MSIM4404
Edisi 1

MODUL 01

Keamanan dan Ancaman pada *Cyberspace*

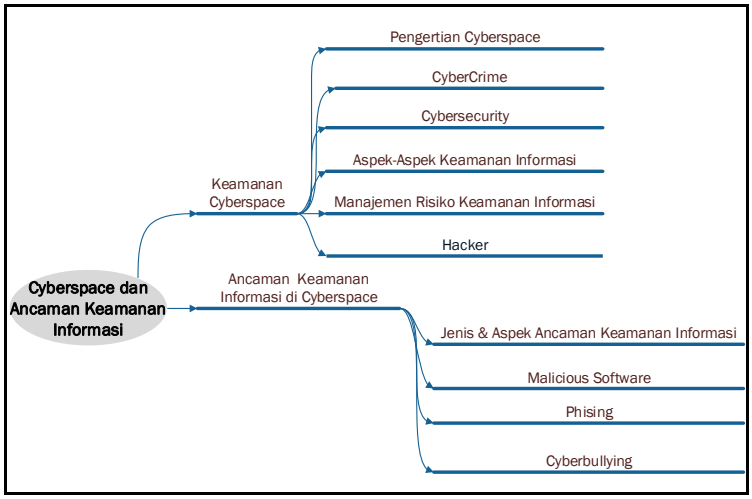
Zaenal Arifin, S.T., M.Kom.

Daftar Isi

Pendahuluan

Sebagai dasar dalam mempelajari keamanan jaringan, perlu dipelajari dan dipahami terlebih dahulu yang dimaksud dengan istilah-istilah *cyber*, di antaranya *cyberspace*, *cyberlaw*, *cyber security* dan hal-hal yang termasuk aspek-aspek keamanan informasi, manajemen risiko, keamanan informasi, dan berkaitan dengan *hacker*.

Selanjutnya dalam modul ini akan dibahas tentang ancaman dan gangguan yang umum terjadi di dunia maya. Terdapat beberapa jenis dan aspek ancaman serta beberapa bentuk ancaman yang umum terjadi di dunia maya, seperti *malicious software*, aktivitas *phising*, *cyberbullying*.



Gambar 1.1
Mind Map Cyberspace dan Ancaman Keamanan Informasi

Setelah mempelajari Modul 1, Anda diharapkan mampu:

1. menjelaskan pengertian *cyberspace*,
2. menjelaskan pengertian *cybercrime*,
3. menjelaskan pengertian *cyber security*,
4. menguraikan manajemen risiko keamanan informasi,
5. menguraikan aspek-aspek keamanan informasi,
6. menjelaskan sistem keamanan jaringan,
7. menyebutkan jenis-jenis peretas (*hacker)*,
8. menguraikan jenis dan aspek ancaman keamanan informasi,
9. menyebutkan *malicious software* (perangkat lunak berbahaya),
10. menjelaskan aktivitas *phising*,
11. menjelaskan aktivitas *cyberbullying*.

Kegiatan Belajar 1

Keamanan *Cyberspace*

Cyberspace atau dunia maya merupakan hasil integrasi dari media elektronik dan peralatan teknologi jaringan komunikasi; yang terhubung dengan peralatan komunikasi yang tersebar di seluruh penjuru dunia dan digunakan untuk keperluan saling berkomunikasi secara *online*.

A. PENGERTIAN *CYBERSPACE*

Kata *cyberspace* berasal dari kata *cybernetics* dan *space*, pertama kali diperkenalkan oleh penulis novel fiksi ilmiah, William Gibson dalam buku ceritanya, *Burning Chrome* tahun 1982 dan menjadi populer pada novel berikutnya, *Neuromancer* pada tahun 1984 yang menyebutkan bahwa:

> *"Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding".*

Menurut Dysson, *cyberspace* merupakan suatu ekosistem biolektronik di semua tempat yang memiliki telepon, kabel *coaxial*, *fiber optic*, atau gelombang elektromagnetik. *Cyberspace* memiliki beberapa karakteristik sebagai berikut.

1. Beroperasi secara *virtual* atau maya. Berada di dalam dunia maya, dihuni oleh orang-orang yang saling berinteraksi, berdiskusi, dan bertukar pikiran, tetapi tanpa harus melakukan pertemuan secara fisik. Dan sebenarnya penghuni dunia maya tidak hanya manusia, tetapi termasuk di dalamnya ada data, informasi, surat elektronik, ide-ide, dan bahkan sampai pada ilmu pengetahuan. Dunia maya penuh lalu-lalang data dan informasi.
2. Dunia *cyber* selalu berubah dengan cepat karena interaksi yang dilakukan oleh hampir semua orang dari seluruh dunia; dengan didukung kemudahan *update* data maka perubahan yang terjadi dalam dunia *cyber* pun sangat cepat.

3. Dunia maya tidak mengenal batas-batas teritorial, penghuni *cyberspace* tersebar di banyak negara melakukan interaksi tanpa mengenal batas teritorial.
4. Orang-orang yang hidup dalam dunia maya dapat melaksanakan aktivitas tanpa harus menunjukkan identitasnya karena interaksi yang dilakukan dalam *cyberspace* tidak melibatkan interaksi secara fisik maka interaksi yang dilakukan pun tidak harus menunjukkan identitas yang sesungguhnya.
5. Informasi di dalamnya bersifat publik. Suatu hal yang amat bernilai di dalam *cyberspace* adalah informasi atau "hasil pemikiran intelektual" yang bersifat publik, tidak dimiliki oleh siapa pun dan tidak memerlukan otorisasi bagi siapa pun untuk menggunakannya hanya bagi dirinya sendiri.

B. *CYBERCRIME*

Informasi merupakan suatu aset yang sangat berharga dan merupakan salah satu sumber daya strategis untuk meningkatkan nilai usaha dan kepercayaan publik. Informasi dikumpulkan, disimpan, diorganisasikan, dan disebarluaskan dalam berbagai bentuk, salah satunya adalah dalam bentuk berkas elektronik atau digital. Informasi yang memiliki nilai dan merupakan *asset* tidak luput dari ancaman, berbagai cara digunakan untuk memperoleh informasi tersebut secara ilegal, aktivitas tersebut dikenal sebagai *cybercrime*.

Cybercrime merupakan aktivitas kejahatan dengan menggunakan teknologi komputer atau jaringan komputer sebagai alat, sasaran maupun tempat terjadinya kejahatan. Menurut Andi Hamzah dalam bukunya *Aspek-Aspek Pidana di Bidang Komputer* mendefinisikan *cybercrime* sebagai kejahatan di bidang komputer, yang secara umum dapat diartikan sebagai penggunaan komputer secara ilegal.

Beberapa faktor aktivitas *cybercrime* sebagai berikut.

1. Segi teknis, adanya teknologi internet akan menghilangkan batas wilayah negara, saling terhubungnya antara jaringan yang satu dengan jaringan yang lain memudahkan pelaku kejahatan untuk melakukan aksinya.
2. Segi sosio-ekonomi, adanya *cybercrime* menghasilkan nilai ekonomi. Aktivitas kejahatan di dunia maya berkorelasi dengan keamanan jaringan sehingga banyak pengguna yang sangat membutuhkan perangkat keamanan jaringan, hal ini menyebabkan *cybercrime* merupakan bagian dari kegiatan ekonomi dunia.

Ruang lingkup dalam *cybercrime*, antara lain:

1. komputer sebagai instrumen untuk melakukan kejahatan, seperti pencurian, penipuan, dan pemalsuan melalui internet;
2. komputer dan perangkatnya sebagai objek penyalahgunaan, data-data di dalam komputer yang menjadi objek kejahatan diubah, dimodifikasi, dihapus, atau diduplikasi secara tidak sah;

3. penyalahgunaan yang berkaitan dengan komputer atau data, digunakan secara ilegal atau tidak sah;
4. akuisisi, pengungkapan, atau penggunaan informasi dan data yang tidak sah, berkaitan dengan masalah penyalahgunaan hak akses dengan cara-cara yang ilegal.

Jenis-jenis *cybercrime* berdasarkan motif, terdiri dari:

1. sebagai tindak kriminal murni. Kejahatan dilakukan secara sengaja dengan memanfaatkan internet sebagai sarana kejahatan. Sebagai contoh *carding*, yakni pencurian nomor kartu kredit milik orang lain untuk digunakan dalam transaksi perdagangan di internet;
2. sebagai tindakan kejahatan "abu-abu". Aktivitasnya sulit untuk dianggap sebagai tindak kriminal atau bukan; karena motif kegiatannya belum tentu bukan untuk berbuat kejahatan. Contohnya aktivitas *port scanning* merupakan aktivitas pengumpulan informasi terhadap kondisi *port* pada suatu sistem milik orang lain.

Jenis-jenis *cybercrime* berdasarkan sasaran, terdiri dari berikut ini.

1. *Cybercrime* yang menyerang individu. Kejahatan yang dilakukan terhadap seseorang atau individu dengan motif dendam atau iseng yang bertujuan untuk merusak nama baik. Contoh: pornografi, *cyberstalking*, *cyber trespass*.
2. *Cybercrime* yang menyerang hak cipta (hak milik). Kejahatan yang dilakukan terhadap hasil karya seseorang dengan motif menggandakan, memasarkan, mengubah yang bertujuan untuk kepentingan materi/non materi.
3. *Cybercrime* yang menyerang pemerintah. Kejahatan yang dilakukan terhadap aset yang dimiliki oleh pemerintah dengan motif melakukan teror, membajak, ataupun merusak keamanan untuk merusak citra institusi pemerintah.

C. *CYBER SECURITY*

Ancaman di dunia maya beragam bentuknya, jika ancaman tersebut berubah menjadi serangan maka akan dapat menimbulkan risiko terhadap sistem yang diserang. Untuk meminimalisasi risiko yang dapat terjadi akibat serangan terhadap suatu sistem maka diperlukan upaya pengamanan terhadap sistem. *Cyber security* merupakan aktivitas pengamanan terhadap sumber daya teknologi informasi untuk mencegah terjadinya *cybercrime*.

Cyber security adalah bagian dari keamanan informasi yang melindungi sistem yang terhubung ke internet, termasuk perangkat keras, perangkat lunak, program, dan data dari potensi serangan *cyber*. Melindungi integritas jaringan dari akses elektronik yang tidak sah. Keamanan jaringan adalah keamanan *cyber* yang dirancang untuk melindungi integritas jaringan dan data apa pun yang dikirim melalui perangkat jaringan. *Cyber security* atau keamanan dunia maya mengarah pada teknologi, proses,

dan praktik yang dirancang untuk melindungi jaringan, perangkat, program, dan data dari serangan, kerusakan, atau akses tidak sah.

Peran *cyber security* sangat penting karena pada umumnya semua organisasi pemerintah, militer, perusahaan swasta melakukan aktivitas pengumpulan, pemrosesan, dan penyimpanan data di komputer dan perangkat lain yang terhubung dengan jaringan. Umumnya data tersebut dapat berupa informasi sensitif sehingga jika terdapat pengungkapan data secara tidak sah dapat menimbulkan dampak negatif. Keamanan informasi mengacu pada proses dan teknik yang digunakan untuk melindungi informasi dan data sensitif dari akses yang tidak sah, dalam bentuk cetak atau elektronik. Informasi adalah sesuatu yang bernilai bagi setiap orang dan bisnis, yang lebih penting dalam melindungi mereka dari pencurian atau cedera. Keamanan informasi, yang dirancang untuk menjaga kerahasiaan, integritas, dan ketersediaan data.

D. MANAJEMEN RISIKO KEAMANAN INFORMASI

Manajemen risiko adalah proses untuk menyeimbangkan biaya operasional dan ekonomi terhadap langkah perlindungan dan mencapai keuntungan dalam kemampuan misi dengan melindungi sistem teknologi informasi dan data yang mendukung misi organisasi. Pengertian lain dari manajemen risiko adalah proses identifikasi kerentanan dan ancaman terhadap sumber daya informasi yang digunakan oleh organisasi dalam mencapai tujuan bisnis dan memutuskan penanggulangan atau menentukan mekanisme kontrol yang akan dilakukan untuk mengurangi risiko sampai pada tingkat yang dapat diterima.

Perangkat *hardware*, *software*, sistem, informasi, dan manusia merupakan aset bagi suatu organisasi yang perlu/harus dilindungi dari risiko keamanannya. Mekanisme pengamanan informasi tidak bisa hanya disandarkan semata-mata hanya pada peralatan (*tools*) pengamanan teknologi informasi saja, melainkan perlu adanya pemahaman dari organisasi tentang apa yang harus dilindungi dan menentukan secara tepat solusi yang dapat menangani permasalahan terhadap kebutuhan keamanan informasi. Pengelolaan keamanan informasi perlu dilakukan secara sistemik dan komprehensif.

Untuk dapat membangun dan menerapkan sistem keamanan informasi, organisasi sebaiknya memulai dengan melakukan analisis terhadap risiko-risiko yang mungkin timbul akibat dari penerapan sistem keamanan yang kurang efektif. Analisis risiko yang dilakukan secara periodik dan berkesinambungan dilakukan dengan suatu pendekatan sistematis dari proses berikut.

1. Identifikasi terhadap kejadian-kejadian yang dapat mengancam keamanan informasi dan potensi dampak kerugian yang ditimbulkan jika mekanisme kontrol kurang efektif.
2. Analisis tingkat peluang/probabilitas terjadinya hal-hal yang tidak diinginkan tersebut akibat adanya sejumlah kelemahan pada sistem yang tidak dilindungi dengan kontrol tertentu.

Hasil dari analisis tersebut akan menghasilkan nilai prioritas dalam mengambil sejumlah tindakan terkait dengan risiko keamanan informasi yang dihadapi. Dengan adanya prioritas yang jelas maka akan dapat didefinisikan kontrol-kontrol mana saja yang perlu diterapkan.

Risiko didefinisikan sebagai potensi *output* yang tidak diharapkan dari pelanggaran keamanan informasi oleh ancaman keamanan informasi. Untuk mengatasi risiko keamanan diperlukan kemampuan dalam mengelola risiko keamanan informasi dengan mengikuti tahapan-tahapan berikut.

1. Membangun *asset* berbasis profil ancaman, langkah ini akan menghasilkan sebagai berikut.
   a. Daftar *asset* yang penting bagi organisasi.
   b. Kebutuhan keamanan terhadap *asset* penting.
   c. Praktik keamanan terkini yang telah diterapkan oleh organisasi untuk melindungi *asset*.
   d. Daftar kelemahan kebijakan organisasi terkini.
2. Mengidentifikasi kerentanan pada infrastruktur teknologi informasi, pada tahap ini mengevaluasi kelemahan perangkat-perangkat teknologi informasi seperti *server*, PC, perangkat jaringan.
3. Mengembangkan strategi keamanan dan perencanaannya.

Dari tahap 1 dan 2 diperoleh profil ancaman dan kelemahan infrastruktur sistem jaringan informasi. Tahap 3 menindaklanjuti dengan merangkum kegiatan sebelumnya menjadi bentuk profil risiko dengan tingkat ukuran risiko (secara kualitatif) yang dikaitkan dengan dampaknya bagi perusahaan serta rencana mitigasi risiko. *Output* dari tahap ini, antara lain:

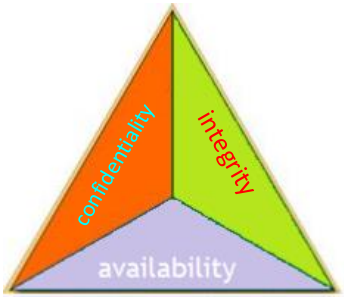
1. daftar risiko-risiko terhadap aset-aset penting,
2. mengukur tingkat risiko,
3. strategi proteksi,
4. rencana-rencana pengurangan/mitigasi risiko.

E. ASPEK-ASPEK KEAMANAN INFORMASI

Bentuk dan mekanisme penyimpanan informasi dapat terdiri dari berbagai macam bentuk; tetapi harus selalu ada upaya untuk melindungi keamanan informasi tersebut sebaik mungkin. Data dan informasi yang berada di dalam suatu infrastruktur jaringan dikatakan aman, jika memenuhi 3 aspek keamanan informasi berikut.

1. **Kerahasiaan (*confidentiality*),** aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima, dan disimpan.

2. **Keutuhan (*integrity*),** aspek yang menjamin akurasi dan keutuhan informasi serta menjaga informasi dari kerusakan atau ancaman lain yang mengakibatkan berubah informasi dari aslinya.
3. **Ketersediaan (*availability*),** aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan pengguna yang berhak dapat mengakses informasi kapan pun, tanpa adanya gangguan kegagalan akses informasi.



Gambar 1.2
Triangle CIA (*Confidentility*, *Integrity*, *Availability*)

Tiga elemen dasar *confidentiality*, *integrity*, dan *availability* (CIA) merupakan dasar di antara program-program keamanan yang dikembangkan. Ketiga elemen tersebut merupakan mata rantai yang saling berkaitan dalam konsep perlindungan informasi.

Keamanan bisa dicapai dengan beberapa cara, strategi-strategi dari keamanan informasi masing-masing memiliki fokus dan dibangun berdasarkan tujuan tertentu sesuai kebutuhan. Contoh dari keamanan informasi, antara lain:

1. ***personal security*** adalah keamanan informasi yang berhubungan dengan keamanan personil,
2. ***physical security*** adalah keamanan informasi yang memfokuskan pada strategi untuk mengamankan individu atau anggota organisasi, *asset* fisik, dan tempat kerja dari berbagai ancaman,
3. ***operasional security*** adalah keamanan informasi yang membahas strategi suatu organisasi untuk mengamankan organisasi sehingga dapat beroperasi tanpa gangguan,
4. ***communication security*** adalah keamanan informasi yang bertujuan mengamankan media dan teknologi komunikasi serta apa yang ada di dalamnya,
5. ***network security*** adalah keamanan informasi yang memfokuskan pada pengamanan peralatan jaringan, jaringan dan isinya, serta kemampuan untuk menjaga jaringan tersebut agar tetap dapat melakukan fungsi komunikasi data dalam organisasi.

E. SISTEM KEAMANAN JARINGAN

Beberapa pengertian yang terkait dengan sistem keamanan jaringan sebagai berikut.

1. Sistem keamanan jaringan adalah suatu sistem yang memiliki tugas untuk melakukan pencegahan dan identifikasi kepada pengguna yang tidak sah dalam jaringan komputer. Langkah pencegahan ini berfungsi untuk menghentikan penyusup untuk mengakses lewat sistem jaringan komputer. Tujuan dari dilakukan sistem keamanan jaringan komputer adalah untuk antisipasi dari ancaman dalam bentuk fisik maupun logik baik secara langsung atau tidak langsung yang mengganggu sistem keamanan jaringan.
2. Keamanan jaringan merupakan salah satu bentuk untuk memonitor akses jaringan dan mencegah segala bentuk penyalahgunaan sumber daya jaringan yang tidak sah.
3. Keamanan jaringan menurut Mariusz Stawowski dalam jurnalnya "*The Principles of Network Security Design*" adalah keamanan jaringan yang utama sebagai upaya perlindungan sumber daya sistem terhadap ancaman yang berasal dari luar jaringan.
4. Sistem keamanan jaringan adalah proses untuk mengidentifikasi dan mencegah pengguna yang tidak sah dari suatu jaringan komputer. Tujuannya tentu saja untuk mengantisipasi risiko ancaman berupa perusakan bagian fisik komputer maupun pencurian data seseorang.

Tugas dari keamanan jaringan ini dikontrol oleh seorang administrator jaringan. Keamanan jaringan menjadi salah satu cara untuk memproteksi atau memberikan perlindungan terhadap jaringan dari berbagai ancaman luar yang datang, yang berpotensi merusak jaringan.

G. *HACKER*

Terkadang suatu teknologi atau suatu sistem informasi yang telah dibuat memiliki kerentanan; untuk menemukan kerentanan sistem diperlukan personil yang mampu melakukan analisis dengan mempelajari sistem tersebut secara mendalam sehingga ditemukan titik-titik kritis dari kerentanan agar dapat segera dilakukan upaya perbaikan. Personil tersebut dikenal sebagai *hacker*.

Hacker umumnya mempunyai keinginan untuk mengetahui secara mendalam mengenai cara kerja suatu sistem, komputer atau jaringan komputer sehingga menjadi ahli dalam bidang penguasaan sistem, komputer atau jaringan komputer. *Hacker* menggunakan keahliannya untuk mengidentifikasi kekurangan dalam sistem komputer dan berupaya untuk memperbaikinya untuk mencegah insiden lain dari akses yang tidak sah.

Hacker dalam menganalisis kelemahan suatu sistem tidak merusak keadaan/kondisi aslinya; sebab tujuan dari aktivitas *hacker* adalah hanya untuk mencari kelemahan atau celah keamanan. *Hacker* memiliki etika serta mengetahui dan menyadari seluruh akibat dari apa yang dilakukannya, dan bertanggung jawab atas apa yang dilakukannya.

Hacker dapat diklasifikasi secara umum menjadi tiga kategori berikut.

1. ***White hat hacker,*** seseorang yang mencoba untuk mempelajari, menganalisis dan mengetahui kelemahan suatu sistem sebagai bagian dari aktivitas *vulnerability assessment* atau *penetration testing* yang bertujuan untuk memperbaiki atau memberikan rekomendasi perbaikan terhadap adanya temuan terhadap kerentanan sistem.
2. ***Black hat hacker*** atau dikenal dengan *cracker* adalah seseorang yang mencoba untuk mempelajari, menganalisis, dan mengetahui kelemahan sebuah sistem untuk merusak atau mencuri informasi yang sensitif. Umumnya motivasi utama mereka adalah menggunakan pengetahuan untuk mendapatkan data pribadi yang penting, atau mencuri uang dari rekening bank, atau kegiatan yang bersifat negatif lainnya.
4. ***Grey hat hacker*** merupakan seseorang yang menjadi konsultan keamanan, tetapi kadang kala pada situasi dan kondisi lain melakukan penyerangan dengan memanfaatkan kelemahan sistem dari sebuah target.

Beberapa jenis *hacker* berdasarkan tujuan meretas sistem dapat dikelompokkan sebagai berikut.

1. ***Red hat hacker*** merupakan mirip *white hat hacker*, tidak hanya berupaya mempertahankan sistem, tetapi juga dalam kondisi tertentu berupaya menyerang peretas lain. Umumnya *red hat hacker* merupakan agen pemerintah.
2. ***State-sponsored hackers*** merupakan *hacker* terlatih yang dibiayai oleh negara atau pemerintah biasanya bertujuan untuk mata-mata dan perang *cyber* (*cyber warfare*).
3. ***Cyber terrorist*** mereka menyebarkan ancaman-ancaman untuk tujuan tertentu.
4. ***Hacktivist*** merupakan *black hat* yang menyerang sambil menyebarkan suatu pesan khusus, misalnya melalui *deface website*.
5. ***Corporate hacker*** merupakan *hacker* yang menyerang properti intelektual dan data penting suatu perusahaan. Tujuan mereka adalah untuk mendapatkan informasi mengenai kompetitor suatu perusahaan.
6. ***Script kiddies*** merupakan *hacker* pemula yang memiliki sedikit pengetahuan dan menggunakan *tools* buatan orang lain, biasanya tidak dapat mengembangkan serangan dan pertahanan.
7. ***Blue hat hackers*** biasanya sebagai konsultan keamanan komputer yang terbiasa melakukan *bug-test* sistem sebelum diluncurkan. Mereka mencari celah yang bisa dimanfaatkan dalam rangka untuk mencoba menutup celah ini.

Latihan

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

1) Sebutkan dan jelaskan jenis-jenis *hacker*! Jelaskan pula perbedaan *hacker* dan *cracker*!
2) Sebutkan dan jelaskan jenis-jenis *cybercrime*!
3) Sebutkan dan jelaskan tahapan-tahapan dalam mengelola risiko keamanan!
4) Jelaskan pengertian dari keamanan jaringan dan hubungannya dengan *cyberspace*!
5) Jelaskan manfaat mempelajari keamanan jaringan!

Petunjuk Jawaban Latihan

1) Jenis-jenis *hacker* dan perbedaan *hacker* dan *cracker*.
   Hacker dapat diklasifikasi secara umum menjadi tiga kategori berikut.
   a) *White hat hacker*, seseorang yang mencoba untuk mempelajari, menganalisis, dan mengetahui kelemahan sebuah sistem sebagai bagian dari aktivitas *vulnerability assessment* atau *penetration testing* yang bertujuan untuk memperbaiki atau memberikan rekomendasi perbaikan terhadap adanya temuan terhadap kerentanan sistem.
   b) *Black hat hacker* atau dikenal dengan *cracker* adalah seseorang yang mencoba untuk mempelajari, menganalisis, dan mengetahui kelemahan sebuah sistem untuk merusak atau mencuri informasi yang sensitif.
   c) *Grey hat hacker* merupakan seseorang yang menjadi konsultan keamanan, tetapi terkadang di situasi dan kondisi lain melakukan penyerangan dengan memanfaatkan kelemahan sistem dari sebuah target.

   Beberapa jenis *hacker* berdasarkan tujuan meretas sistem sebagai berikut.
   a) *Red hat hacker* merupakan mirip *white hat hacker*, tidak hanya berupaya mempertahankan sistem, tetapi juga dalam kondisi tertentu berupaya menyerang peretas lain.
   b) *State-sponsored hackers* merupakan *hacker* terlatih yang dibiayai oleh negara atau pemerintah biasanya bertujuan untuk mata-mata dan perang *cyber* (*cyber warfare*).
   c) *Cyber terrorist* mereka menyebarkan ancaman-ancaman untuk tujuan tertentu.
   d) *Hacktivist* merupakan *black hat* yang menyerang sambil menyebarkan suatu pesan khusus, misalnya melalui *deface website*.

e) *Corporate hacker* merupakan *hacker* yang menyerang properti intelektual dan data penting suatu perusahaan. Tujuan mereka adalah untuk mendapatkan informasi mengenai kompetitor suatu perusahaan.

f) *Script kiddies* merupakan *hacker* pemula yang memiliki sedikit pengetahuan dan menggunakan *tool* buatan orang lain, biasanya tidak dapat mengembangkan serangan dan pertahanan.

g) *Blue hat hackers* biasanya sebagai konsultan keamanan komputer yang terbiasa melakukan *bug-test* sistem sebelum diluncurkan. Mereka mencari celah yang bisa dimanfaatkan dan mencoba menutup celah ini.

2) Jenis-jenis *cybercrime*.

Jenis-jenis *cybercrime* berdasarkan motif, antara lain:

a) sebagai tindak kriminal murni. Kejahatan dilakukan secara sengaja dengan memanfaatkan internet sebagai sarana kejahatan. Contoh *carding*, pencurian nomor kartu kredit milik orang lain untuk digunakan dalam transaksi perdagangan di internet,

b) aktivitasnya sulit untuk dianggap sebagai tindak kriminal atau bukan karena motif kegiatannya belum tentu bukan untuk berbuat kejahatan. Contohnya aktivitas *port scanning* merupakan aktivitas pengumpulan informasi terhadap kondisi *port* pada suatu sistem milik orang lain.

Jenis-jenis *cybercrime* berdasarkan sasaran sebagai berikut.

a) *Cybercrime* yang menyerang individu. Kejahatan yang dilakukan terhadap seseorang atau individu dengan motif dendam atau iseng yang bertujuan untuk merusak nama baik. Contoh: pornografi, *cyberstalking*, *cyber trespass*.

b) *Cybercrime* yang menyerang hak cipta (hak milik). Kejahatan yang dilakukan terhadap hasil karya seseorang dengan motif menggandakan, memasarkan, mengubah yang bertujuan untuk kepentingan materi/nonmateri.

c) *Cybercrime* yang menyerang pemerintah. Kejahatan yang dilakukan terhadap aset yang dimiliki oleh pemerintah dengan motif melakukan teror, membajak, atau pun merusak keamanan untuk merusak citra institusi pemerintah.

3) Tahapan-tahapan dalam mengelola risiko keamanan sebagai berikut.

a) Membangun aset berbasis profil ancaman.

b) Mengidentifikasi kerentanan pada infrastruktur teknologi informasi, pada tahap ini mengevaluasi kelemahan perangkat-perangkat teknologi informasi.

c) Mengembangkan strategi keamanan dan perencanaannya. Dari tahap 1 dan 2 diperoleh profil ancaman dan kelemahan infrastruktur sistem jaringan informasi. Tahap 3 menindaklanjuti dengan merangkum kegiatan sebelumnya menjadi bentuk profil risiko dengan tingkat ukuran risiko (secara kualitatif) yang dikaitkan dengan dampaknya bagi perusahaan serta rencana mitigasi risiko.

4) Pengertian dari keamanan jaringan dan hubungannya dengan *cyberspace*.
Petunjuk: pahami terlebih dahulu *cyberspace* dan keamanan jaringan, kemudian korelasikan kedua hal tersebut.

5) Manfaat mempelajari keamanan jaringan.
Petunjuk: apa yang Anda rasakan dengan mempelajari keamanan jaringan?

Rangkuman

Cyberspace atau dunia maya merupakan hasil integrasi dari media elektronik dan peralatan teknologi jaringan komunikasi dengan menghubungkan peralatan komunikasi yang tersebar di seluruh penjuru dunia digunakan untuk keperluan komunikasi secara *online.*

Cybercrime merupakan aktivitas kejahatan dengan menggunakan teknologi komputer atau jaringan komputer sebagai alat, sasaran maupun tempat terjadinya kejahatan.

Cyber security merupakan aktivitas pengamanan terhadap sumber daya teknologi informasi untuk mencegah terjadinya *cybercrime*. Keamanan informasi, yang dirancang untuk menjaga

1. kerahasiaan (*confidentiality*), aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima, dan disimpan,
2. keutuhan (*integrity*), aspek yang menjamin akurasi dan keutuhan informasi serta menjaga informasi dari kerusakan atau ancaman lain yang mengakibatkan berubah informasi dari aslinya,
3. ketersediaan (*availability*), aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan pengguna yang berhak dapat mengakses informasi kapan pun, tanpa adanya gangguan kegagalan akses informasi.

Analisis risiko yang dilakukan secara periodik dan berkesinambungan dilakukan dengan suatu pendekatan sistematis dari proses berikut.

1. Identifikasi terhadap kejadian-kejadian yang dapat mengancam keamanan informasi dan potensi dampak kerugian yang ditimbulkan jika mekanisme kontrol kurang efektif.
2. Analisis tingkat probabilitas terjadinya hal-hal yang tidak diinginkan tersebut akibat adanya sejumlah kelemahan pada sistem yang tidak dilindungi dengan kontrol tertentu.

Hacker umumnya mempunyai keinginan untuk mengetahui secara mendalam mengenai cara kerja suatu sistem, komputer atau jaringan komputer sehingga menjadi ahli dalam bidang penguasaan sistem, komputer, atau jaringan komputer.

Tes Formatif 1

Pilihlah satu jawaban yang paling tepat!

1) Yang dimaksud dengan risiko adalah ....
   A. kejadian-kejadian yang dapat mengancam
   B. potensi *output* yang tidak diharapkan dari suatu pelanggaran
   C. kerentanan pada infrastruktur teknologi informasi
   D. potensi *output* yang diharapkan dari suatu pelanggaran

2) Aspek keamanan informasi yang menjamin akurasi dan keutuhan informasi adalah ....
   A. *confidentiality*
   B. *integrity*
   C. *availability*
   D. *authorization*

3) Keamanan informasi yang memfokuskan pada pengamanan peralatan jaringan, jaringan, dan isinya adalah ….
   A. *communication security*
   B. *operasional security*
   C. *network security*
   D. *personal security*

4) Berikut ini merupakan definisi dari sistem keamanan jaringan, *kecuali* ….
   A. upaya perlindungan sumber daya sistem terhadap ancaman yang berasal dari luar jaringan
   B. proses untuk mengidentifikasi dan mencegah pengguna yang tidak sah dari suatu jaringan komputer
   C. untuk memonitor akses jaringan dan mencegah segala bentuk penyalahgunaan sumber daya jaringan yang tidak sah
   D. untuk memonitor akses jaringan dan mencegah segala bentuk penyalahgunaan sumber daya jaringan yang tidak sah

5) *Hacker* yang memiliki sedikit pengetahuan dan menggunakan *tool* adalah ….
   A. *script kiddies*
   B. *black hat*

C. *red hat*
D. jawaban A, B, dan C salah

6) Proses mengidentifikasi kerentanan dan ancaman terhadap sumber daya informasi untuk menentukan mekanisme kontrol disebut ….
A. manajemen keamanan informasi
B. manajemen keamanan jaringan
C. manajemen risiko keamanan informasi
D. jawaban A, B, dan C benar

7) Berikut ini merupakan jenis-jenis *cybercrime* berdasarkan sasaran, *kecuali* ….
A. menyerang individu
B. menyerang hak cipta
C. menyerang pemerintah
D. *port scanning*

8) Contoh jenis *cybercrime* yang merupakan tindakan krimal murni adalah ….
A. *port scanning*
B. *carding*
C. *gathering information*
D. jawaban A, B, dan C salah

9) Berikut ini merupakan karakteristik dari *cyberspace*, *kecuali* ….
A. tidak mengenal batas-batas teritorial *marine* klimatologi
B. dapat melaksanakan aktivitas tanpa harus menunjukkan identitasnya
C. informasi di dalamnya bersifat privat
D. selalu berubah dengan cepat

10) Berikut ini adalah ruang lingkup dari *cybercrime*, *kecuali* ....
A. komputer dan perangkatnya sebagai objek penyalahgunaan
B. penyalahgunaan yang berkaitan dengan komputer atau data, digunakan secara ilegal atau tidak sah
C. komputer sebagai instrumen untuk melakukan kejahatan
D. akuisisi, pengungkapan, atau penggunaan informasi dan data yang sah

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 1 yang terdapat di bagian akhir modul ini. Hitunglah jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 1.

$$\text{Tingkat Penguasaan} = \frac{\text{Jumlah Jawaban yang Benar}}{\text{Jumlah Soal}} \times 100$$

Arti tingkat penguasaan

<70%	70% - 79%	80% - 89%	90% - 100%
kurang	cukup	baik	baik sekali

Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan Kegiatan Belajar 2. **Bagus!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 1, terutama bagian yang belum dikuasai.

Kegiatan Belajar 2

Ancaman Keamanan Informasi pada *Cyberspace*

Ancaman adalah aksi yang terjadi dari dalam atau luar sistem yang dapat mengganggu keseimbangan sistem informasi. Ancaman keamanan informasi dapat berasal dari individu, organisasi, mekanisme, atau peristiwa yang memiliki potensi untuk membahayakan sumber daya informasi perusahaan.

A. JENIS DAN ASPEK ANCAMAN KEAMANAN INFORMASI

Berdasarkan sumbernya ancaman dapat berasal dari:

1. internal, potensi ancaman yang ditimbulkan berasal dari dalam mencakup karyawan perusahaan, konsultan, pegawai temporer, kontraktor, mitra bisnis perusahaan. Ancaman internal tingkat risikonya relatif lebih tinggi dibandingkan dengan ancaman yang berasal dari eksternal dikarenakan pengetahuan ancaman internal terhadap sistem diketahui lebih mendalam;
2. eksternal, ancaman eksternal misalnya perusahaan lain yang memiliki produk yang sama dengan produk perusahaan atau disebut juga pesaing usaha. Tingkat keberhasilannya akan lebih tinggi jika bekerja sama dengan pihak internal.

Berdasarkan sifatnya ancaman terhadap teknologi informasi terbagi menjadi dua bagian sebagai berikut.

1. Ancaman aktif merupakan ancaman akibat adanya suatu tindak kejahatan yang dilakukan pada sistem. Beberapa contoh jenis ancaman aktif, antara lain:
   a. penipuan dan pencurian data, penipuan dan pencurian data dapat dilakukan dengan memanfaatkan beberapa celah keamanan sistem informasi organisasi untuk kepentingan pribadi. Ancaman ini dapat terjadi melalui internal maupun dari pihak luar akibat adanya kerentanan pada sistem;
   b. sabotase pegawai, ancaman ini biasa terjadi pada pegawai yang merasa tidak puas akibat pemecatan terhadap dirinya atau ada pegawai yang merasa tidak puas terhadap organisasi;
   c. serangan *hacker* jahat, serangan oleh pihak yang tidak bertanggung jawab untuk keuntungan pribadi dengan mengakses sistem secara ilegal.

2. Ancaman pasif merupakan ancaman akibat
   a. kegagalan sistem, ancaman ini meliputi kegagalan aliran listrik, kerusakan perangkat dan sebagainya dampak dari ancaman ini terjadinya *downtime* terhadap sistem;
   b. *human error* (kesalahan manusia dalam memproses sistem), contoh kesalahan *input* data, kesalahan konfigurasi sistem sehingga terjadinya kesalahan dalam pemrosesan data;
   c. bencana alam yang terjadi, seperti banjir, gempa sehingga menyebabkan menimbulkan *downtime* pada sistem.
3. Aspek ancaman keamanan sistem informasi, terdiri dari:
   a. *interruption* merupakan ancaman terhadap *availability*, yaitu data dan informasi yang berada dalam sistem komputer dibuang atau dirusak sehingga menjadi tidak ada atau tidak berguna. Contohnya, *hard disk* yang dirusak, memotong jalur komunikasi, *denial of service*;
   b. *interception*, pihak yang tidak berwenang berhasil mengakses aset atau informasi dengan cara menyadap data yang melalui jaringan publik atau menyalin data secara tidak sah;
   c. modifikasi, pihak yang tidak berwenang berhasil mengakses dan mengubah informasi. Contoh, mengubah isi dari *website* dengan pesan-pesan yang merugikan pemilik *website* (*defacing*);
   d. *fabrication* merupakan ancaman terhadap informasi yang dilakukan oleh orang yang tidak berwenang dengan cara menyisipkan objek palsu ke dalam sistem. Contohnya, memasukkan pesan-pesan palsu seperti *email* palsu ke dalam jaringan komputer.
4. Langkah-langkah yang dilakukan untuk mengurangi dampak dari risiko ancaman keamanan informasi tersebut, antara lain:
   a. ditumbuhkannya budaya sadar akan ancaman keamanan informasi, yaitu melalui edukasi yang berkesinambungan terkait keamanan informasi untuk mengurangi dampak yang ditimbulkan dari suatu ancaman/serangan;
   b. melakukan *hardening* (penguatan, *patch*) terhadap sistem yang dibangun maupun sistem operasi yang terpasang pada suatu sistem;
   c. menyediakan sistem kontrol terhadap akses dan otoritas perubahan sistem;
   d. melakukan manajemen konfigurasi, yaitu proses evaluasi untuk perubahan konfigurasi sistem dan sistem pencatatan terhadap pihak yang melakukan perubahan;
   e. menyediakan sistem *backup*, yaitu melakukan *backup* data maupun sistem secara periodik tergantung dari nilai perubahan data maupun sistem tersebut dan dipastikan untuk dilakukan uji coba efektivitas metode *backup* yang diterapkan dan disimpan di tempat yang aman;
   f. melakukan pemeliharaan terhadap sistem dan dilakukan oleh pihak yang memiliki hak akses dan kompeten.

B. *MALICIOUS SOFTWARE* (PERANGKAT LUNAK BERBAHAYA)

Malicious software atau *malware* adalah perangkat lunak yang dibuat untuk dapat memasuki dan terkadang merusak sistem komputer, jaringan, atau sistem secara ilegal tanpa diketahui oleh pemilik sistem. Pemasangan *malware* bertujuan untuk merusak atau mencuri data dari perangkat yang dimasuki.

Terdapat beberapa jenis *malware* sebagai berikut.

1. ***Virus*** merupakan program yang memiliki kemampuan untuk memanipulasi data, menyebarkan, mengubah, dan merusak suatu sistem aplikasi. Kemampuan lain dari virus adalah dapat mereplikasi dirinya sendiri dan menempelkan salinan dirinya pada program lain di suatu komputer. Mekanisme penyebaran dari *malware* ini dilakukan melalui perantara, misalnya pengguna menyalin file bervirus ke komputer yang lain melalui *flashdisk*.
2. ***Worm*** merupakan program yang memiliki kemampuan untuk menyebarkan dirinya melalui salinan dan secara mandiri menyebar melalui jaringan tanpa interaksi dengan pengguna.
3. ***Trojan*** *horse* merupakan program yang tidak terdeteksi, program ini dapat merusak sistem dan bertujuan untuk mendapatkan informasi dari sistem target secara diam-diam.
4. ***Adware*** merupakan sebuah *malware* yang memunculkan pesan-pesan iklan pada tampilan pengguna tanpa izin dan mengganggu saat terhubung ke internet. *Adware* dimasukkan secara diam-diam oleh pembuat program dengan kemampuan untuk mengunduh dan menampilkan materi iklan secara otomatis tanpa diketahui penggunanya.
5. ***Spyware*** merupakan aplikasi yang bisa membocorkan data atau informasi perilaku atau kebiasaan *user* komputer. Program tersebut bisa mengumpulkan berbagai informasi seputar *user* dan selanjutnya mengirimkan informasi tersebut ke lokasi yang telah ditentukan sebelumnya.
6. ***Bots*** merupakan *malware* mirip *worm* yang dapat menduplikatkan diri dan menyebarkan virus ke komputer. Namun, *bots* memerlukan perintah atau arahan dari si pembuat *bot* supaya bereaksi. Biasa dimanfaatkan untuk serangan DoS (*denial of service*), dan DDoS (*distributed denial of service*).
7. ***Ransomware*** merupakan jenis *malware* yang melakukan blokir data korban dengan cara mengenkripsi data/file sehingga pengguna tidak dapat mengakses data yang dimilikinya sampai pengguna bersedia membayar uang tebusan.
8. ***Backdoor*** disisipkan ke dalam kode sistem maupun suatu program secara diam-diam sehingga pembuat *backdoor* dapat memperoleh akses untuk masuk ke dalam sistem pengguna. *Malware* jenis ini memasuki sistem dengan memanfaatkan celah *backdoor* dari suatu perangkat yang sering diselipkan melalui *trojan* atau *worm*.

9. ***Scareware*** merupakan *malware* yang dirancang untuk memaksa pengguna melakukan tindakan tertentu karena takut. *Scareware* memalsukan jendela *pop-up* sehingga menyerupai jendela dialog sistem operasi. Menyampaikan pesan palsu yang menyatakan bahwa sistem berisiko dan jika pengguna menyetujuinya maka sistem miliknya akan terinfeksi *malware*.
10. ***Rootkit*** merupakan *malware* yang dirancang untuk mengubah sistem operasi dan kemudian membuat *backdoor*. Penyerang kemudian menggunakan *backdoor* tersebut untuk mengakses komputer dari jarak jauh. *Rootkit* melakukan modifikasi terhadap sistem forensik dan alat bantu pemantauan sehingga membuat *rootkit* sangat sulit dideteksi. Umumnya, sistem operasi yang terinfeksi *rootkit* harus dihapus dan diinstal ulang.

C. *PHISING*

Phising adalah suatu bentuk kejahatan dunia maya dengan menggunakan metode penipuan untuk mendapatkan informasi rinci terkait akun tertentu melalui cara yang tidak sah. Istilah *phising* berasal dari kata *fishing* dalam bahasa Inggris yang berarti memancing, dalam hal ini adalah memancing informasi dan kata sandi dari target.

Mekanisme *phising* dilakukan dengan cara target dihubungi melalui *email*, layanan sosmed (Whatsapp, Facebook dan sebagainya) oleh seseorang yang menyamar sebagai lembaga yang sah untuk memikat individu agar memberikan data sensitif seperti informasi yang dapat diidentifikasi secara pribadi, rincian informasi finansial, serta kata sandi. Umumnya pada *email* tersebut terdapat tautan yang mengarahkan ke halaman web palsu yang tampilannya dibuat sama seperti *website* yang asli untuk menjebak seseorang sehingga target memberikan informasi melalui *website* palsu tersebut. Informasi tersebut kemudian digunakan untuk mengakses akun-akun penting dan dapat mengakibatkan pencurian identitas dan kerugian finansial.

1. Jenis-Jenis *Phising*

Teknik *phising* terus berkembang sehingga terdapat beberapa jenis *phising* sebagai berikut.

a. ***Spear phising,*** praktik penipuan dengan cara mengirim *email* yang seolah-olah berasal dari pengirim yang dikenal atau dipercaya untuk membujuk individu yang ditargetkan agar bersedia untuk mengungkapkan informasi rahasia. Isi *email* tersebut biasanya berisi tautan yang mengarahkan penerima ke situs *web* palsu yang berisi *malware*. Upaya ini ditargetkan untuk mencuri informasi sensitif, seperti kredensial (*credential*) akun atau informasi keuangan dari korban tertentu. Meskipun sering dimaksudkan untuk mencuri data untuk tujuan jahat, penjahat *cyber* mungkin juga berniat untuk menginstal *malware* di komputer pengguna yang ditargetkan.

b. ***Deceptive phising,*** jenis penipuan ini dilakukan dengan cara mengirim *email* yang mengatasnamakan dari perusahaan/lembaga gadungan yang dikenal oleh target untuk meminta data-data pribadi. Biasanya, alamat *email* pengirim semacam ini meminta target untuk
   1) melakukan verifikasi informasi akun,
   2) masukkan kembali informasi, seperti *login* atau kata sandi,
   3) meminta target mengubah kata sandi,
   4) melakukan pembayaran.

   Setelah informasi ini dimasukkan, peretas akhirnya mendapatkan informasi dan dapat mengakses akun milik target. Kemudian memanfaatkan informasi sensitif tersebut untuk mendapatkan keuntungan.

c. ***Smishing*** merupakan jenis *phising* yang melibatkan pesan teks melalui SMS. Biasanya pelaku kejahatan meminta korban untuk menelepon nomor yang tertera, membalas pesan dengan memberikan informasi yang diperlukan. Contohnya pengumuman hasil undian atau hadiah yang berasal dari perusahaan besar dan mengatasnamakan diri mereka bagian dari perusahaan tersebut.

d. ***Whale phising*** merupakan teknik *spear phising* yang secara khusus ditujukan untuk individu yang kaya, berkuasa, atau terkemuka yang dianggap sebagai *big fish* atau *whale* (ikan paus).

2. Ciri-Ciri *Phising*

Beberapa aktivitas *phising* umumnya memiliki ciri-ciri berikut.

a. Menggunakan sapaan yang umum (*generic greeting*), *email phising* selalu mengirimkan *email* ke sejumlah besar alamat *email*. Untuk menghemat waktu, peretas menggunakan nama umum, seperti *dear user*, *dear client*, *dear paypal*, sahabat mandiri dan sebagainya.

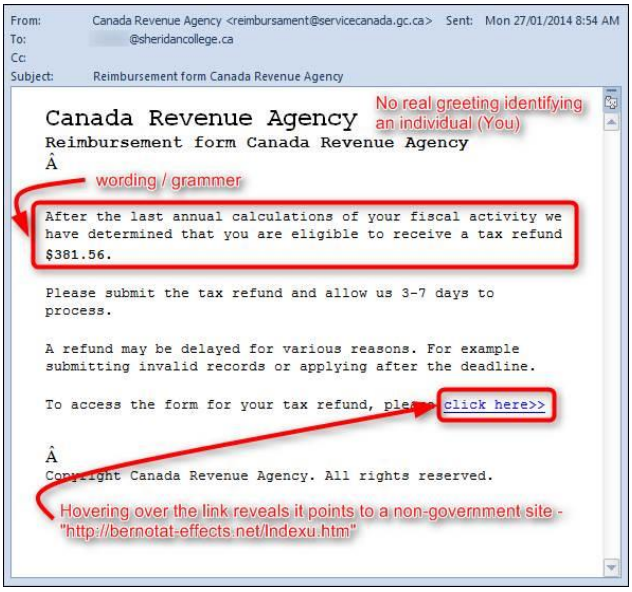
   Contoh terlihat pada Gambar 1.3 menggunakan sapaan umum *dear client*.

b. Alamat pengirim tidak sesuai, pengirim menggunakan alamat *email* yang tidak sama dengan alamat resmi nama *domain* perusahaan pengirim. Contoh pada Gambar 1.3 terlihat alamat *email* pengirim memiliki nama *domain* yang berbeda (amazoncanada.ca) dengan nama *domain* dari perusahaan asli (amazon.com).

Sumber: it.sheridancollege.ca/

Gambar 1.3
Contoh *Email Phising*

Tautan alamat URL singkat atau mengarah ke alamat yang tidak sesuai dengan alamat URL asli. Serangan *phishing* akan mengundang korban untuk mengklik ke URL yang terlihat resmi seperti pada Gambar 1.3. atau tautan alamat URL yang singkat contohnya "*click here*" seperti pada Gambar 1.4.

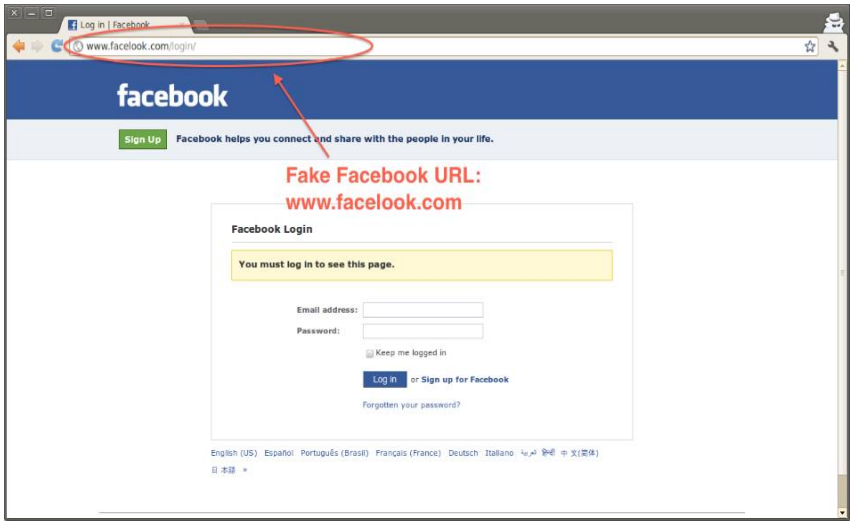


Sumber: it.sheridancollege.ca/

Gambar 1.4
Contoh Email *Phising*

c. Tampilan *website* yang sangat mirip dengan tampilan rujukannya.

d. Alamat *website typo*, untuk mengelabui korban, pelaku menggunakan nama domain dari *website* palsu hampir mirip dengan *website* aslinya contoh www.facebook.com dibuat dengan domain www.facelook.com.



Gambar 1.5
Contoh *Website Phising*

e. *Website* yang digunakan oleh pelaku, tidak menggunakan protokol HTTPS. Agar dapat memberikan keamanan pada pengguna, umumnya situs-situs besar atau kredibel menggunakan SSL (*Secure Socket Layer*) untuk *website*-nya sehingga *website* diakses menggunakan HTTPS, seperti yang dapat dilihat pada bagian *address bar*. Anda bisa melihat di bagian *address bar*.

3. Cara Menghindari *Phising*

Untuk menghindari *phising*, terdapat beberapa hal yang dapat dilakukan, antara lain:

a. mengetahui secara jelas identitas pengirim *email*,
b. teliti dan hati-hati dalam menerima *email*,
c. jangan meng-klik sembarangan,
d. memastikan *website* yang diakses merupakan *website* asli dan aman,
e. menggunakan *password* yang sulit dikenali orang,
f. *install* dan *update* antivirus.

D. *CYBERBULLYING*

Internet memberikan ruang untuk siapa saja untuk dapat saling berkomunikasi tanpa bertatap muka, serta dapat saling bertukar informasi dalam waktu yang sama

meskipun terpisah oleh jarak. Ruang *virtual* menawarkan kebebasan berpendapat yang dapat berdampak positif atau pun negatif. Salah satu dampak negatif yang ditimbulkan adalah memungkinkannya seseorang untuk membuat pernyataan, pendapat, atau tindakan yang menyakiti orang lain.

Cyberbullying merupakan suatu kondisi ketika teknologi informasi digunakan untuk mengirimkan pesan atau gambar yang ditujukan untuk mengintimidasi, menyakiti hati (secara psikologis) atau mempermalukan orang lain.

Definisi lain yang terkait dengan *cyberbullying*, antara lain:

1. menurut Willard, *cyberbullying* adalah perlakuan kejam yang dilakukan dengan sengaja kepada orang lain dengan mengirimkan atau mengedarkan bahan yang berbahaya atau terlibat dalam bentuk-bentuk agresi sosial menggunakan internet atau teknologi digital lainnya,
2. menurut Bauman, *cyberbullying* adalah penggunaan dari teknologi komunikasi modern yang ditujukan untuk mempermalukan, menghina, mempermainkan atau mengintimidasi individu untuk menguasai dan mengatur individu tersebut.

Menurut Willard, *cyberbullying* dapat muncul dalam berbagai bentuk sebagai berikut.

1. ***Impersonation*** merupakan perilaku berpura-pura menjadi orang lain dan mengirimkan pesan-pesan atau status yang tidak baik.
2. ***Denigration*** merupakan perilaku menyebarkan keburukan seseorang di internet dengan maksud merusak reputasi atau nama baik seseorang.
3. ***Flaming*** merupakan perilaku yang berupa mengirim pesan teks dengan kata-kata kasar. Perilaku ini biasanya dilakukan dengan mengirimkan gambar-gambar yang bertujuan untuk menghina orang tertentu melalui grup *chat*.
4. ***Harassment*** merupakan bentuk lain dari *flaming* perilaku mengganggu dengan mengirim pesan menggunakan kata-kata yang tidak sopan melalui *email*, sms, pesan teks pada media sosial, yang ditujukan kepada seseorang secara terus-menerus. Umumnya *harassment* dilakukan dengan saling berbalas pesan atau bisa disebut perang teks.
5. ***Outing & Trickery***. *Trickery* merupakan perilaku membujuk seseorang agar memperoleh rahasia pribadi seseorang, kemudian menyebarkan rahasia tersebut. Perilaku menyebarkan rahasia pribadi orang lain dikenal dengan istilah *outing*.
6. ***Exclusion*** merupakan perilaku dengan sengaja dan kejam mengeluarkan seseorang dari grup *online*.
7. ***Cyberstalking*** merupakan perilaku berulang kali mengirimkan ancaman membahayakan atau pesan-pesan yang mengintimidasi dengan menggunakan komunikasi elektronik. *Cyberstalking* merupakan salah satu tindak kriminal yang paling sering terjadi di dunia maya. Menurut Begotti, *Cyberstalking* merupakan perilaku menyimpang yang menyerang wilayah privasi seseorang menggunakan media internet, seperti *email*, media sosial, dan komunikasi internet lainnya secara berulang dengan tujuan untuk mengendalikan atau mengontrol, mengintimidasi, mengancam, memaksa, dan mengganggu.

Salah satu tindakan *cyberstalking* yang pada saat ini sering terjadi dikenal dengan istilah *doxing* atau *doxxing* (berasal dari kata "*dox*", singkatan dari dokumen). Kegiatan ini merupakan suatu tindakan berbasis internet untuk meneliti dan menyebarluaskan informasi pribadi secara publik (termasuk data pribadi) terhadap seseorang individu atau organisasi. Metode ini digunakan untuk memperoleh informasi termasuk mencari basis data yang tersedia untuk umum dan situs sosial media, meretas, dan rekayasa sosial. Tindakan ini erat terkait dengan *vigilantisme* internet dan *hacktivisme*. Seperti kasus Eiger, Denny Siregar dan sebagainya.

Doxing dapat menimbulkan berbagai macam bahaya termasuk pelecehan, penghinaan di dunia maya, pungutan liar, paksaan, analisis bisnis, analisis risiko, membantu penegak hukum atau *vigilante* versi keadilan. *Vigilante* dapat berarti sebagai main hakim sendiri, di mana seseorang akan menegakkan hukum dengan caranya sendiri. Istilah ini berasal dari bahasa Latin "*Vigiles Urbani*" yang diberikan kepada penjaga malam di Romawi kuno yang bertugas memadamkan kebakaran dan menjaga keamanan.

Menurut Safaria, *cyberbullying* pada umumnya memiliki karakteristik sebagai berikut.

1. *Cyberbullying* yang dilakukan berulang-ulang.
2. Menyiksa secara psikologis.
3. *Cyberbullying* dilakukan dengan tujuan.
4. Terjadi di dunia maya.

Latihan

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

1) Sebutkan jenis-jenis *cyberbullying!*
2) Sebutkan jenis dan ciri-ciri *phising!*
3) Sebutkan jenis-jenis *malware!*
4) Sebutkan perbedaan antara *virus* dan *worm!*

Petunjuk Jawaban Latihan

1) Jenis-jenis *cyberbullying* sebagai berikut.
   a) *Impersonation* merupakan perilaku berpura-pura menjadi orang lain dan mengirimkan pesan-pesan atau status yang tidak baik.
   b) *Denigration* merupakan perilaku menyebarkan keburukan seseorang di internet dengan maksud merusak reputasi atau nama baik seseorang.

c) *Flaming* merupakan perilaku yang berupa mengirim pesan teks dengan kata-kata kasar.

d) *Harassment* merupakan bentuk lain dari *flaming* perilaku mengganggu dengan mengirim pesan menggunakan kata-kata yang tidak sopan melalui *email*, sms, pesan teks pada media sosial, yang ditujukan kepada seseorang secara terus-menerus.

e) *Outing & Trickery*. *Trickery* merupakan perilaku membujuk seseorang agar memperoleh rahasia pribadi seseorang, kemudian menyebarkan rahasia tersebut, perilaku menyebarkan rahasia pribadi orang lain dikenal dengan istilah *outing*.

2) Jenis dan ciri-ciri *phising*.

Jenis-jenis *phising* sebagai berikut.

a) *Spear phising*, praktik penipuan dengan cara mengirim *email* yang seolah-olah berasal dari pengirim yang dikenal atau terpercaya untuk membujuk individu yang ditargetkan mau mengungkapkan informasi rahasia.

b) *Deceptive phising*, jenis penipuan ini dilakukan dengan cara mengirim *email* yang mengatasnamakan dari perusahaan/lembaga gadungan yang dikenal oleh target untuk meminta data-data pribadi.

c) *Smishing* merupakan jenis *phising* yang melibatkan pesan teks melalui SMS.

d) *Whale phising* merupakan teknik *spear phising* yang secara khusus ditujukan untuk individu yang kaya, berkuasa, atau terkemuka yang dianggap sebagai *big fish* atau *whale* (ikan paus).

Ciri-ciri *phising* sebagai berikut.

a) Menggunakan sapaan yang umum (*generic greeting*), *email phising* selalu mengirimkan *email* ke sejumlah besar alamat *email*.

b) Alamat pengirim tidak sesuai, pengirim menggunakan alamat *email* yang tidak sama dengan alamat resmi nama domain perusahaan pengirim.

c) Tautan alamat URL singkat atau mengarah ke alamat yang tidak sesuai dengan alamat URL asli.

d) Tampilan *website* yang sangat mirip dengan tampilan rujukannya.

e) Alamat *website typo*, untuk mengelabui korban, pelaku menggunakan nama domain dari *website* palsu hampir mirip dengan *website* aslinya contoh www.facebook.com dibuat dengan domain www.facelook.com.

f) *Website* tidak menggunakan protokol HTTPS, untuk memberikan keamanan pada pengguna umumnya situs-situs besar atau kredibel menggunakan SSL untuk *website*-nya.

3) Jenis-jenis *malware* sebagai berikut.
   a) Virus merupakan program yang memiliki kemampuan untuk memanipulasi data, menyebarkan, mengubah, dan merusak suatu sistem aplikasi. Kemampuan lain dari virus adalah dapat mereplikasi dirinya sendiri dan menempelkan salinan dirinya pada program lain di suatu komputer. Mekanisme penyebaran dari *malware* ini dilakukan melalui perantara, misalnya pengguna menyalin file bervirus ke komputer yang lain melalui *flashdisk*.
   b) *Worm* merupakan program yang memiliki kemampuan untuk menyebarkan dirinya melalui salinan dan secara mandiri menyebar melalui jaringan tanpa interaksi dengan pengguna.
   c) *Trojan horse* merupakan program yang tidak terdeteksi, program ini dapat merusak sistem dan bertujuan untuk mendapatkan informasi dari sistem target secara diam-diam.
   d) *Adware* merupakan sebuah *malware* yang memunculkan pesan-pesan iklan pada tampilan pengguna tanpa izin dan mengganggu saat terhubung ke internet.
   e) *Spyware* merupakan aplikasi yang bisa membocorkan data atau informasi perilaku atau kebiasaan *user* komputer.
   f) *Bots* merupakan *malware* mirip *worm* yang dapat menduplikatkan diri dan menyebarkan virus ke komputer. Namun, *bots* memerlukan perintah atau arahan dari si pembuat *bots* supaya bereaksi.
   g) *Ransomware* merupakan jenis *malware* yang melakukan blokir data korban dengan cara mengenkripsi sehingga pengguna tidak dapat mengakses data yang dimilikinya sampai pengguna bersedia membayar uang tebusan.
   h) *Backdoor* disisipkan ke dalam kode sistem maupun sebuah program secara diam-diam.
   i) *Scareware* merupakan *malware* yang dirancang untuk memaksa pengguna melakukan tindakan tertentu karena takut.
   j) *Rootkit* merupakan *malware* ini dirancang untuk mengubah sistem operasi untuk membuat *backdoor*.

4) Perbedaan antara *virus* dan *worm*.
   Petunjuk: perhatikan kembali jawaban No. 3.

Rangkuman

Ancaman keamanan informasi merupakan aksi yang terjadi dari dalam atau luar sistem yang dapat mengganggu keseimbangan sistem informasi dapat berasal dari individu, organisasi, mekanisme, atau peristiwa yang memiliki potensi untuk membahayakan sumber daya informasi. Ancaman dapat dikategorisasi berdasarkan sumber ancaman, sifat, dan aspek ancaman.

Terdapat banyak bentuk ancaman pada *cyberspace* sebagai berikut.

1. *Malicious software* atau *malware* adalah perangkat lunak yang dibuat untuk dapat memasuki dan terkadang merusak sistem komputer, jaringan, atau sistem secara ilegal tanpa diketahui oleh pemilik sistem. Terdapat beberapa jenis *malware*, antara lain: *virus*, *Trojan*, *rootkit*, *worm*, *spyware*, *adware*, dan sebagainya.
2. *Phising* adalah suatu bentuk kejahatan dunia maya dengan menggunakan metode penipuan untuk mendapatkan informasi rinci terkait akun tertentu melalui cara yang tidak sah.
3. *Cyberbullying* merupakan suatu kondisi ketika teknologi informasi digunakan untuk mengirimkan pesan atau gambar yang ditujukan untuk mengintimidasi atau mempermalukan orang lain.

Tes Formatif 2

Pilihlah satu jawaban yang paling tepat!

1) Yang dimaksud dengan ancaman adalah ....
   A. proses untuk mengidentifikasi dan mencegah pengguna yang tidak sah dari suatu jaringan komputer
   B. potensi *output* yang tidak diharapkan dari suatu pelanggaran
   C. aksi yang terjadi dari dalam atau luar sistem yang dapat mengganggu keseimbangan sistem informasi
   D. akuisisi, pengungkapan, atau penggunaan informasi dan data yang sah

2) *Denial of service* merupakan ancaman terhadap ketersediaan sehingga DoS masuk ke dalam aspek ancaman ….
   A. *interruption*
   B. *interception*
   C. *modification*
   D. *fabrication*

3) Berikut ini merupakan langkah-langkah yang dilakukan untuk mengurangi dampak dari risiko ancaman keamanan informasi, *kecuali* ….
   A. melakukan pemeliharaan pada saat sistem sedang dibangun
   B. melakukan manajemen konfigurasi

C. melakukan *hardening* (penguatan, *patch*) terhadap sistem
D. menyediakan sistem *backup*

4) Program yang menyebabkan kerusakan sistem ketika dijalankan disebut ….
A. *denial of service*
B. *phising*
C. *packet sniffer*
D. *malicious code*

5) Orang yang tidak memiliki otorisasi dapat mengakses dan juga mengubah, merusak sumber daya informasi. Contohnya mengubah isi pesan atau mengacak program. Ini merupakan ancaman yang disebut ….
A. *interruption*
B. *interception*
C. *modification*
D. *fabrication*

6) *Malware* yang menyerang dengan cara mengakses dari jaringan dan mengambil banyak data serta dapat mengatur konfigurasi komputer tanpa diketahui adalah ….
A. *virus*
B. *worm*
C. *backdoor*
D. *adware*

7) Perhatikan gambar berikut.


TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

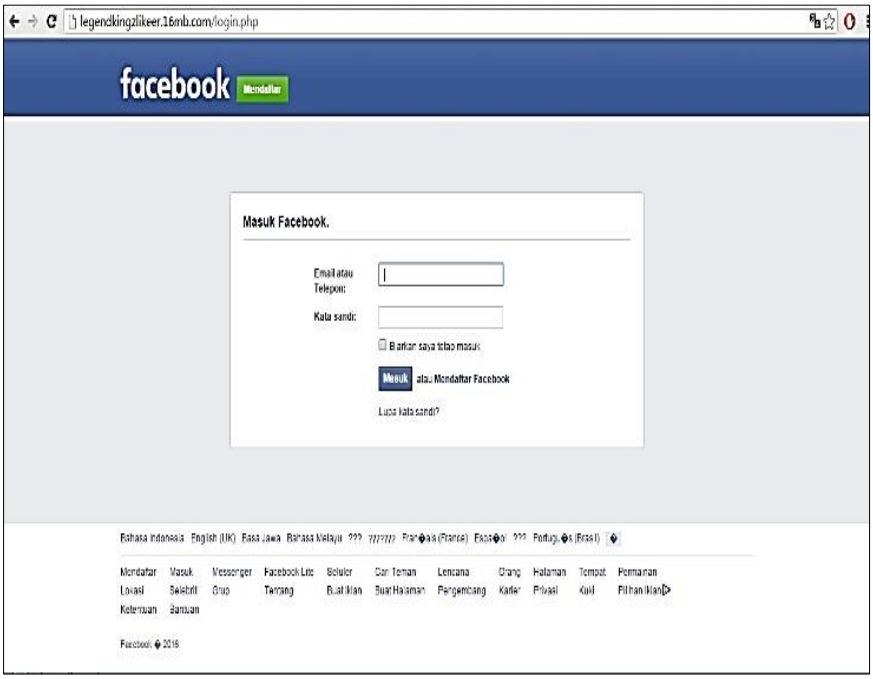
Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Email di atas termasuk dalam kategori *email phising* karena ….

A. menggunakan *generic greeting*
B. tautan ke alamat tertentu menggunakan http
C. pengirim mencoba menipu penerima agar mengungkapkan informasi rahasia dengan melakukan konfirmasi ke halaman web tertentu
D. jawaban A, B, dan C benar

8) Perhatikan gambar berikut.



Web di atas termasuk dalam kategori web *phising* karena ….

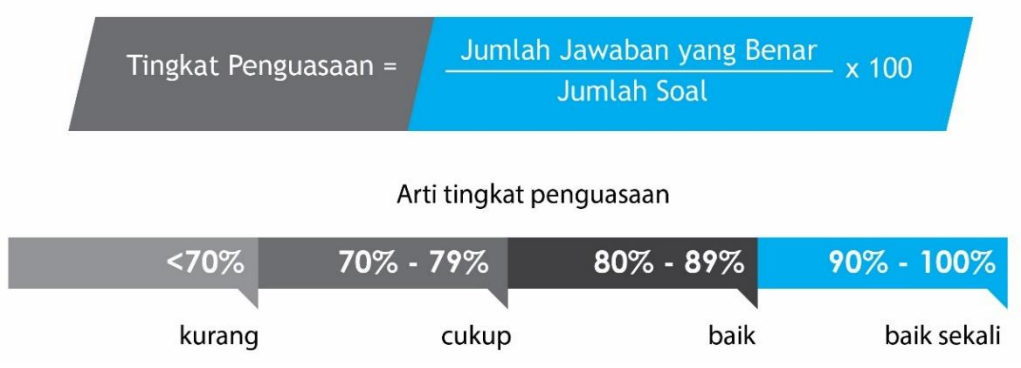
A. Facebook tidak menggunakan bahasa Indonesia
B. Facebook tidak pernah meminta alamat *email*
C. alamat *website* tidak sesuai
D. jawaban A, B, dan C salah

9) Perilaku mengganggu dengan mengirim pesan menggunakan kata-kata yang tidak sopan melalui media sosial yang ditujukan kepada seseorang secara terus-menerus disebut ….

A. *denigration*
B. *harassment*
C. *trickery*
D. *exclusion*

10) Yang dimaksud dengan *cyberstalk* adalah perilaku ....
   A. berulang kali mengirimkan ancaman membahayakan atau pesan-pesan yang mengintimidasi dengan menggunakan komunikasi elektronik
   B. membujuk seseorang agar memperoleh rahasia pribadi seseorang
   C. menyebarkan rahasia pribadi orang lain
   D. dengan sengaja dan kejam mengeluarkan seseorang dari grup *online*

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 2 yang terdapat di bagian akhir modul ini. Hitunglah jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 2.



Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan modul selanjutnya. **Bagus!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 2, terutama bagian yang belum dikuasai.

Kunci Jawaban Tes Formatif

Tes Formatif 1

1) B
2) B
3) C
4) D
5) A
6) C
7) D
8) B
9) C
10) D

Tes Formatif 2

1) C
2) A
3) A
4) D
5) C
6) C
7) D
8) C
9) B
10) A

Glosarium

Ancaman : aksi yang terjadi dari dalam atau luar sistem yang dapat mengganggu keseimbangan sistem informasi.

Address bar : suatu kolom teks yang berada di bagian atas *browser* halaman *website*, yang berfungsi untuk menuliskan alamat halaman *website* yang dituju.

Backup : menyalin data atau sistem ke dalam suatu tempat penyimpanan baik *online* maupun *offline*.

Carding : berbelanja menggunakan nomor dan identitas kartu kredit orang lain, yang diperoleh secara ilegal, biasanya dengan mencuri data di internet.

Cracker : seseorang yang mengakses sistem milik orang lain secara ilegal dan cenderung bersifat destruktif.

Cyber : sesuatu yang berhubungan dengan internet atau dunia maya.

Cyberbullying : suatu kondisi ketika teknologi informasi digunakan untuk mengirimkan pesan atau gambar yang ditujukan untuk mengintimidasi atau mempermalukan orang lain.

Cybercrime : aktivitas kejahatan dengan menggunakan teknologi dan jaringan komputer sebagai alat, sasaran maupun tempat terjadinya kejahatan.

Cyber security : bagian dari keamanan informasi yang melindungi sistem yang terhubung ke internet, termasuk perangkat keras, perangkat lunak, program, dan data dari potensi serangan *cyber*.

Cyberspace : ruang siber, merupakan hasil integrasi dari media elektronik dan peralatan teknologi jaringan komunikasi data yang menghubungkan peralatan komunikasi yang tersebar di seluruh penjuru dunia.

Cyberstalking : penggunaan internet atau sarana elektronik lainnya untuk menguntit atau melecehkan individu, kelompok, atau organisasi.

Cyber trespass : penggunaan teknologi komputer untuk meningkatkan akses pada sistem komputer suatu organisasi atau individu dan *website* yang dilindungi dengan *password*.

Deface website : tindakan yang dilarang karena melakukan perubahan terhadap halaman *website* perorangan atau instansi, dengan tujuan yang merugikan pemilik *website* tersebut.

Downtime : kondisi sistem tidak dapat beroperasi total atau mati.

Doxing : suatu tindakan berbasis internet untuk meneliti dan menyebarluaskan informasi pribadi secara publik (termasuk data pribadi) terhadap seseorang individu atau organisasi.

Gelombang elektromagnetik : suatu gelombang yang dapat memancar tanpa media rambat, yang dapat digunakan untuk memancarkan sinyal.

Hacker : personil yang melakukan analisis dengan mempelajari secara mendalam tentang suatu sistem.

Hardening : upaya untuk melakukan perbaikan terhadap *bug* atau kelemahan yang dimiliki oleh suatu sistem. Bentuknya dengan melakukan instalasi berupa *patch*, *hotfix* atau *service pack* untuk memperbaiki bug atau kelemahan suatu sistem.

Host : komputer atau perangkat lain yang terhubung ke jaringan komputer.

Kerentanan : kelemahan dalam prosedur keamanan sistem, desain, implementasi, atau kontrol internal yang dapat dilakukan (dipicu secara tidak sengaja atau dieksploitasi secara sengaja) dan mengakibatkan pelanggaran keamanan atau pelanggaran kebijakan keamanan sistem.

Kabel *fiber optic* : suatu kabel jaringan yang terbuat dari bahan plastik atau kaca.

Kabel *coaxial* : suatu kabel jaringan yang dibungkus dengan bahan metal.

Online : menjelaskan bahwa sistem atau perangkat yang digunakan pengguna sedang berada pada suatu koneksi dengan internet.

Port : mekanisme yang mengizinkan suatu *host* untuk mendukung beberapa sesi koneksi dengan *host* lainnya dan program di dalam jaringan atau rangkaian nomor yang dimiliki oleh komputer sebagai penghubung ke komputer lain melalui jaringan tertentu.

Port scanning : aktivitas yang dilakukan untuk memeriksa satu per satu status *port* TCP dan UDP pada suatu *host* (komputer, perangkat teknologi informasi).

URL	:	*Uniform Resource Locator*, istilah lain untuk menyebut alamat *website*.
Sosmed	:	media sosial yang berfungsi untuk melakukan komunikasi sosial melalui media maya atau internet.
Update	:	kondisi setelah dilakukannya suatu perubahan pada data tertentu. Perubahan tersebut dapat berupa edit, hapus, simpan dan sebagainya.
Vigilante	:	dapat berarti sebagai main hakim sendiri, di mana seseorang akan menegakkan hukum dengan caranya sendiri.

Daftar Pustaka

Batelli, F., & Bruchi, D. (2008). *Network security: From risk analysis to protection strategies*. ISACOM Stampa: PrintArt.

Bauman, S. (2008). The role of elementary school caunselors in redusing school bullying. *The Elementary School Journal*.

Begotti, T., & Maran, D. A. (2019). *Characteristics of cyberstalking behavior, consequences, and coping strategies* : *A cross- sectional study in a sample of italian university students*.

Dyson, E., Gilder, G., Keyworth, G., & Toffler, A. (1994). *Cyberspace and the american dream: A magna carta for the knowledge age, future insight*.

S. Gary, G. Alice, & F. Alexis. (2002). *Risk management guide for information technology systems*. National Institute of Standards and Technology.

Statowski, M. (2007). The principles of network security design. *ISSA Journal*.

Willard, N. (2005). *Cyberbullying and cyberthreats*. Washington: U.S. Department of Education.