

NOTA PENERANGAN

SEMESTER	4 DVM	NO. KOD KSKV	DKB4023/P(1/6)
JABATAN	JABATAN TEKNOLOGI MAKLUMAT		
PROGRAM	DIPLOMA TEKNOLOGI MAKLUMAT		
KOD / KURSUS	DKB 4023 KESELAMATAN SIBER		
NO. DAN TAJUK KOMPETENSI	K1 Introduction to Cyber Security K2 Cyber Attacks K3 Malware & Cyber Attacks Operate K4 Scan Network K5 An Introduction to Cryptography & Digital Signatures K6 Ethical Hacking		
NO. KOD KSKV	DKB4023/P(1/6)		

TAJUK: INTRODUCTION TO CYBER SECURITY

PENERANGAN:

Unit ini akan membincangkan tentang perkembangan sistem komputer dan rangkaian:

- 1.1 *What is Cyber Security?*
- 1.2 *Cyber Security Terminology*
- 1.3 *Types of Cyber Security Bkn*
- 1.4 *Types of cybersecurity tools*
- 1.5 *The benefit of cybersecurity*
- 1.6 *Cons and pros of cybersecurity*

1.1 INTRODUCTION TO CYBER SECURITY

Cyber security atau dikenali sebagai keselamatan siber ialah amalan melindungi orang, sistem komputer dan rangkaian daripada kecurian, kerosakan atau akses tanpa kebenaran. Ini bagi memastikan maklumat digital anda selamat daripada serangan siber. Keselamatan siber boleh diibaratkan sebagai setara digital untuk mengunci pintu dan tingkap bagi mengelakkan pecah masuk.

Keselamatan siber menggunakan pelbagai teknologi, proses dan dasar (policies) bagi melindungi daripada kecurian, kerosakan atau akses tanpa kebenaran. Di peringkat perusahaan, keselamatan siber adalah kunci kepada keseluruhan strategi pengurusan risiko, khususnya pengurusan risiko siber. Ancaman keselamatan siber biasanya termasuk perisian tebusan (*ransomware*) dan perisian *malware* yang lain, penipuan pancingan data (*phishing scam*), kecurian data (*data theft*) dan yang terbaru adalah serangan yang dikuasakan oleh kecerdasan buatan (AI). Perbadanan Data Antarabangsa (International Data Corporation) mengunjurkan bahawa perbelanjaan keselamatan akan mencecah USD 377 bilion menjelang 2028.

Serangan siber dan jenayah siber boleh mengganggu, merosakkan dan memusnahkan perniagaan, komuniti serta kehidupan. Insiden keselamatan boleh membawa kepada kecurian identiti, pemerasan dan kehilangan maklumat sensitif, kesan yang boleh menjejaskan perniagaan dan ekonomu dengan ketara.

Kepentingan Cyber Security

Penjenayah siber menggunakan teknologi baharu untuk kelebihan mereka. Sebagai contoh, perniagaan menggunakan pengkomputeran awan (*cloud computing*) untuk kecekapan dan inovasi. Tetapi penjenayah siber melihat kemajuan ini sebagai satu platform yang boleh digunakan untuk dieksploitasi. Keselamatan Siber merupakan aspek yang tidak dapat dipisahkan dari operasi setiap organisasi. Berikut merupakan beberapa kepentingan Keselamatan Siber dalam menjaga kelestarian dan keselamatan organisasi.

i. Melindungi Data dan Maklumat Penting

Salah satu peranan utama keselamatan siber adalah melindungi data dan maklumat penting daripada akses yang tidak sah. Data sensitif seperti maklumat pelanggan, rahsia perniagaan dan maklumat kewangan merupakan sasaran utama bagi para penyerang siber. Strategi keselamatan siber yang kukuh akan membantu memastikan bahawa data tersebut selamat dan terlindung daripada percubaan menggodam.

ii. Mencegah Serangan dan Gangguan Operasi

Serangan siber dapat mengakibatkan gangguan serius terhadap operasi sesebuah organisasi. Serangan malware, ransomware dan serangan DDoS (Distributed Denial of Service) dapat menyebabkan sistem menjadi tidak berfungsi, mengganggu produktiviti dan menyebabkan kerugian kewangan yang signifikan. Penyelesaian keselamatan siber yang dilaksanakan dengan betul membantu mencegah serangan sedemikian dan mengekalkan operasi yang lancar.

iii. Menjaga Kepercayaan Pelanggan

Keamanan data merupakan faktor utama dalam membangun dan memelihara kepercayaan pelanggan. Ketika pelanggan percaya bahawa maklumat peribadi mereka selamat di dalam pangkalan data perniagaan, mereka akan merasa lebih selesa untuk berinteraksi dan menjalankan perniagaan dengan organisasi tersebut. Ini merupakan kepentingan keselamatan siber yang membantu memastikan bahawa data pelanggan tetap dilindungi dan privasi mereka dihormati.

iv. Mematuhi Peraturan dan Standard Keselamatan

Kebanyakan industri memiliki peraturan yang ketat berkaitan keselamatan data dan privasi yang harus dipatuhi oleh entiti perniagaan. Amalan keselamatan siber yang betul membantu perniagaan dalam mematuhi semua peraturan dan piawaian keselamatan yang berkenaan, mengurangkan risiko undang-undang dan kewangan serta membina reputasi sebagai organisasi yang bertanggungjawab secara beretika.

v. Mengurang Risiko Kewangan

Serangan siber boleh menyebabkan kerugian kewangan yang signifikan bagi sesuatu perniagaan. Kos pemulihan, kehilangan pendapatan akibat gangguan operasi, dan denda undang-undang adalah beberapa contoh kesan kewangan yang boleh timbul daripada serangan siber. Melabur dalam penyelesaian keselamatan siber yang berkesan membantu mengurangkan risiko kewangan yang berlaku.

vi. Menjamin Aktiviti Digital Lancar

Dalam era perniagaan yang disambungkan secara digital, kelancaran aktiviti perniagaan sangat bergantung kepada keselamatan infrastruktur teknologi maklumat. Serangan siber dapat mengganggu aktiviti digital seperti komunikasi email, transaksi online dan kerjasama berkumpulan. Pelaksanaan strategi keselamatan siber yang betul memastikan aktiviti digital perniagaan berjalan lancar tanpa gangguan daripada pihak yang tidak bertanggungjawab.

vii. Menjaga Reputasi Perniagaan

Reputasi sesebuah perniagaan merupakan aset yang sangat berharga dan terdedah kepada serangan siber. Pelbagai insiden keselamatan seperti kebocoran data atau serangan ransomware boleh merosakkan reputasi jenama dan mengurangkan kepercayaan pelanggan serta pihak berkepentingan lain.

1.2 CYBER SECURITY TERMINOLOGY

Keselamatan Siber merangkumi pelbagai istilah yang berkaitan dengan melindungi sistem komputer, rangkaian dan data daripada diakses, penggunaan, pendedahan, gangguan, pengubahsuaian atau pemusnahan yang tidak dibenarkan. Konsep utama termasuk *malware*, *phishing*, *encryption*, *firewalls* dan kawalan akses. Memahami istilah ini adalah penting bagi individu dan organisasi untuk mengemudi landskap digital dengan selamat.

(<https://thrivedx.com/resources/article/25-cyber-security-terms>)

Terminologi	Maksud
1. Antivirus Software	Direka untuk mengesan, mencegah dan mengalih keluar malware daripada komputer. Penggunaan perisian antivirus adalah kritikal dalam menjaga peranti daripada ancaman virus, <i>worm</i> dan trojan.
2. Firewall	Firewall ialah sistem keselamatan yang memantau dan mengawal trafik masuk dan keluar rangkaian berdasarkan peraturan yang ditetapkan. Ia penting untuk melindungi rangkaian daripada capaian yang tidak dibenarkan dan ancaman siber
3. Penyulitan (Encryption)	Penyulitan menghalang capaian yang tidak dibenarkan dengan menukar data kepada kod. Alat penting ini melindungi maklumat sensitif, seperti nombor kad kredit atau mesej peribadi, terutamanya apabila dihantar melalui internet.
4. Ransomware	Merupakan perisian malware yang mengunci anda daripada komputer atau fail anda dan menuntut wang tebusan, biasanya dalam mata wang kripto, untuk memulihkan akses.
5. Spyware	Ialah perisian yang memantau aktiviti komputer anda secara rahsia dan mengumpul maklumat peribadi, seperti tabiat menyemak imbas (browsing habits) atau

	kata laluan tanpa kebenaran anda. Spyware sering digunakan untuk tujuan jahat seperti pencurian identiti.
6. Advanced Persistent Threat (APT)	APT adalah serangan siber yang berpanjangan dan disasarkan di mana penceroboh mendapat akses kepada rangkaian dan kekal tersembunyi. Selalunya cuba mencuri maklumat sensitif.
7. Black Hat Hackers	Merupakan penjenayah siber yang mencari dan menggunakan kelemahan dalam rangkaian dan sistem bagi tujuan mencuri data atau menyebarkan <i>malware</i> .
8. Botnet	Merupakan rangkaian komputer yang dijangkiti <i>malware</i> dan dikawal dari jauh oleh penggodam. Botnet sering digunakan untuk melancarkan serangan berskala besar seperti menghantar spam atau melaksanakan serangan <i>Distributed Denial of Service (DdoS)</i>
9. Clickjacking	Merupakan sejenis serangan siber di mana penyerang memperdaya pengguna untuk mengklik pada sesuatu selain daripada apa yang mereka jangkakan. Ini boleh menyebabkan memuat turun perisian hasad atau berkongsi maklumat sensitif secara tidak sengaja.
10. Data Breach (Pencerobohan Data)	Berlaku apabila individu yang tidak dibenarkan mengakses data peribadi, rekod kewangan atau bukti kelayakan log masuk.
11. Deepfake	lalah video atau imej yang dijana AI yang mengubah realiti secara realistik dan meyakinkan. Ini boleh digunakan untuk menyebarkan maklumat salah, melakukan penipuan atau memanipulasi individu.

1.3 TYPES OF CYBER SECURITY

Keselamatan Siber boleh membawa maksud yang berbeza bergantung pada aspek teknologi yang diuruskan. Berikut ialah kategori keselamatan siber yang perlu diketahui oleh pakar IT.

(<https://www.comptia.org/en/blog/what-is-cybersecurity/>)

Jenis Keselamatan Siber	Penerangan
1. Keselamatan Rangkaian (Network Security)	Melibatkan semua aktiviti yang diperlukan untuk melindungi infrastruktur rangkaian anda. Ia mungkin melibatkan mengkonfigurasi Firewall, melindungi VPN, mengurus kawalan akses atau melaksanakan perisian antivirus.
2. Endpoint Security	Endpoint ialah peranti yang disambungkan ke rangkaian anda, termasuk desktop, komputer riba, tablet, peranti mudah alih dan TV pintar. Melindungi Endpoint memerlukan pengesanan ancaman dan aktiviti anomali, penggunaan pengesanan berbilang (multi-factor authentication) dan sebagainya.
3. Keselamatan Aplikasi (Application Security)	Melibatkan konfigurasi tetapan keselamatan dalam aplikasi individu untuk melindunginya daripada serangan siber. Ini mungkin melibatkan penyelesaian pepijat dalam kod dan melaksanakan langkah keselamatan siber untuk melindungi daripada penjahat.
4. Keselamatan Maklumat (Information Security)	Keselamatan maklumat termasuk sebarang perlindungan data yang anda letakkan. Istilah ini melibatkan sebarang aktiviti yang anda lakukan untuk memastikan maklumat pengenalan peribadi dan data sensitif lain kekal di bawah <i>lock and key</i> .
5. Keselamatan Awan (Cloud Security)	Keselamatan awan secara khusus melibatkan aktiviti yang diperlukan untuk mencegah serangan terhadap aplikasi dan infrastruktur awan. Aktiviti ini membantu memastikan semua data kekal peribadi dan selamat antara aplikasi berasaskan internet.
6. Mobile Security	Keselamatan mudah alih memastikan semua peranti dilindungi daripada kelemahan. Memandangkan pengguna semua maklumat sensitif dan menggunakan peranti untuk segala-galanya daripada membeli-belah hingga menghantar e-mel kerja, keselamatan ini akan membantu memastikan data peranti selamat daripada penjenayah siber.

1.4 TYPES OF CYBER SECURITY TOOLS

Dalam era digital yang semakin berkembang pesat, ancaman siber telah menjadi isu global yang serius. Setiap individu, organisasi, mahupun negara terdedah kepada risiko seperti penggodaman, kecurian data, perisian hasad dan pelbagai serangan siber lain. Oleh itu, penggunaan **alat keselamatan siber** amat penting dalam memastikan sistem rangkaian, maklumat dan data sentiasa berada dalam keadaan selamat. Terdapat pelbagai jenis alat keselamatan siber yang digunakan dalam pelbagai aspek pertahanan digital, bergantung kepada fungsi dan keperluan sesebuah sistem.

Jenis Alat Keselamatan Cyber	Penerangan
1. Perisian antivirus dan anti malware	Ia berfungsi untuk mengesan, menyekat dan membuang perisian hasad seperti virus, trojan, spyware, dan ransomware. Perisian ini memainkan peranan penting dalam melindungi sistem daripada serangan yang datang melalui e-mel, fail yang dimuat turun, atau peranti luaran seperti pemacu USB. Contoh perisian terkenal termasuk Windows Defender, Avast, dan Malwarebytes.
2. Firewall	Firewall bertindak sebagai pengawal sempadan antara rangkaian dalaman dan luaran dengan memantau serta mengawal trafik yang masuk dan keluar. Ia boleh berbentuk perisian atau perkakasan, dan membolehkan pengguna menentukan peraturan akses untuk melindungi sistem daripada akses yang tidak sah. Firewall membantu mencegah serangan seperti port scanning, DDoS, dan penyusupan data.
3. Alat Penyulitan (Encryption Tools)	Digunakan untuk menyulitkan maklumat supaya hanya pihak yang diberi kebenaran sahaja dapat membacanya. Ini amat penting terutama dalam komunikasi jarak jauh seperti e-mel dan transaksi kewangan atas talian. Antara contoh alat penyulitan yang digunakan secara meluas ialah Pretty Good Privacy (PGP), VeraCrypt, dan BitLocker.
4. Pengurus Kata Laluan (Password Managers)	Memainkan peranan penting dalam memastikan kerahsiaan dan kekuatan kata laluan. Dengan peningkatan bilangan akaun digital, pengguna sering menggunakan kata laluan yang sama atau lemah. Alat ini membantu menjana, menyimpan dan mengisi kata laluan secara automatik dengan cara yang selamat. Antara pengurus kata laluan yang terkenal termasuk LastPass, Dashlane dan 1Password.

5. Alat pemantauan Rangkaian (Network monitoring tools)	Digunakan untuk memantau prestasi dan keselamatan rangkaian secara masa nyata. Ia membantu mengenal pasti tingkah laku luar biasa, gangguan perkhidmatan, atau penggunaan sumber yang tidak normal. Contoh alat ini ialah Wireshark, Nagios, dan SolarWinds, yang membolehkan pentadbir sistem mengenal pasti dan bertindak terhadap ancaman dengan pantas.
6. Alat Ujian Penembusan (Penetration testing tools)	Digunakan oleh juruaudit keselamatan untuk mensimulasikan serangan siber terhadap sistem dan rangkaian bagi mengenal pasti kelemahan sebelum dieksploitasi oleh pihak luar. Contohnya, Metasploit, Burp Suite, dan Kali Linux merupakan alat penting dalam misi mencari dan membetulkan kelemahan sebelum ia mengundang bencana keselamatan sebenar.

Kesimpulannya, penggunaan alat keselamatan siber adalah satu keperluan dan bukan lagi satu pilihan. Setiap alat mempunyai fungsi tersendiri dan digunakan dalam pelbagai aspek keselamatan maklumat, sama ada pada peringkat individu, organisasi mahupun kerajaan. Dalam menghadapi ancaman siber yang semakin kompleks dan canggih, pengetahuan tentang jenis-jenis alat keselamatan siber dan cara penggunaannya adalah penting untuk memastikan sistem kekal terlindung, operasi tidak terganggu, dan data kekal selamat.

1.5 THE BENEFIT OF CYBERSECURITY

Pada zaman serba digital ini, penggunaan teknologi maklumat telah menyentuh hampir setiap aspek kehidupan manusia – daripada komunikasi, pendidikan, perniagaan sehinggalah kepada pengurusan kerajaan. Dalam keterbukaan dan kepantasan teknologi ini, wujud pula pelbagai ancaman yang boleh menggugat keselamatan sistem dan data. Oleh itu, **keselamatan siber** memainkan peranan yang sangat penting dalam melindungi maklumat digital daripada sebarang ancaman luar seperti pencerobohan, penggodaman, kecurian data, dan serangan perisian hasad. Terdapat pelbagai kelebihan yang diperoleh hasil daripada pelaksanaan sistem keselamatan siber yang berkesan.

Salah satu manfaat utama keselamatan siber ialah **perlindungan terhadap data sensitif**. Dalam dunia moden, data dianggap sebagai aset paling berharga, sama ada data peribadi, kewangan, perniagaan atau kerajaan. Tanpa perlindungan yang kukuh, data ini mudah terdedah kepada akses tidak sah atau penyalahgunaan. Dengan adanya sistem keselamatan siber seperti enkripsi, kawalan akses dan pengesanan pencerobohan, data dapat disimpan dan dihantar dengan selamat serta dapat mengelakkan berlakunya kebocoran maklumat yang serius.

Selain itu, keselamatan siber juga membantu **mencegah kerugian kewangan**. Serangan siber seperti penipuan dalam talian, ransomware dan pencurian identiti boleh menyebabkan kerugian yang sangat besar kepada individu dan organisasi. Contohnya, serangan ransomware boleh menyulitkan sistem penting dan menuntut wang tebusan yang tinggi. Melalui langkah-langkah keselamatan yang betul, seperti penggunaan firewall, antivirus dan sistem pengesanan ancaman, kerugian ini dapat diminimumkan atau dielakkan sama sekali.

Seterusnya, keselamatan siber menyumbang kepada **pengekalan reputasi organisasi**. Dalam perniagaan moden, kepercayaan pelanggan dan pihak berkepentingan terhadap keselamatan maklumat sangat penting. Sebarang kebocoran maklumat atau pencerobohan terhadap sistem boleh menjejaskan nama baik organisasi serta menyebabkan kehilangan kepercayaan. Dengan itu, pelaburan dalam keselamatan siber bukan sahaja melindungi sistem, malah turut menjaga imej dan kredibiliti sesebuah institusi di mata umum.

Keselamatan siber juga memastikan **ketersediaan sistem dan perkhidmatan** sentiasa berjalan lancar tanpa gangguan. Ini sangat penting terutama bagi sektor kritikal seperti perbankan, kesihatan dan pengangkutan, di mana gangguan sistem boleh memberi kesan langsung kepada kehidupan harian masyarakat. Sistem keselamatan seperti alat pemantauan rangkaian dan mekanisme sandaran data akan memastikan sistem dapat pulih dengan cepat sekiranya berlaku serangan.

Tambahan pula, pelaksanaan keselamatan siber yang berkesan akan membantu organisasi **mematuhi peraturan dan undang-undang** yang berkaitan dengan perlindungan data, seperti Akta Perlindungan Data Peribadi (PDPA) di Malaysia. Kegagalan mematuhi peraturan ini bukan sahaja boleh menyebabkan denda dan tindakan undang-undang, malah juga boleh menjejaskan operasi organisasi tersebut.

Akhir sekali, keselamatan siber turut memainkan peranan penting dalam **menjaga keselamatan dan kedaulatan negara**. Infrastruktur penting negara seperti sistem ketenteraan, sistem komunikasi, tenaga dan kesihatan perlu dilindungi daripada ancaman pengintipan siber dan serangan pengganas siber. Serangan ke atas sistem ini boleh menyebabkan ketidakstabilan negara dan menjejaskan keselamatan awam.

Sebagai kesimpulan, keselamatan siber bukan sahaja penting untuk melindungi maklumat dan sistem, tetapi juga untuk menjamin kelangsungan operasi, kestabilan kewangan, reputasi organisasi dan keselamatan negara. Oleh itu, pelaburan dalam keselamatan siber harus dilihat sebagai satu keperluan asas dalam era digital masa kini. Kesedaran dan pendidikan dalam aspek ini juga perlu diperluas agar setiap lapisan masyarakat dapat memainkan peranan mereka dalam membentuk persekitaran digital yang lebih selamat dan beretika.

1.6 CONS AND PROS OF CYBERSECURITY

Keselamatan siber merupakan elemen penting dalam dunia digital masa kini. Ia merangkumi langkah-langkah teknikal dan prosedur yang digunakan untuk melindungi sistem rangkaian, komputer, dan data daripada ancaman siber seperti pencerobohan, perisian hasad, dan pencurian maklumat. Walaupun keselamatan siber memberikan banyak manfaat, ia juga tidak terlepas daripada beberapa kelemahan atau cabaran tertentu. Justeru, penting untuk kita memahami **kebaikan dan keburukan keselamatan siber** secara menyeluruh bagi membolehkan pelaksanaan yang lebih bijak dan efektif.

Kebaikan Keselamatan Siber

Antara kebaikan utama keselamatan siber ialah **perlindungan terhadap data dan sistem**. Dalam dunia yang serba digital, hampir semua urusan melibatkan data sensitif — seperti maklumat peribadi, kewangan, dan korporat. Sistem keselamatan siber memastikan data ini tidak mudah diakses atau dimanipulasi oleh pihak yang tidak bertanggungjawab.

Selain itu, keselamatan siber membantu dalam **mengekal privasi pengguna**. Setiap individu berhak terhadap privasi atas maklumat peribadi mereka. Melalui kaedah penyulitan, kawalan akses, dan kata laluan yang kukuh, keselamatan siber memastikan data pengguna tidak dicerobohi atau disalah guna oleh pihak luar.

Dari sudut perniagaan pula, keselamatan siber menyokong **kelangsungan operasi organisasi**. Serangan siber seperti ransomware atau DDoS boleh melumpuhkan operasi sesebuah organisasi. Dengan sistem keselamatan yang baik, gangguan ini dapat dielakkan dan operasi perniagaan dapat diteruskan tanpa halangan besar.

Satu lagi kelebihan penting ialah **kemampuan mengesan ancaman lebih awal**. Dengan penggunaan sistem pemantauan dan pengesanan ancaman seperti IDS dan SIEM, organisasi boleh mengesan dan bertindak balas terhadap potensi serangan sebelum ia menyebabkan kerosakan besar.

Akhir sekali, keselamatan siber membantu sesebuah organisasi atau institusi **mematuhi undang-undang dan peraturan** berkaitan perlindungan data, seperti Akta Perlindungan Data Peribadi (PDPA). Pemuatan ini bukan sahaja melindungi organisasi daripada tindakan undang-undang, malah turut menunjukkan komitmen mereka terhadap keselamatan dan kepercayaan pengguna.

Keburukan atau Cabaran Keselamatan Siber

Walaupun keselamatan siber sangat penting, terdapat beberapa **kelemahan dan cabaran** yang tidak boleh diabaikan. Salah satu keburukan utama ialah **kos pelaksanaan yang tinggi**. Pembelian perisian keselamatan, peralatan khas, latihan pekerja serta penyelenggaraan sistem memerlukan perbelanjaan yang besar, terutamanya bagi organisasi kecil atau institusi pendidikan.

Selain itu, **kompleksiti teknikal** dalam sistem keselamatan siber juga menjadi satu halangan. Bukan semua organisasi mempunyai kepakaran dalaman yang mencukupi untuk memahami dan mengurus sistem keselamatan yang kompleks. Ini boleh menyebabkan kesilapan konfigurasi dan pendedahan kepada ancaman jika tidak diuruskan dengan betul.

Dari sudut pengguna, sistem keselamatan yang terlalu ketat kadangkala **menyusahkan pengguna harian**. Contohnya, keperluan untuk memasukkan kata laluan yang kompleks dan proses pengesahan berganda (2FA) boleh menimbulkan rasa tidak selesa atau membebankan pengguna biasa.

Tambahan pula, terdapat risiko **positif palsu (false positive)**, di mana sistem keselamatan menganggap sesuatu aktiviti sah sebagai ancaman. Ini boleh menyebabkan gangguan kepada operasi biasa dan menimbulkan kekeliruan dalam kalangan pengguna serta pentadbir sistem.

Akhir sekali, **pemantauan berterusan dan sumber manusia yang cekap** diperlukan untuk memastikan sistem keselamatan sentiasa dikemaskini dan mampu bertindak terhadap ancaman baru. Kekurangan perhatian dalam hal ini boleh menyebabkan sistem keselamatan menjadi usang dan mudah ditembusi.

Kesimpulan

Secara keseluruhan, keselamatan siber membawa lebih banyak kebaikan berbanding keburukan. Ia sangat penting dalam memastikan sistem dan maklumat kekal selamat dalam dunia digital yang penuh ancaman. Walaupun terdapat cabaran seperti kos tinggi dan kesukaran teknikal, kesedaran dan pelaburan dalam keselamatan siber adalah sangat berbaloi. Pengguna dan organisasi perlu mengambil langkah proaktif untuk menyeimbangkan antara keselamatan dan kemudahan penggunaan bagi memastikan perlindungan yang menyeluruh dan berkesan dalam jangka masa panjang.

Rujukan :

<https://privy.id/blog/pentingnya-cyber-security/>

[https://www.researchgate.net/publication/376600966 CYBER SECURITY TOOLS AND THEIR USES](https://www.researchgate.net/publication/376600966_CYBER_SECURITY_TOOLS_AND_THEIR_USES)

<https://powerconsulting.com/blog/pros-and-cons-cyber-security/>