat unik setiap organisasi.

Sebagai penyedia latihan yang berdaftar di bawah HRD Corp dan rakan rasmi Canva, kami telah bekerjasama secara meluas dengan pelbagai kementerian, jabatan kerajaan, dan agensi sektor awam dalam membina kemahiran digital dan memperkasa kecekapan kerja.

Kami percaya bahawa latihan perlu bersifat praktikal, disesuaikan dengan keperluan peserta, dan relevan dengan tugasan harian. Komitmen kami adalah untuk memastikan pelaburan latihan memberikan pulangan maksimum kepada organisasi.

Agenda

Slides

01.
Pengenalan

Berapa banyak aplikasi yang anda telah gunakan sejak bangun pagi ini — dan data apa yang telah anda kongsikan tanpa disedari?

Apa itu Data?

- Maklumat tentang anda atau aktiviti anda
- Boleh bersifat peribadi (nama, nombor IC) atau tingkah laku (sejarah pelayaran, lokasi)
- Dicipta dan dikongsi setiap kali kita menggunakan teknologi

Apa itu Privacy?

Definisi: Kawalan terhadap maklumat anda

- Hak anda untuk mengawal maklumat peribadi anda
- Menentukan apa, bila, dan dengan siapa maklumat dikongsi
- Melindungi maklumat anda daripada disalah guna atau didedahkan tanpa izin




What Your Apps Know About You

Type of Data	What They Collect
👤 **Personal Info**	Name, IC number, phone number, email, profile photo
🌍 **Location**	GPS coordinates, travel history, nearest cell towers, IP-based location
📱 **Device Details**	Model, OS version, battery level, carrier, IMEI number
🧠 **Usage Behavior**	Screen taps, scrolls, time spent, most-used features, in-app search
👥 **Contacts & Calendars**	Access to phonebook, calendar events, birthdays *(with permission)*
🖼️ **Media & Files**	Photos, camera access, microphone, storage files *(if allowed)*
💬 **Messages**	SMS for OTP, push notifications, message metadata *(e.g. WhatsApp time stamps)*
💳 **Payment Info**	Credit cards, e-wallets, purchase history, billing addresses
🧬 **Biometric/Health**	Step count, heart rate, sleep data, face/fingerprint (used for authentication)
📊 **Advertising IDs**	Unique ad ID, browsing patterns, third-party cookies and trackers

Mengapa Perlindungan Data Lebih Penting Berbanding Sebelumnya

- Kehidupan harian kita bergantung kepada data digital
- Setiap transaksi, komunikasi dan rekod menghasilkan data
- Kebocoran data bukan lagi perkara luar biasa — ia berlaku setiap hari
- Akibatnya memberi kesan kepada individu dan organisasi
- Perlindungan data bermula dengan kesedaran dan tindakan kecil oleh individu

02.

Ancaman dan Risiko

Ancaman Apa Yang Kita Hadapi?

- Ancaman siber adalah nyata, semakin berkembang dan sentiasa berubah
- Penyerang menyasarkan sistem dan manusia
- Kesilapan manusia yang mudah sering menyebabkan kebocoran data yang besar

Social Engineering: Manipulasi Psikologi

Bagaimana penggodam mengeksploitasi sifat manusia:

- Penyerang memanipulasi emosi untuk memperdaya mangsa
- Taktik biasa: *fear*, *urgency*, *greed*, *trust*
- Mereka sering menyamar sebagai individu yang anda kenali atau percayai

Common Tactics Hackers Use

- Urgency: "Act now or lose access!"
- Fear: "Your account will be suspended!"
- Greed: "You have won RM10,000!"
- Curiosity: "See who viewed your profile!"
- Authority Pressure: "Message from your boss or IT department."

Phishing: Penipuan Digital

Bagaimana serangan phishing berlaku:

- E-mel palsu yang menyamar sebagai sumber yang dipercayai
- Menipu anda supaya klik pautan berbahaya atau memberikan maklumat
- Satu klik yang silap boleh menjejaskan keselamatan organisasi anda

Contoh Serangan Phishing

E-mel Palsu Bank

- "PENTING: Akaun anda telah dikunci!" — E-mel palsu kononnya dari bank meminta anda klik dan sahkan maklumat.

Penipuan Penghantaran Bungkusan

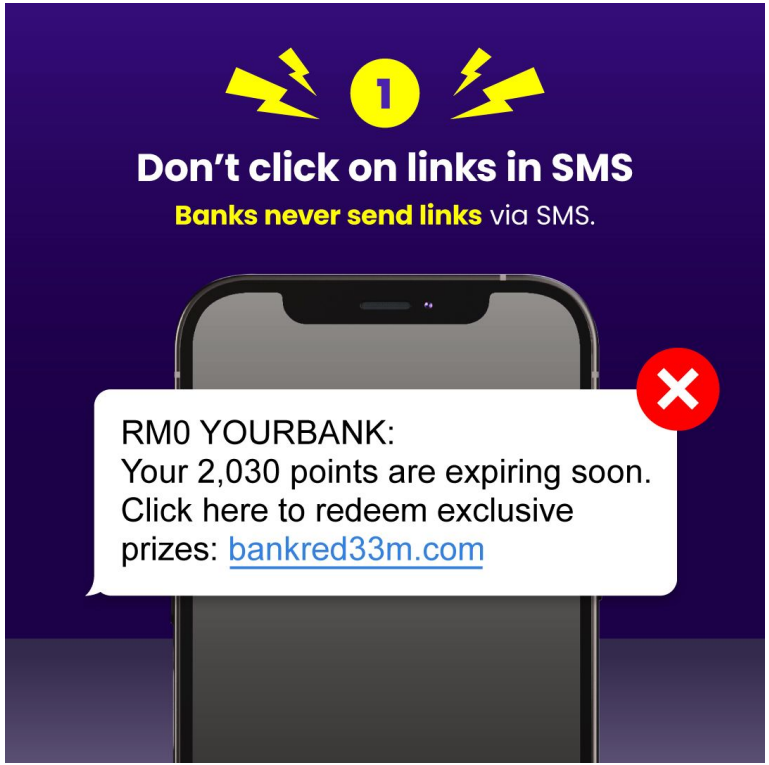
- "Bungkusan anda ditahan — bayar RM2.50 untuk pelepasan." — Notis palsu daripada PosLaju atau DHL.

Penipuan Pulangan Cukai Kerajaan

- "Anda layak menerima pulangan cukai." — E-mel atau SMS palsu yang menyamar sebagai LHDN.

Penipuan WhatsApp Tawaran Kerja

- "Kerja dari rumah, RM500 sehari!" — Tawaran kerja palsu untuk mencuri maklumat peribadi.



Malware: Ancaman Tersembunyi

- Malware = perisian berniat jahat yang boleh merosakkan atau mencuri daripada anda
- Boleh masuk melalui e-mel, muat turun, atau aplikasi palsu
- Penyerang senyap — mencuri data, mengintip aktiviti, atau mengunci sistem

Tips to Prevent a Malware Attack

1. Jangan muat turun perisian daripada sumber yang tidak diketahui
2. Jangan klik pada pop-up
3. Amalkan penggunaan kata laluan yang kukuh seperti menukar kata laluan lalai dan menggunakan pelbagai jenis aksara
4. Laksanakan kawalan identiti dan akses seperti multi-factor authentication (MFA)
5. Jangan meminjamkan peranti anda kepada orang lain, walaupun kepada seseorang yang anda kenali
6. Jangan buka e-mel atau lampiran daripada penghantar yang tidak dikenali
7. Jangan klik pada pautan yang tidak diketahui di media sosial, e-mel, mesej teks, atau mana-mana peranti lain
8. Berhati-hati dengan aplikasi yang dimuat turun. Semak ulasan di app store untuk memastikan tiada pihak berniat jahat terlibat
9. Jangan jail-break telefon anda
10. Pastikan sistem operasi dan plugins sentiasa dikemas kini dan hanya muat turun kemas kini rasmi

Ransomware: Menawan Data Sebagai Tebusan

- Mengunci fail atau sistem anda dan menuntut wang tebusan
- Pembayaran biasanya diminta dalam bentuk mata wang kripto
- Tiada jaminan anda akan mendapat semula data anda walaupun telah membayar

03.

Di Mana Data Anda Disimpan?

Di manakah data anda
berada sekarang?

Dalam telefon anda?
Dalam laptop anda?
Di Malaysia?

Di Mana Data Anda Disimpan?

- Data disimpan merentasi peranti, aplikasi dan pelayan awan
- Sebahagian besar daripadanya disimpan di luar negara — sering kali tanpa pengetahuan anda
- Lokasi data menentukan siapa yang boleh mengakses dan mengawal maklumat tersebut

Challenge: Tahukah Anda?

Adakah anda sedar di mana data peribadi dan data kerja anda disimpan?

- Peranti tempatan?
- Di awan?
- Di negara mana?

Jika anda tidak tahu, privasi dan keselamatan anda sudah pun terancam

Contoh TikTok: Lokasi Data

- Syarikat induk TikTok, ByteDance, berpusat di China
- Data pengguna mungkin disimpan di AS, Singapura, atau China
- Undang-undang negara asing, bukan undang-undang Malaysia, menentukan bagaimana data anda diakses

Data Sovereignty Risks

Implikasi penyimpanan data di luar negara

- Data yang disimpan di luar negara tertakluk kepada undang-undang asing
- Malaysia mempunyai kuasa yang terhad untuk melindungi data tersebut
- Risiko data diakses, dipantau, atau disalah guna oleh pihak luar

Siapa Yang Boleh Mengaksesnya?

Risiko akses oleh pihak berkuasa asing:

- Kerajaan asing boleh mengakses data melalui undang-undang mereka
- Kakitangan syarikat hos mungkin boleh mengakses atau salah urus data
- Penggodam boleh mengeksploit kelemahan piawaian keselamatan antarabangsa
- Anda kehilangan kawalan sepenuhnya apabila data disimpan di luar negara

Renungan

Adakah anda selesa dengan perkara ini?

- Data anda mungkin disimpan di luar Malaysia
- Anda mungkin tidak tahu siapa yang boleh mengakses data tersebut
- Adakah anda benar-benar selesa kehilangan kawalan terhadap maklumat anda?

04.

Mitos vs Realiti - Storan Awan

Keselamatan Awan: Mitos vs Realiti

❌ Mitos	✅ Realiti
Awan tidak selamat — data mudah digodam	Penyedia cloud terkemuka melabur berjuta ringgit dalam keselamatan setiap tahun
Saya tidak tahu di mana data saya — lebih baik simpan secara tempatan	Cloud menyediakan **ketelusan**, **kawalan lokasi**, dan ***redundancy***
Jika data di awan, sesiapa pun boleh akses	Terdapat **pengurusan akses**, ***encryption***, dan **log audit** yang ketat
Storan tempatan lebih selamat kerana saya boleh lihat perantinya	Peranti tempatan mudah hilang, dicuri, diserang malware atau tiada salinan sandaran
Kalau cloud terhenti, semua data saya akan hilang	Sistem cloud ada **sandaran automatik**, **pemulihan bencana**, dan **pemindahan lokasi automatik**

Amalan Terbaik untuk Storan Awan

Tabiat baik semasa menggunakan storan awan:

✅ Gunakan kata laluan yang kuat dan unik

✅ Aktifkan Pengesahan Dua Faktor (2FA)

✅ Semak kebenaran perkongsian secara berkala

✅ Elakkan menyimpan data sensitif yang tidak perlu

✅ Simpan salinan sandaran (backup) tempatan bagi fail kritikal

05.

Perlindungan Data Sensitif Organisasi

Data Leaks vs Data Breaches

Data Breach

- Disebabkan oleh akses tanpa kebenaran (biasanya oleh penggodam)
- Tujuannya untuk mencuri, menjual, atau menahan data sebagai tebusan
- Sering menyasarkan rekod kewangan, maklumat peribadi (PII), atau rahsia perdagangan
- Memerlukan langkah keselamatan yang kukuh untuk mengelakkan eksploitasi

Data Leak

- Disebabkan oleh pendedahan secara tidak sengaja (contoh: kecuaian atau salah konfigurasi)
- Tiada penglibatan penggodam — data hanya dibiarkan tanpa perlindungan
- Boleh berlaku ketika data disimpan (at rest) atau semasa penghantaran (in transit) antara sistem
- Sukar dikesan dan sama berbahaya seperti breaches

Jangan Simpan Apa yang Anda Tidak Perlukan

✅ Setiap data yang disimpan menambah risiko keselamatan

✅ Hanya kumpul dan simpan maklumat yang diperlukan sahaja

✅ Lakukan audit dan padam data lama secara berkala

✅ Kurang data disimpan = impak lebih kecil jika berlaku kebocoran

06.

Tanggungjawab Peribadi & Amalan Baik

5 Golden Rules

1. Gunakan Kata Laluan & Frasa Laluan Kukuh
    a. Sekurang-kurangnya 12–16 character, gabungkan huruf, nombor & simbol
2. Aktifkan Pengesahan Dua Faktor (2FA)
    a. Lapisan keselamatan tambahan untuk e-mel, bank & akaun awan
3. Semak Kebenaran Aplikasi & Pautan
    a. Benarkan akses minimum sahaja
4. Elakkan Perkongsian Maklumat Sensitif Secara Terbuka
    a. Fikir sebelum kongsi di media sosial atau mesej
5. Gunakan Rangkaian Selamat & Sandaran Data
    a. Elakkan Wi-Fi awam untuk urusan sensitif

Keselamatan Data Semasa Menggunakan Alat Gen AI

1. Jangan Masukkan Data Sulit atau PII
    a. Elakkan nama penuh, nombor IC, alamat, atau maklumat kewangan dalam prompt
2. Gunakan *Data Masking*
    a. Tukar butiran sebenar kepada contoh atau placeholder
3. Pilih Platform AI yang Dipercayai
    a. Pastikan ada dasar privasi yang jelas & perlindungan data yang kukuh
4. Semak & Kawal Simpanan Sejarah Perbualan
    a. Matikan “chat history” jika tidak diperlukan
5. Patuhi Dasar & Garis Panduan Organisasi
    a. Ikut polisi dalaman untuk penggunaan AI dengan selamat

Renungan

✅ Gunakan kata laluan dan frasa laluan yang kukuh dan unik

✅ Aktifkan Pengesahan Dua Faktor (2FA)

✅ Arahkan kursor dan semak pautan sebelum klik

✅ Hanya pasang aplikasi daripada sumber yang dipercayai

✅ Sandarkan data penting dengan selamat

✅ Fikir dahulu sebelum berkongsi maklumat dalam talian

07.

Rangka Kerja Undang-Undang - PDPA

Hak Anda di Bawah PDPA

- Akses data peribadi anda pada bila-bila masa
- Betulkan maklumat yang salah atau tidak terkini
- Tarik balik kebenaran penggunaan data anda
- Pilih untuk tidak menerima komunikasi pemasaran

Tanggungjawab Organisasi

Keperluan keselamatan dan pematuhan

- Mesti mendapatkan keizinan sebelum mengumpul data peribadi
- Mesti menerangkan bagaimana data akan digunakan
- Mesti melindungi data peribadi dengan langkah keselamatan yang kukuh
- Mesti memadam data apabila tidak lagi diperlukan
- Mesti membenarkan pengguna mengakses dan membetulkan maklumat mereka

08.
Penutup

Ringkasan Penutup

- Data adalah aset penting — perlindungannya adalah tanggungjawab semua pihak
- Ancaman keselamatan sentiasa wujud — berhati-hati dalam setiap tindakan digital
- Storan awan (cloud) lebih selamat jika dikendalikan dengan amalan terbaik
- Amalkan budaya keselamatan data — bermula dengan diri sendiri setiap hari

Any Questions?

Follow our Social Media

https://twenty-four.io/links/

twenty-four
CONSULTING

Contact Us

Email Address
hello@twenty-four.io

Website
www.twenty-four.io

Phone Number
+60 17-242 4053 (Adam)

Check us out on

Address
Twenty-Four Consulting PLT (202404000540)
No. 8, Jalan Yap Kwan Seng
31st Floor, Menara Ambank
50450 Kuala Lumpur, Malaysia