

SIBERPEDIA

PANDUAN PINTAR KEAMANAN SIBER



SIBERPEDIA PANDUAN PINTAR KEAMANAN SIBER

Penulis:

Azrina Darmayani

Editor:

Muhammad Salahudin

Donny B.U



Kata Pengantar

Ancaman keamanan siber merupakan sebuah bentuk ancaman baru di tengah arus globalisasi dan interkonektivitas yang semakin tinggi antarindividu maupun entitas global. Dengan natur dunia siber yang sangat luas, keamanan siber bukan hanya menjadi masalah bagi pemerintah ataupun pembuat kebijakan, namun juga individu pengguna. Dibutuhkan sumber daya manusia yang mumpuni dalam mengatasi tantangan-tantangan dari keamanan siber tersebut. Pengetahuan terkait keamanan siber merupakan sebuah hal yang krusial dimiliki oleh para pengguna teknologi, tidak hanya pada skala besar seperti organisasi, namun juga pengguna perseorangan.

Meskipun begitu, tingkat literasi dan kesadaran masyarakat Indonesia terkait keamanan siber masih sangat rendah. Dengan semakin tingginya angka kejahatan siber di Indonesia, hal ini tentunya menjadi sebuah permasalahan yang sangat serius. Selain peningkatan jumlah tenaga ahli pada bidang Teknologi Informasi, Indonesia juga membutuhkan masyarakat yang dapat menerapkan perilaku bijaksana dalam beraktivitas di dunia siber. Untuk itu, diperlukan sosialisasi dan juga edukasi kepada masyarakat untuk memiliki kesadaran dan literasi yang memadai terkait keamanan siber.

Buku ini mengulas mengenai pentingnya keamanan siber di Indonesia, ruang lingkup dari keamanan siber, dan bagaimana entitas maupun individu dapat meningkatkan keamanannya di ranah siber. Penjelasan dalam buku ini disampaikan dalam bahasa yang sederhana dan mudah dipahami oleh para pembaca awam dengan harapan pembaca dapat dengan mudah mengaplikasikannya dalam kehidupan sehari-hari dan mendorong terciptanya budaya keamanan siber yang kuat di Indonesia.



01

Asal Mula Pentingnya Keamanan Siber

Internet dan Gaya Hidup Baru di Indonesia	08
Peningkatan Kejahatan Siber	12

02

Beberapa Hal yang Harus Dipahami Terkait Keamanan Siber

Keamanan Siber di Era Digital Baru	23
Ruang Lingkup Keamanan Siber	25
Keamanan Siber di Internet	48
Keamanan Siber di Bidang Perbankan	58
Keamanan Siber di Bidang E-Commerce	62
Keamanan Siber di Bidang Fintech	67
Keamanan Siber di Sosial Media	69





Sumber : Mojix.com, 2017

03 *Cara Pintar untuk Aman di Dunia Siber*

Cara Pintar untuk Pengguna	91
----------------------------	----

Cara Pintar untuk Perangkat	100
-----------------------------	-----

Cara Pintar untuk Akses	106
-------------------------	-----

BAB I

Asal Mula Pentingnya Keamanan Siber

“It is only when they go wrong that machines remind you how powerful they are” – Clive James

Semakin teknologi berkembang, semakin beragam pula kesempatan dan tantangan yang muncul bersamaan dengannya. Berselancar di internet mungkin masih menjadi hal yang seringkali dianggap sangat jauh dari resiko kejahatan karena kita belum pernah menjadi korbannya. Tetapi jika sudah berhadapan sendiri dengan masalah yang ditimbulkan, kita akan mulai menyadari betapa kuatnya mesin dan sistem komputer saat ini.

Melalui pembahasan kali ini, penulis akan mengajak untuk berpikir sedikit lebih berbeda dan menjadi lebih bijak dalam melakukan apapun di internet atau ruang siber. Hal-hal kecil yang akan membuat kita memiliki pandangan lebih jauh dalam menggunakan laptop, ponsel pintar, dan berbagai media yang digunakan untuk terkoneksi dengan internet.

Saat membaca tulisan ini, kita dapat melihat keseluruhan proses menggunakan komputer, mulai dari riset, mengetik, dan mencetak. Semua yang ada disini, sejatinya hanya terkonversi sebagai bilangan

biner 0 dan 1. Dalam kenyataannya, hal ini juga terjadi di hidup kita saat ini. Dimana kehidupan dan keberadaan seseorang di ruang siber terkodefikasi dan terbentuk sebagai data.

Oleh karena itu, untuk mengikuti perkembangan zaman dan teknologi yang semakin canggih, perlu adanya pemahaman bagaimana sistem operasi dan cara penggunaan yang tepat guna agar internet dan dunia siber dapat kita kendalikan, bukan justru mengendalikan kita.

Perkembangan internet di Indonesia saat ini terjadi begitu cepat. Hal ini memberi pengaruh besar terhadap terciptanya gaya hidup baru. Gaya hidup baru yang membuat kita menjadi hidup jauh lebih dekat dengan internet. Dimana hampir sebagian besar lini kehidupan kita seakan-akan terus bersentuhan dengan produk teknologi ini. Namun di balik kemajuannya, ada beberapa fenomena yang terjadi seiring dengan perkembangan internet. Salah satunya adalah kejahatan di internet atau kejahatan siber. Kejahatan siber sendiri dapat memberikan kerugian baik secara materil dan non materil yang berpotensi terjadi bahkan dalam aktivitas sehari-hari. Oleh karena itu, perlu adanya upaya untuk mengantisipasi kemungkinan terjadinya serangan ini dengan memahami dan mengenal lebih dekat keamanan siber.

INTERNET DAN GAYA HIDUP BARU DI INDONESIA

Globalisasi memberikan dampak yang sangat besar bagi perkembangan dunia teknologi, informasi, dan komunikasi di Indonesia. Kemajuan ini juga memberikan perubahan terhadap gaya hidup bagi masyarakat Indonesia yang menjadi cenderung lebih dekat dengan teknologi. Berdasarkan hasil survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) dalam rilis yang berjudul “Penetrasi dan Perilaku Pengguna Internet Indonesia 2017” pengguna internet di Indonesia telah mencapai angka 143,26 juta jiwa atau setara dengan 54,7% total populasi dari republik ini (Buletin APJII Edisi 22, Maret 2018). Diperkuat dengan data

dari Google Consumer Barometer bahwa 79% dari pengguna internet di Indonesia menggunakan internet dalam frekuensi harian.

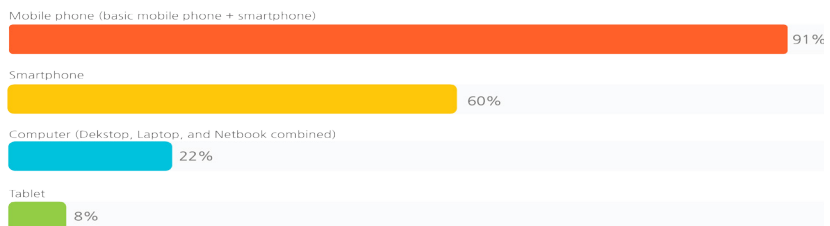
How often do people go online (for personal Internet usage)?



Sumber : Google Consumer Barometer 2018

Tidak bisa dipungkiri bahwa internet menjadi bagian yang tidak dapat dipisahkan dari kehidupan kita saat ini. Kondisi ini juga menjadi peluang baru bagi para pelaku bisnis. Pasar yang sangat besar mendorong pengusaha untuk terus berinovasi termasuk dalam memanfaatkan trend yang tengah berkembang, memahami kebutuhan dasar manusia, dan menjahit keduanya dalam sebuah produk berbasis internet. Kemunculan berbagai macam perusahaan berbasis daring adalah bukti nyata dari hal ini. Berbagai perusahaan penyediaan transportasi, makanan, barang kebutuhan rumah tangga, hingga pendidikan tambahan yang lahir di internet menciptakan sebuah pola gaya hidup baru bagi masyarakat Indonesia yang kini lebih menggantungkan kehidupannya terhadap internet.

Which devices do people use?



Sumber : Google Consumer Brometer 2018

Dalam menggunakan internet, sebagian besar masyarakat Indonesia berfokus pada penggunaan *mobile phone* dan *smart phone*. App Annie, sebuah perusahaan analisis dan riset pasar aplikasi *mobile* mengungkapkan sebuah fakta menarik terkait perkembangan pasar aplikasi *mobile* di Indonesia. Pada laporannya yang berjudul “2017 Retrospective: A Monumental Year for the App Economy”, penduduk Indonesia tercatat sebagai salah satu negara yang paling aktif dalam menggunakan aplikasi *mobile*, bersaing dengan negara-negara seperti Cina, India, Brazil, dan Korea Selatan (Tech in Asia, 2018). Indonesia juga menjadi negara yang menduduki peringkat tertinggi dalam durasi konsumsi aplikasi *mobile* dengan rata-rata durasi 250 menit atau lebih dari empat jam dalam sehari tepat di bawah Cina.

Sebuah Refleksi

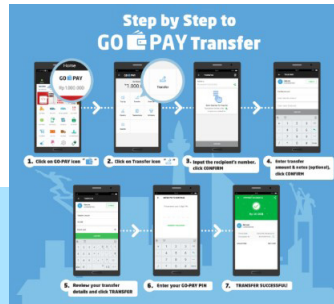
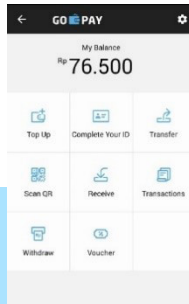
Sadar atau tidak, saat pertama mulai menggunakan berbagai aplikasi ada beberapa proses sakral yang rutin harus kita jalani seperti memasukkan data pribadi untuk proses registrasi.



Sesederhana memasukkan nama lengkap, alamat surat elektronik, tanggal lahir, hingga se-kompleks membagikan ketertarikan, hobi, tempat tinggal, latar belakang pendidikan dan pekerjaan, informasi tentang keluarga dan teman, sampai momen-momen penting dalam kehidupan.

Beranjak ke ritual selanjutnya yang sedang populer saat ini, kita juga seringkali melakukan transaksi internet yang mengintegrasikan rekening bank atau kantong uang online melalui *fintech* yang saat ini sedang populer di pasaran.

Kemunculan transaksi-transaksi melalui internet seperti *e-banking*, *e-commerce*, *e-trade*, *e-business*, *e-government*, *e-learning*, hingga *e-retailing* disatu sisi memberi kemudahan yang sangat praktis dan cenderung positif. Tetapi dampak positif ini tidak serta merta datang sendiri tanpa adanya dampak negatif. Dari berbagai aktivitas yang akrab dalam keseharian kita seperti yang telah dideskripsikan diatas, pernahkah kita menyadari bahwa semua aksi yang dilakukan di dunia digital akan terekam secara abadi? Dan semua data yang kita bagikan bisa saja disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab?



Oleh karena itu penting sekali untuk bisa mengejar kemajuan teknologi dengan kemampuan mengenai keamanan siber yang bisa diterapkan dalam kehidupan sehari-hari.

kehidupan yang akrab dalam keseharian kita seperti yang telah dideskripsikan diatas, pernahkah kita menyadari bahwa semua aksi yang dilakukan di dunia digital akan terekam secara abadi? Dan semua data yang kita bagikan bisa saja disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab?

Oleh karena itu penting sekali untuk bisa mengejar kemajuan teknologi dengan kemampuan mengenai keamanan siber yang bisa diterapkan dalam kehidupan sehari-hari.

Setiap aktivitas yang kita lakukan di internet dapat memperkuat identitas kita di ruang siber. Internet dengan segala kemajuannya, telah menciptakan dunia baru yang akrab dikenal dengan sebutan *cyber space* atau ruang siber. Ruang siber adalah sebuah dunia komunikasi berbasis komputer yang menawarkan realitas baru berbentuk virtual atau secara tidak langsung dan tidak nyata (Moh. Wildan, *Jurnal Masyarakat Telematika dan Informasi*, Vol. 5 No. 2, 2014). Ruang siber memungkinkan komunikasi antara sesama jaringan komputer yang terbentuk (ITU, 2017). Semakin tinggi intensitas seseorang bermain di dunia internet atau komputer, maka semakin terkoneksi sinyal informasi terkait orang tersebut. Hal ini berdampak pada semakin sempurna gambaran sosoknya di ruang siber. Bayangkan betapa banyak informasi yang bisa disimpulkan oleh pengamat di ruang siber dalam memahami identitas kita melalui berbagai aplikasi, layanan internet, dan sosial media yang kita miliki.

Fakta dimana penggunaan internet tidak dapat dipisahkan dari Indonesia membuktikan bahwa sebagian dari masyarakat kita telah hidup hampir seutuhnya dalam dunia digital. Mulai dari melakukan transaksi finansial, membeli peralatan rumah tangga, makanan, hingga pakaian, mencari hiburan, sampai memesan tiket untuk berpergian, semua dapat dilakukan dengan bantuan jemari dan koneksi internet. Kemajuan internet ini juga memiliki pengaruh yang sangat kuat terhadap jawaban dari pertanyaan “Pilih mana, ketinggalan dompet apa *smartphone*?”

Kemajuan internet dan kecanduan masyarakat terhadap teknologi ini patut diterima dengan bijaksana. Sebab perubahan ini bisa saja menjadi lahan basah bagi pihak-pihak yang ingin memanfaatkan kesempatan dari euphoria ini. Sebab perkembangan kemajuan internet juga merupakan sebuah perkembangan kemajuan bagi kejahatan di internet atau kejahatan siber.

PENINGKATAN KEJAHATAN SIBER

Sejalan dengan kemajuan teknologi yang semakin tidak ter-bendung pergerakannya. Diikuti dengan perubahan besar terhadap masyarakat dan gaya hidup baru di Indonesia. Gaya hidup yang serba



digital. Dimana segala aktivitas bisa berjalan jauh lebih mudah saat koneksi internet berada di genggaman tangan. Perubahan ini turut berpengaruh atas hilangnya batas ruang dan waktu di ruang siber. Sehingga menciptakan peluang untuk memanfaatkan berbagai informasi yang dapat diperoleh melalui internet untuk melakukan sebuah tindak kejahatan di dunia maya atau *cybercrime*.

Cyber crime atau kejahatan siber dapat diartikan sebagai sebagai perbuatan melawan hukum yang dilakukan dengan memakai komputer

sebagai sarana atau alat begitupun menjadikan komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Secara ringkas kejahatan siber didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi komputer yang canggih (Wisnubroto, 1999).

Indonesia sebagai salah satu negara dengan penduduk terpadat di dunia dan kemajuan teknologi internet yang sangat pesat, tidak dapat lepas dari fenomena kejahatan siber. Berdasarkan laporan *The Global Cybersecurity index 2017* yang dirilis oleh *The UN International Telecommunication Union (ITU)*, Indonesia termasuk dalam negara dengan keamanan siber yang lemah dan menjadi salah satu dari 10 negara yang seringkali terkena sasaran setiap saat. Catatan *Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII)* juga memperkuat fakta ini dengan menunjukkan data bahwa sejak Januari hingga Juli 2017, terdapat 177,3 juta serangan siber yang masuk ke Indonesia. Artinya dalam satu hari bisa terdapat 836.200 serangan siber yang umumnya serangan kejahatan ini dilancarkan dalam bentuk fraud dan malware (Kompas, 2017).

Kilas Balik

Di tahun 2017 lalu, Indonesia sempat dihebohkan dengan serangan siber *ransomware* (aplikasi perangkat yang dapat merusak sistem komputer dari jarak jauh) yang berjenis *WannaCry* (memanfaatkan kelemahan sistem pengamanan pada Sistem Operasi Windows yang telah ditambal Microsoft melalui *Security Update Patch*). Serangan *Ransomware WannaCry* yang sempat menyerang Indonesia di tahun 2017 ini sempat menggegerkan ranah berita Indonesia sebab berhasil menyerang setidaknya dua rumah sakit di Jakarta yaitu Dharmais dan Harapan Kita pada 12 Mei 2017, serangan ini menyebabkan data pasien dalam jaringan rumah sakit tidak bisa diakses. Pada 17 Mei 2017 Menkominfo mengklaim Indonesia sudah bebas virus *ransomware WannaCry* yang sebelumnya menginfeksi setidaknya 200 ribu komputer di seluruh dunia. (Techno Okezone, 31 Desember 2017). Mungkin kita juga termasuk dari sebagian orang yang meminimalisir penggunaan koneksi internet dari komputer melalui *Wi-Fi* dan LAN saat kehebohan ini terjadi.

Trend kejahatan siber di Indonesia cenderung meningkat dari tahun ke tahun, dengan tipe dan variasi serangan yang berbeda dari tahun sebelumnya. Walaupun masih terdapat tipe primadona yang masih saja bertahan dari tahun ke tahun. Kejahatan siber sendiri dapat terjadi karena beberapa faktor, yang pertama adalah adanya pelaku kejahatan seperti *cracker*, modus kejahatan, kesempatan untuk melakukan kejahatan, korban kejahatan, reaksi sosial atas kejahatan, serta hukum (Muhammad Danuri dan Suharnawi, 2017). Rata-rata yang menjadi pelaku kejahatan adalah mereka yang lebih menguasai teknologi siber dan internet serta menggunakan kemampuan tersebut untuk melakukan akses ilegal ke jaringan komputer yang secara legal bukan miliknya.

Kejahatan siber seringkali diidentikan dengan kehadiran *hacker* dan *cracker*. Himanen mengemukakan bahwa *hacker* adalah seseorang yang senang memprogram dan percaya bahwa berbagi informasi adalah hal yang sangat berharga, dan *hacker* adalah orang pintar yang ingin mengetahui lebih dalam terkait informasi-informasi ini. Sedangkan *cracker* adalah orang yang merusak sistem keamanan, *cracker* biasanya kemudian melakukan ‘pencurian’ dan tindakan anarki, begitu mereka mendapat akses. Sehingga muncul istilah *whitehat* dan *blackhat*. *Whitehat* adalah *hacker* yang lugu, dan *blackhat* adalah seperti yang disebutkan di atas sebagai *cracker*. Namun demikian, orang lebih senang menyebutkan *hacker* untuk *whitehat* dan *blackhat*, tanpa benar-benar tahu perbedaan makna antara keduanya (Dista Amalia Arifah, 2011).

Jika diklasifikasikan, kejahatan siber sendiri dapat terbagi kedalam dua tipe, yaitu *Insider Attack* dan *External Attack*. *Insider Attack*, seperti yang dapat di duga dari penamaannya, adalah sebuah serangan yang dilakukan oleh pihak-pihak yang memiliki otoritas terhadap akses sistem yang diserang. Biasanya serangan jenis ini dilakukan oleh karyawan atau pegawai yang tidak puas atau kecewa terhadap perusahaannya. Mereka yang memiliki akses yang legal terhadap jaringan komputer di

perusahaan atau institusinya. Sebaliknya dengan *External Attack*, jenis serangan ini murni dari pihak eksternal, bisa merupakan seseorang yang dibayar oleh pihak internal ataupun pihak yang benar-benar asing yang memiliki kepentingan tersendiri. *External Attack* biasanya memberikan kerugian baik secara finansial maupun reputasi, sebab peretas yang masuk ke dalam sistem seringkali mencuri informasi yang bersifat rahasia (Jeetendra Pande, 2017).

Sekilas Info

Pada tahun 2016, Wakil Direktur Tindak Pidana Ekonomi Khusus Bareskrim Polri, Agung Setya dalam seminar yang bertemakan “Kekuatan *Brand* dan Media Sosial di Tengah Evolusi Pasar pada Era Digital-Antisipasi *Digital Crime*” di Jakarta mengungkapkan bahwa 60% kejahatan di dunia siber yang terjadi di Indonesia, khususnya di sektor perbankan, dilakukan oleh pihak dalam (internal) atau pegawai bank itu sendiri. Kejahatan berjenis *Internal Attack* ini menurutnya terjadi karena ada 3 faktor utama yang dilakukan oleh para pegawai bank untuk melakukan kecurangan (*fraud*). Pertama, adanya tekanan untuk melakukan penyelewengan (*pressure*). Kedua, adanya kesempatan yang bisa dimanfaatkan (*opportunity*) dan terakhir, adanya pembenaran terhadap tindakan tersebut (*razionalization*).

(Warta Ekonomi, 2016)

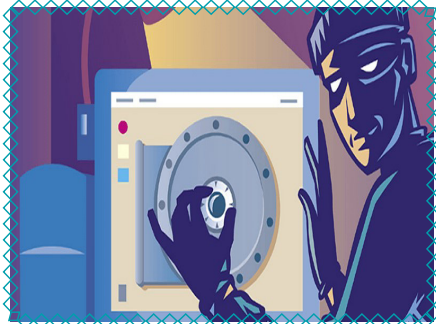
Jenis-jenis aktivitas dari kejahatan siber ini pun beragam. Mulai dari mencuri akses database pengguna kartu kredit, database akun bank, database informasi pelanggan, pembelian dengan kartu kredit palsu atau kartu kredit orang lain yang bukan merupakan hak kita (*carding*), sampai dengan sengaja mengacaukan sistem komputer yang ada (Dista Amalia Arifah, 2011). Berbagai jenis aktivitas tersebut menurut buku *Introduction to Cyber Security* karya Jeetendra Pande, dapat terjadi atas berbagai alasan, seperti uang, pembalasan dendam, pengakuan, anonimitas, dan spionase siber.



Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis utama komputer dan jaringan telekomunikasi ini dalam beberapa literatur dan prakteknya dikelompokkan dalam beberapa bentuk berdasarkan artikel NCB Interpol Indonesia yang berjudul “Cybercrime: Sebuah Fenomena di Dunia Maya (Ari Juliano Gema, 2013), antara lain:

1. Akses Tanpa Izin ke Sistem dan Layanan Komputer (*Unauthorized Access to Computer System and Service*)

Kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (*cracker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukan hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet atau intranet.



Sumber: Astaris 2018



2. Konten Ilegal (*Illegal Contents*)

Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Contohnya adalah pemuatan suatu berita bohong atau fitnah yang

akan menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah, dan sebagainya.



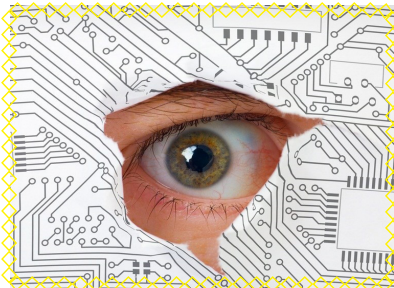
Sumber: Littleapplepost.com 2018

3. Pemalsuan Data (*Data Forgery*)

Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless* dokumen melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi “salah ketik” yang pada akhirnya akan menguntungkan pelaku.

4. Spionase Siber (*Cyber Espionage*)

Spionase siber adalah kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini



Sumber: Security Affairs 2018

biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang *computerized*.

5. Sabotase dan Pemerasan Siber (*Cyber Sabotage and Extortion*)

Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, virus komputer ataupun suatu program tertentu,

sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase tersebut, tentunya dengan bayaran tertentu. Kejahatan ini sering disebut sebagai *cyber-terrorism*.



Sumber: Pascarioty 2018

6. Pelanggaran terhadap Kekayaan Intelektual (*Offense against Intellectual Property*)

Kejahatan ini ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran



suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.



Sumber : Daily FT 2018

7. Pelanggaran Privasi (*Infringements of Privacy*)

Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara computerized, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

Melengkapi bentuk-bentuk kejahatan siber diatas, Jeetendra Pande dalam buku *Introduction to Cyber Security* mengemukakan jenis-jenis kejahatan siber dalam skema yang lebih luas dan rinci meliputi:

1. *cyber stalking*: mengikuti dan melecehkan seseorang di ruang siber untuk menjatuhkan popularitasnya
2. *child pornography*: memiliki atau menyebarkan foto dan video anak di bawah 18 tahun saat melakukan perilaku seksual
3. *forgery and counterfeiting*: memalsukan dokumen
4. *software piracy and crime related to IPRs*: pembajakan perangkat lunak dan kejahatan terkait hak kekayaan intelektual, seperti mengunduh lagu dan film illegal
5. *cyber terrorism*: menintimidasi dan memaksa pemerintah atau warga sipil untuk kepentingan soisial maupun politis
6. *Phishing*: upaya memperoleh informasi pribadi dan sensitif menggunakan perangkat elektronik
7. *computer vandalism*: upaya menghancurkan sumber daya komputer melalui kekuatan fisik atau jahat)
8. *computer hacking*: memodifikasi perangkat keras maupun lunak komputer secara illegal
9. membuat dan menyebarkan virus melalui internet
10. *Spamming*: mengirimkan pesan beruntut salam jangka waktu tertentu
11. *cross site scripting*: menyuntikkan kode jahat kedalam situs terpercaya untuk kepentingan pribadi
12. *online action fraud*: penipuan berbasis internet

13. *cyber squatting*: aksi mengambil alih domain tertentu yang merupakan *trademark* demi mendapatkan keuntungan dengan harga yang lebih tinggi
14. *logic bomb* :kode jahat yang dimasukkan kedalam perangkat lunak yang sah
15. *web jacking* : upaya *hacker* untuk mem-blok atau mengubah sebuah situs demi kepentingan ekonomi, sosial, maupun politik
16. *internet time thefts*: meretas nama dan nama pengguna seseorang untuk berselancar di internet dengan ditanggung pemilik identitas
17. *denial of service attack*: serangan yang dilakukan dengan menambahkan *traffic* untuk melumpuhkan sebuah jaringan
18. *salami attack* : kejahatan siber yang dimulai dari hal kecil hingga menyebar menjadi besar
19. *data drizzling*: praktik mengganti data sebelum masuk ke sistem komputer
20. *email spoofing*: proses mengganti pokok informasi dari sebuah surat elektronik agar sumber aslinya tidak diketahui

Berbagai macam bentuk kejahatan siber seperti yang telah dijelaskan diatas, berkembang seiring dengan kemajuan teknologi dan peningkatan penggunaan internet di Indonesia. Secara umum, perspektif perbandingan dari kejahatan siber dalam pasal-pasal UU ITE yang mengadopsi *European Union Convention on Cybercrime*, Budapest, 2001 sendiri pada prinsipnya terbagi kedalam dua kelompok besar, yaitu kejahatan yang menjadikan sistem komputer sebagai target dan kejahatan yang menggunakan sistem komputer sebagai alat. Dimana keduanya tidak hanya terjadi di ranah dan institusi besar saja tetapi juga dapat terjadi di ranah

kehidupan sehari-hari di dalam lingkup yang lebih kecil. Keberadaan internet dan dunia siber yang begitu dekat dengan kita, mengharuskan kita untuk bersikap lebih bijak dalam beraktivitas di dunia maya untuk memperkecil resiko menjadi korban dari tindak kejahatan siber. Salah satu solusinya adalah dengan mengenal lebih dekat penawar dari kejahatan siber dengan memahami kemandirian siber.

Sekilas Info



Gambar: Twitter CCIC Polri

Dengan perkembangan internet yang semakin maju di Indonesia, kecepatan siber secara alamiah akan ikut meningkat. Berdasarkan data yang diperoleh Okezone dari Direktorat Tindak Pidana Kejahatan Siber (Dit Tipidsiber) Bareskrim Polri di tahun 2017 dari bulan Januari-Oktober, jajaran Polisi Republik Indonesia (POLRI) telah menangani 1.763 kasus kejahatan siber, yang meliputi penipuan lelang secara *online*, pemalsuan cek, penipuan kartu kredit atau *carding*, *confidence fraud* (penipuan kepercayaan), penipuan identitas, dan pornografi anak. Dari total kasus tersebut, sampai Desember 2017, POLRI setidaknya telah dapat menyelesaikan 835 kasus kejahatan siber. (Putranegara Batubara, 2017)

Bentuk kejahatan siber diatas adalah contoh-contoh kasus kejahatan yang cenderung terjadi dalam ruang lingkup praktis yang erat dengan kehidupan kita sehari-hari, bukan perang siber antar negara, ataupun espinase, dan kejadian Estonia maupun Georgia. Kedekatan bentuk kejahatan siber dengan model seperti ini yang mengharuskna kita sebagai pengguna ruan siber untuk menjadi lebih bijak dalam hidup di dunia maya ini setidaknya untuk kepentingan kita sendiri.

BAB II

BEBERAPA HAL YANG HARUS DIPAHAMI TERKAIT KEAMANAN SIBER

Istilah keamanan siber mungkin masih tidak terlalu akrab di telinga sebagian orang. Tetapi di tengah kemajuan teknologi informasi dan komunikasi, menjadi lebih pintar dan bijak di ruang siber seakan menjadi tuntutan agar dapat hidup aman di dunia ini. Untuk bisa memahami lebih dalam terkait keamanan siber, berikut beberapa hal yang harus dipahami terkait konsep ini.

KEAMANAN SIBER DI ERA DIGITAL BARU

Keamanan siber adalah kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan siber, organisasi dan aset pengguna internet (ITU, 2018). Organisasi dan aset pengguna dalam keamanan siber juga meliputi perangkat yang terhubung komputasi, personil, infrastruktur, aplikasi, layanan, sistem telekomunikasi dan totalitas informasi yang dikirimkan atau disimpan dalam ruang siber (Handrini Ardiyanti, 2014). Singkatnya, keamanan siber adalah aktivitas pengamanan untuk mencegah terjadinya tindak kejahatan siber seperti yang dijelaskan pada pembahasan sebelumnya.

Pada umumnya, mereka yang sudah sadar tentang pentingnya keamanan siber adalah mereka yang bekerja di bidang keamanan siber secara profesional atau pihak-pihak yang memang tertarik dengan perkembangan dunia teknologi, informasi dan komunikasi. Namun, pemahaman

dari sebagian besar masyarakat luas cenderung masih sangat minim, walaupun resiko kerugian ini begitu dekat dengan aktivitas kehidupan kita sehari-hari di tengah dunia yang digital saat ini.

Kemanan siber menjadi penting untuk dipahami karena jika serangan terjadi akan banyak kerugian yang dapat dialami. Baik serangan yang sifatnya besar dan organisasional ataupun serangan berskala kecil yang menimpa perseorangan. Belum lagi di era digital baru saat ini, fenomena masyarakat yang menjadi lebih dekat dan lebih hidup di ruang siber, membuka peluang yang besar bagi pelaku kejahatan siber untuk dapat memanfaatkan berbagai informasi yang dapat mereka peroleh melalui sinyal-sinyal komputer dan internet. Oleh karenanya, kedekatan kita dengan internet saat ini tetap perlu dibentengi dengan memahami setidaknya dasar-dasar keamanan siber sehingga dapat mengantisipasi terjadinya kejahatan siber setidaknya untuk kita sendiri.

Sekilas Tips

Upaya memperkuat pertahanan suatu sistem kemanan siber dapat dijalankan melalui proses dalam ranah teknis dan praktikal. Dalam konteks kemanan siber di level makro yang berkaitan dengan sistem komputasi canggih dan berskala besar, sebuah proses peningkatan keamanan (*security hardening*), umumnya meliputi masalah teknis, seperti pengamanan dari sisi jaringan, sistem operasi, keamanan data dan *source code* aplikasi. Dalam merealisasikan usaha teknis ini, seringkali institusi keuangan dan telekomunikasi secara rutin menyewa konsultan keamanan untuk melakukan kegiatan '*penetration testing*' (Mochammad James Falahuddin, 2015). *Penetration Testing* atau yang lebih populer dengan istilah "*Pen-Test*" dilakukan dengan bertujuan untuk mengukur sejauh apa kekuatan sebuah sistem yang dimiliki dapat bertahan terhadap berbagai serangan-serangan yang berpotensi mengeksploitasi sistem tersebut. Hasil dari test ini kemudian menjadi titik balik untuk memperbaiki dan memperkuat sistem pada titik-titik lemah yang terdeteksi.

Secara praktis, serangan siber yang berpeluang menimpa kita dalam kehidupan sehari-hari adalah penyalahgunaan transaksi bank *online* dan virus yang menyerang perangkat akses ke ruang siber, seperti komputer dan ponsel pintar. Dalam konteks pertama terkait rekening bank yang terintegrasi dengan perangkat kita secara *online*, upaya meningkatkan keamanan siber untuk hal ini adalah dengan menggunakan perangkat atau ponsel pintar terpisah saat ingin melakukan aktivitas ini. Hal ini dilakukan untuk mengantisipasi jika komputer atau ponsel yang biasa digunakan menjadi korban dari serangan siber, dimana semakin sering kita menggunakan suatu perangkat, maka semakin besar pula kemungkinan perangkat tersebut menjadi korban serangan. Oleh karena itu, menggunakan komputer atau perangkat khusus untuk mengakses atau mengintegrasikan akun rekening bank *online* akan mengurangi peluang anda untuk menjadi korban dari kejahatan siber. Dalam konteks kedua, untuk mengatasi serangan virus yang menyerang perangkat seperti komputer dan ponsel, kita harus melakukan *backup* secara teratur dan selalu memastikan *harddisk* eksternal tidak terhubung dengan komputer. Dengan cara tersebut, bahkan jika seluruh komputer terenkripsi berkat virus *ransomware*, file yang dimiliki akan tetap dapat diakses (Chris Baraniuk, 2017).

Untuk lebih memahami dan mengenal lebih dekat keamanan siber, mari kita coba ulas lebih dalam tentang seluk-beluk dan ruang lingkup dari keamanan siber dalam konteks yang sangat dekat dengan kehidupan kita sehari-hari!

RUANG LINGKUP KEAMANAN SIBER

Dalam pembahasan kali ini, kita akan membahas pengenalan terkait hal-hal yang sering ditemui dalam keseharian yang ternyata merupakan bagian dari keamanan siber mulai dari Perlindungan Data Pribadi, Privasi, Jejak Digital (*Digital Footprint*), dan *Child Online Protection*.

Perlindungan data pribadi merupakan perlindungan yang dibuat untuk melindungi data pribadi pengguna layanan internet. Data pribadi meliputi identitas seperti tanggal lahir, alamat, riwayat kesehatan, nomor telepon, nama anggota keluarga, nomor rekening, dan lain-lain. Data pribadi penting untuk dilindungi untuk menghindari penyalahgunaan data pengguna yang bersifat rahasia.



Perlindungan data pribadi adalah perlindungan atas setiap data tentang kehidupan seseorang baik yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lain baik secara langsung maupun tidak langsung melalui sistem elektronik maupun non elektronik (Donny BU (*ed.*), 2017).

Kesadaran akan pentingnya melindungi data pribadi dalam media sosial atau yang disimpan pihak ketiga membuat Indonesia menjadi salah satu negara yang mudah diretas. Masyarakat Indonesia tidak terlalu mempersoalkan penggunaan data pribadi untuk keperluan lain. Salah satunya adalah saat mengisi formulir perbankan, asuransi, atau kartu kredit. Masyarakat biasanya sering melewati klausul persetujuan yang diberikan perusahaan karena kurang teliti bahkan tidak membaca sama sekali hingga melakukan persetujuan. Ketika data pribadi sudah terlanjur bocor, akan sulit menutup kembali kebocoran data yang sudah terjadi.

Untuk mengantisipasi penyalahgunaan, masyarakat dihimbau untuk memastikan data pribadi yang sudah disebar pada media sosial atau pihak ketiga ditarik kembali atau diminta tidak muncul ke publik.

Selain itu data yang dimiliki pihak ketiga seperti sekolah, rumah sakit, atau perusahaan bisa dijaga dengan baik. Sehingga yang menjaga bukan hanya diri sendiri tapi lembaga atau organisasi juga wajib menjaga data tersebut (Ruby Alamsyah, Pakar IT. Metrotvnews.com, 2018). Hal yang harus diperhatikan ketika berselancar di internet untuk mengamankan data pribadi: (Plimbi.com, 2015)

1. Memastikan data terenkripsi



Beberapa situs web dan browser telah menggunakan teknologi enkripsi untuk memastikan data terkode dengan aman ketika dikirimkan melalui situs web. Metode enkripsi ini misalnya protokol Secure HTTP (HTTPS) dan sertifikasi SSL (SSL certificate). Ciri enkripsi dapat dilihat ketika membuka laman web yang bersangkutan. Di browser, bisa diidentifikasi halaman web yang menggunakan protokol Secure HTTP dengan awalan “https” atau juga logo gembok seperti gambar diatas.

2. Jaringan Wifi

Ketika berada di tempat publik, harus berhati-hati dengan jaringan wifi yang biasa ditemukan untuk berselancar internet secara gratis. Jaringan wifi ini dapat dimanfaatkan orang untuk mencuri data. Hal yang umum dilakukan adalah dengan membuat access point palsu yang jika orang login melalui akses tersebut, datanya akan dicuri. Maka harus selalu waspada ketika menggunakan akses Internet melalui access point wireless publik seperti ini. Hindari access point yang berpotensi meminta data pribadi seperti account login, password dan sebagainya.

3. Phising



Ketika mengakses website, banyak sekali bertebaran hyperlink liar. Dalam beberapa kasus, hyperlink tersebut dapat mengarahkan ke halaman login palsu sebagai jebakan dan mencuri data pribadi. Hal seperti ini lah yang disebut phising. Ketika berselancar di internet harap diperhatikan hal seperti ini.

4. Password



- Hindari penggunaan tanggal lahir sebagai password
- Hindari penggunaan nama siapapun sebagai password
- Password merupakan kombinasi huruf dan angka
- Panjang password minimal 8 karakter
- Ganti password secara berkala misalnya selama 3 bulan sekali



5. Gunakan mode Incognito

Mode incognito merupakan fitur yang dimiliki oleh kebanyakan browser yang sudah modern. Fitur ini mematikan perekaman data ketika berselancar Internet. Browser tidak akan merekam alamat situs dan laman yang telah dikunjungi. Browser juga tidak dapat merekam data pribadi, seperti nama pengguna untuk login, password, juga cache dan cookies dari situs web yang dikunjungi.



Sekilas Info

Facebook merupakan media sosial dengan jumlah pengguna terbesar di Indonesia. Di tahun 2018 ini, raja sosial media ini kembali diterpa tuduhan serius. Kali ini, Facebook diduga mencuri data privasi pengguna demi kepentingan pihak ketiga. Pencurian data tersebut dilakukan melalui kuis-kuis yang seringkali muncul di aplikasi Facebook, seperti cara mengetahui kepribadian seseorang, rezeki, sampai kapan jodoh datang.

Ternyata, kuis-kuis tersebut memiliki masalah keamanan data. Hal ini terjadi disebabkan oleh status kuis tersebut yang seringkali melibatkan pihak ketiga yang turut diberikan akses terhadap data pengguna. Salah satu dari pihak ketiga ini adalah Cambridge Analytica, sebuah perusahaan konsultan politik Inggris yang dituding mengeksploitasi data 50 juta pengguna Facebook.

Isu mengenai kuis yang beredar di Facebook memang sudah menjadi perdebatan yang berujung pada kesimpulan bahwa keberadaannya merupakan sebuah masalah baru. Kesimpulan ini ditarik dengan alasan bahwa sejumlah kuis Facebook dipakai mengecoh orang-orang untuk mendapatkan informasi pribadi mereka dan menghasilkan uang dari hal itu. (Merdeka.com, 2018)

Informasi ini diungkapkan oleh *Managing Director* Keamanan Siber di Florida Center, Sri Sridharan. Menurutnya, kuis semacam ini kelihatannya memang tak berbahaya, tapi tak pernah diketahui siapa yang sebenarnya meminta informasi tersebut.

Dikutip dari Inquirer, Selasa (20/3/2018), hacker seringkali menggunakan kuis dengan jenis-jenis ini untuk menutup link berbahaya yang bisa digunakan untuk membobol keamanan online. *“Semakin banyak yang mereka tahu tentang Anda, semakin banyak juga cara yang digunakan untuk mengecoh Anda melakukan sesuatu seperti mengklik link yang seharusnya tidak boleh Anda klik,”* tuturnya.

Mengingat banyak kuis yang membahayakan data pribadi, dia pun menyarankan agar pengguna hanya mengikuti kuis dari situs web terpercaya. Pengguna juga diminta waspada jika mengikuti kuis atau jajak pendapat yang mengharuskan login ke akun Facebook.

Salah satu jenis kuis di Facebook yang paling populer adalah kuis kepribadian yang diduga juga menyimpan bahaya serupa. Argumen ini disampaikan oleh Aleksandr Kogan yang membuat aplikasi **thisisyour-digitallife**. Dimana Kogan menyediakan kuis dengan syarat login dengan akun Facebook. Dari eksperimen ini, Kogan menciptakan celah sebagai sosok pembuat kuis untuk melihat sebagian data-data yang dimiliki pengguna di Facebook, seperti identitas dan jejak digital yang mereka miliki.

Oleh karena itu, sangat penting bagi kita untuk memiliki kesadaran agar dapat berhati-hati dalam melakukan berbagai aktivitas di dunia digital. Kuis tersebut memang sejatinya untuk hiburan semata, tetapi menyimpan bahaya laten pencurian data. Inilah yang perlu disadari oleh pengguna untuk selalu berhati-hati setiap mengisi form di internet. Bukan berarti menghindari sama sekali untuk terjun dan menjadi bagian dari masyarakat digital, tetapi menjadi lebih bijak dalam melakukan dan memutuskan setiap keputusan untuk menjaga keamanan kita di dunia siber saat ini.



Privasi merupakan hak individu untuk mengontrol, mengatur, mengubah, dan menghapus informasi tentang dirinya. Hal ini termasuk untuk memutuskan kapan, bagaimana, dan untuk apa informasi itu disampaikan ke pihak lain.

Contoh privasi individu

- Tidak mengekspos ideologi atau keyakinan
- Menutupi riwayat keluarga
- Menolak untuk mengekspos bagian tubuh tertentu
- Merahasiakan jejak medis

(Donny BU (*ed.*), 2018)

Salah satu hal yang penting tentang privasi adalah demi keuntungan tertentu, seperti peluang mendapat hadiah undian, privasi dapat dikorbankan. Pada konteks ini, seseorang memberikan detail personal atau biodata untuk mendapatkan kesempatan memenangkan suatu hadiah. Hal ini cukup riskan karena informasi yang secara sukarela diberikan tersebut bisa saja dicuri atau disalahgunakan oleh orang yang tidak bertanggung jawab.

Privasi penting karena merupakan sebuah senjata yang cukup kuat. Data pribadi yang diberikan kepada orang lain merupakan hal yang ma-

hal. Semakin orang lain tahu mengenai informasi tentang diri sendiri, orang tersebut dapat menguasai diri kita. Maka dari itu privasi begitu penting karena pada saat ini internet selalu lekat dalam kehidupan kita.

Sekilas Info

Pada pertengahan 2017, salah satu berita terkait dunia digital Indonesia yang cukup ramai diperbincangkan adalah soal persekusi yang dilakukan oleh sejumlah pihak yang diawali dengan penelusuran melalui jejaring media sosial. Persekusi menurut *Koordinator Southeast Asia Freedom of Expression Network (SAFEnet)* Damar Juniarto adalah tindakan memburu orang atau golongan tertentu, yang dilakukan suatu pihak dengan sewenang-wenang secara sistematis atau luas.

Istilah yang cenderung masih awam ini dapat dideskripsikan sebagai tindakan tidak manusiawi, yang dimaksudkan menimbulkan penderitaan baik fisik dan psikis. Kemudian menjadi serangan sistematis dan meluas. Adapun beberapa tahapan yang dilakukan oleh pelaku persekusi adalah Pertama adalah penentuan target operasi yang dilakukan dengan mengumumkan di media sosial, yang kemudian dilaporkan. Biasanya pelaku melakukan *screenshot* atas konten yang diposting oleh target yang dianggap menistakan Islam dan ulama. Kemudian mereka masuk ke dalam database buronan umat Islam dan pelaku dapat melaporkan target dengan mengirim ke Muslim Cyber Army dengan email Mca@gmail.com.

Kemudian tahap kedua adalah seruan untuk memburu target yang dianggap menistakan dan menghina ulama. Salah satunya dengan membuat ajakan Aksi Bela Islam seperti di Karawang, Jawa Barat, dengan seruan menangkap dan penjarakan Aking penista agama. Seperti dalam kasus Aking yang dianggap menistakan agama dalam postingannya terkait PKI

Pada tahap akhir, target persekusi akan dibawa ke kepolisian untuk diperkarakan secara hukum, dengan dilaporkan sebagai tersangka dengan Pasal 28 ayat 2 Undang-Undang ITE dan atau Pasal 156a KUHP dengan status “Meminta dilakukan penahanan”.

Persekusi pada hakikatnya merupakan salah satu contoh pelanggaran privasi. Di era internet, informasi dengan cepat meluas dalam hitungan detik. Dengan banyaknya pemberitaan mengenai hal-hal negatif, tidak menutup kemungkinan seseorang bisa mengalami persekusi oleh orang lain. Klarifikasi pun mungkin tidak akan didengar. Hal ini perlu dikaji kembali sebab seseorang pada dasarnya berhak mengeluarkan pendapat berdasarkan apa yang diyakininya tanpa perlu dipersekusi orang lain.

Ketiga, pelaku persekusi akan melakukan intimidasi dan memaksa target untuk menuliskan permohonan maaf, dengan dibubuhi materai Rp 6 ribu. Surat itu juga wajib dibaca dan langsung didokumentasikan melalui video dan foto melalui media sosial. Dimana hasil video dan foto ini akan kembali diviralkan di sosial media seperti Indri Soraya di Tangerang dan yang terbaru anak usia 15 tahun Putra Mario Afian di Cipinang Muara.

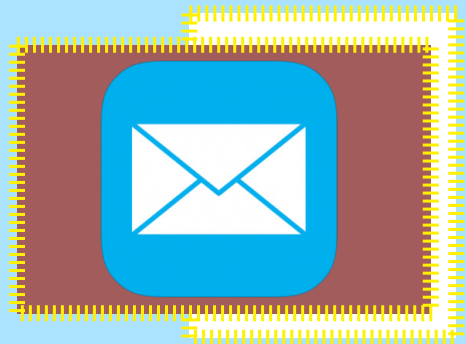
Sekilas Tips (Pemmzchannel.com, 2017)

1. Hati-hati dalam mengirim informasi sensitive



Berbagai website atau aplikasi akan meminta untuk mengunggah data-data pribadi seperti foto atau scan KTP. Hal ini harus diperhatikan. Selain itu kebiasaan mengunggah foto tiket perjalanan juga harus disadari. Karena hal tersebut dapat memberikan informasi kepada orang untuk melakukan hal buruk, seperti merampok rumah. Selain itu perlu diperhatikan juga *privacy policy* untuk layanan dunia maya yang sedang digunakan. Dengan begitu dapat diketahui data pribadi yang diunggah akan digunakan untuk apa oleh penyedia layanan.

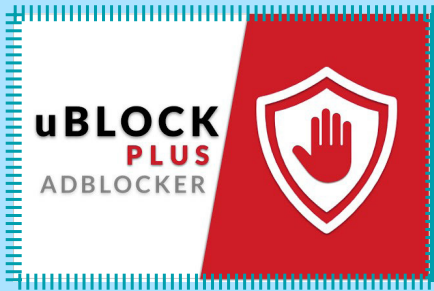
2. **Gunakan email lain**



Sumber gambar: <https://www1.bournemouth.ac.uk/students/log-service>

Saat mendaftar di media sosial atau aplikasi yang membutuhkan email, daftarlh di email lainnya selain email utama. Hal ini akan menghindari dari pencurian data melalui email.

3. Menggunakan ad-blocker.



Banyak situs dengan konten iklan yang muncul tiba-tiba (pop-up) dan menghalangi membaca konten yang disajikan di dalamnya. Beberapa jenis iklan seperti itu disusupi oleh kode pelacakan sesi browsing. Pelacakan atas pola-pola penggunaan browser (termasuk info tentang situs seperti apa yang biasanya dikunjungi, berapa lama waktu yang dihabiskan di situs tertentu, dan informasi lainnya) tentunya akan mengganggu privasi. Karena itu bijak rasanya untuk mengaktifkan ad-blocker untuk mengeliminasi pengganggu. Selain itu bisa juga menggunakan peramban Firefox Quantum yang begitu menghargai privasi di dunia internet.

JEJAK DIGITAL (DIGITAL FOOTPRINT)

Sandi S. Varnado dalam jurnalnya berjudul “Your Digital Footprint Left Behind at Death: An Illustration of Technology Leaving the Law Behind”, mengungkapkan bahwa jejak digital merupakan kumpulan jejak dari semua data digital, baik dokumen maupun akun digital. Jejak digital dapat tersedia baik bagi data digital yang disimpan di komputer (tanpa terhubung internet) maupun yang disimpan secara online. (*Tirto.id, 2018*)

Konten yang dibuat sendiri oleh pengguna dan konten yang dibuat oleh orang lain tentang pengguna

- Konten yang dibuat oleh pengguna seperti tulisan di blog, komentar di website, foto dan profil yang diupload oleh pengguna di media sosial.
- Data dari interaksi pengguna dengan website/aplikasi. Aktivitas pengguna direkam. Berbagai hal yang direkam antara lain halaman web yang dilihat, frekuensi kunjungan dan jangka waktu antar kunjungan, klik, waktu yang dihabiskan pada setiap halaman website, interaksi dengan form, landing page dan downloadable content. Setiap klik, gerakan mouse, keyboard dan interaksi dengan web (melalui PC atau mobile) dapat direkam dan disimpan.
- Data sisipan seperti alamat IP, ISP, lokasi fisik, reputasi, konteks, rekaman telepon, like, friend, perilaku, dll

Ada 2 jenis jejak digital:

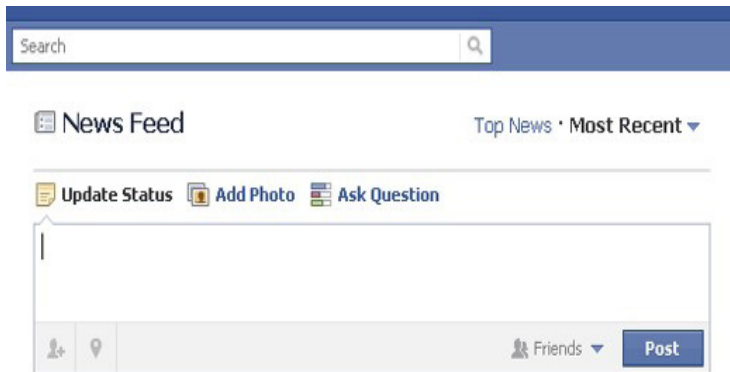
Pasif dan Aktif

Pasif



Jejak digital pasif merupakan jejak yang tidak sengaja ditinggalkan. Tidak ada tindakan aktif yang dilakukan si pemilik jejak dalam menghasilkan jejak digital itu. Contohnya adalah ketika mengunjungi website, server akan mendeteksi alamat IP kita dan mengetahui ISP yang kita gunakan dan lokasi kita pada saat mengakses website. Selain itu jejak digital pasif juga dapat berupa search history dalam situs pencarian

Aktif



Jejak digital aktif merupakan segala jejak digital yang tercipta atas peran aktif si pengguna. Contohnya adalah form yang diisi secara online, update status di jejaring sosial, email yang dikirim dan diterima.

Mengapa jejak digital penting?

Jejak digital yang tercipta atas tindakan digital penggunanya bisa disebut bom waktu yang tertanam. Bom tersebut akan meledak jika terdapat pihak tertentu yang menargetkan pemilik jejak digital. Hal tersebut diperparah jika si pemilik jejak diketahui memiliki jejak yang dapat merugikan dirinya sendiri. Kelly Moore dalam jurnalnya "The Influence of Personality on Facebook Usage, Wall Posting, and Regret,

menceritakan bahwa 20 persen pengguna Facebook tak mau apapun yang ia unggah ke media sosial itu dilihat oleh atasan mereka.

Meskipun jejak digital memiliki risiko yang berbahaya, pemilik seringkali tidak menyadari. Gwenn Schurgin O’Keeffe dalam jurnalnya “*The Impact of Social Media on Children, Adolescents, and Families*” mengungkapkan adanya anggapan bahwa apa yang terjadi di ranah online, hanya ada di dunia itu oleh para pemilik jejak digital (Tirto.id, 2018). Padahal setiap komen, *likes*, dan apapun yang kita ikuti dan lakukan akan terekam selama-lamanya atau abadi.

Sekilas Info

Rini merupakan kandidat penerima beasiswa di Inggris. Ia sudah menyelesaikan berbagai tahap dari administrasi hingga tahap final. Pada tahap terakhir, Rini melakukan wawancara final dengan pemberi beasiswa. Pemberi beasiswa sangat senang dengan pribadi Rini dan mengatakan bahwa Rini merupakan kandidat terbaik. Setelah wawancara final, pemberi beasiswa akan melakukan background check sebagai verifikasi.

Setelah melakukan background check melalui media sosial, terungkaplah bahwa Rini kerap menggunakan bahasa kasar dalam media sosialnya. Selain itu Rini juga kerap mengunggah gambar yang tidak pantasnya diunggah. Akibat hal tersebut Rini gagal mendapatkan beasiswa.

Dari kasus ini kita dapat belajar bahwa selalu berhati-hatilah setiap ingin mengunggah apapun di ruang siber karena akibat dari perbuatan kita sekecil apapun bisa berakibat fatal sebagaimana yang dialami Rini. Proses mencari beasiswa yang tidak mudah dan perlu waktu dan tenaga untuk mengurusnya. Ketika gagal di tahap terakhir dan jika disebabkan oleh postingan di media sosial. Sungguh kenyataan yang berujung ironis.

Sekilas Tips – (Fosi.org, 2016)

Berikut adalah cara untuk membersihkan jejak digital kita di dunia maya:

1. Periksa jejak digital

Cobalah mencari diri sendiri di situs pencarian. Lihatlah apa yang terdapat dalam hasil pencarian tersebut. Periksalah bagaimana situs tersebut menampilkan informasi tentang diri sendiri. Jika kurang berkenan, segera hubungi pihak situs terkait dan meminta untuk menghapus informasi yang ada. Beberapa situs yang menggunakan aturan privasi terkadang menerapkan perubahan aturan tanpa memberi tahu. Periksalah bagaimana situs itu menampilkan informasi tentang diri dan atur kembali jika ada perubahan yang membuat informasi anda terekspos di publik.

2. Selalu perbarui versi perangkat lunak

Malware dapat menyerang kapan saja. Oleh karena itu, melakukan pembaruan sistem, aplikasi anti virus dan firewall merupakan hal wajib yang sebaiknya dilakukan secara periodik. Hal tersebut juga dapat diatur secara otomatis dalam aplikasi tersebut.

3. Bijak sebelum menulis

Beberapa hal yang tampil dalam internet bukan hanya sekedar informasi tentang diri sendiri, tetapi cara berperilaku juga kerap terekam secara otomatis dalam internet. Maka dari itu diperlukan pemikiran yang matang sebelum menulis atau mengunggah apapun ke internet.

4. Perhatikan perangkat mobile

Ponsel atau tablet merupakan perangkat yang memberikan akses langsung terhadap diri sendiri secara pribadi. Pelajari aturan privasi di dalam perangkat tersebut kemudian pastikan untuk tidak mengizinkan aplikasi yang akan “menarik” data pribadi tanpa sepengetahuan diri sendiri.

5. Bangun citra diri yang positif

Gunakan akses internet untuk hal yang positif. Salah satu caranya adalah dengan menampilkan keahlian dan buat dalam bentuk konten berupa tulisan, gambar, atau video sehingga dapat berguna bagi orang banyak. Hal tersebut akan membuat citra diri secara positif di dunia maya.

CHILD ONLINE PROTECTION



Internet membawa kemudahan akses informasi bagi siapa saja, termasuk anak-anak. Hal ini membuat anak-anak rentan terhadap dampak negatif internet. Untuk melindungi anak-anak dari dampak negatif internet, *International Telecommunication Union* (ITU) membuat program *Child Online Protection* (COP), yang dibentuk pada tahun 2008, sebagai upaya dari *Global Cyber Security Agenda* dalam menyatukan seluruh lapisan masyarakat dan semua sektor, untuk memberikan keamanan serta menghadirkan pengalaman menggunakan internet dengan baik untuk anak-anak di penjuru dunia. (Wantiknas, 2016)

Tujuan dari OCP antara lain:

- ✓ Mengidentifikasi resiko bagi anak-anak dalam dunia maya
- ✓ Menciptakan kesadaran bagi pembuat kebijakan, industri, orang tua, pendidik, serta anak-anak
- ✓ Pengembangan alat-alat praktis untuk mengurangi resiko
- ✓ Berbagi pengetahuan dan pengalaman

Untuk merealisasikan OCP, terdapat beberapa mitra kerjasama seperti:

- ✓ UNICEF
- ✓ UNODC
- ✓ UNICRI
- ✓ UNIDIR
- ✓ European Commission
- ✓ Interpol
- ✓ ENISA (European Network and Information Security

Agency)

- ✓ Insafe
- ✓ Commonwealth Telecommunications Organisation (CTO)
- ✓ IMPACT

Di Indonesia, berlatar belakang kekhawatiran tentang keselamatan anak Indonesia di dunia daring, sejumlah institusi yaitu Komisi Perlindungan Anak Indonesia (KPAI), Yayasan Nawala, Yayasan SEJIWA, ECPAT Indonesia, Relawan TIK, dan ICT Watch, mendirikan Indonesia Child Online Protection (ID-COP). Forum ini menerima laporan dan keluhan masyarakat yang berkaitan dengan child trafficking (perdagangan anak), cyber bullying (kekerasan di internet), dan online child prostitution (prostitusi anak di online).

Berdasarkan data dari KPAI, sejak 2011 sampai 2014, ada 932 laporan kasus pornografi dan kriminal di dunia maya yang menargetkan anak-anak sebagai korban. Berdasarkan survei Biro Pusat Statistik, menunjukkan bahwa antara 2010 – 2014, ada 80 juta anak yang telah mengakses pornografi online, jumlahnya terus meningkat. Sebanyak 90% anak-anak yang mengakses pornografi online, telah mengawali pengalamannya ketika mereka berusia sekitar 11 tahun, dan mereka mengakses situs-situs porno justru ketika tengah mengerjakan tugas-tugas sekolahnya. ID-COP diharapkan dapat meningkatkan kesadaran masyarakat mengenai bahaya yang mengancam anak-anak di internet, serta menguatkan pengetahuan dan pengalaman para pengambil keputusan dalam mengatasi kasus-kasus di dunia maya yang menargetkan anak-anak. (Liputan6.com, 2015)

Sekilas Info : (Tribunnews.com, 2018)

Pada bulan Maret 2018, kasus video anak perempuan sedang menonton tayangan porno di samping seorang wanita yang diduga ibunya dan viral di media sosial, mendapatkan perhatian khusus dari Komisi Perlindungan Anak Indonesia (KPAI). Komisioner KPAI, Erlinda menyesalkan wajah sang anak yang terlihat jelas dalam rekaman video yang beredar. Menurutnya, hal itu sangat tidak baik untuk tumbuh kembang anak ke depannya. Penyebaran video tersebut menurut Erlinda, akan membentuk suatu sikap dan penilaian yang buruk dari masyarakat terhadap korban dan keluarganya.

Lebih lanjut, Erlinda mengatakan, buruknya pengawasan orang tua terhadap sang anak. Orang tua seharusnya bisa memahami bahwa memberikan kesempatan kepada anak berselancar di dunia maya, tidak hanya dengan pengawasan saja, tapi juga dengan pemahaman dan pengetahuan mengenai mana yang pantas dan tidak pantas untuk anak. Hal yang paling mengkhawatirkan adalah fakta bahwa sang anak sangat menikmati video tersebut, sehingga dikhawatirkan sang anak akan terpengaruh adiksi pornografi sejak dini.

Selain itu, Erlinda juga menyesalkan tindakan pelaku penyebar video tersebut hingga viral di masyarakat. Erlinda prihatin kepada yang merekam kenapa tidak mengambil tindakan malah memviralkan. Kalau pun merekam, kata Erlinda, mengapa tidak menyerahkan pada lembaga yang kompeten untuk segera diambil tindakan. Setidaknya saat deteksi awal penyebaran video ini terjadi, berkomunikasi secara baik pada orang tua tanpa membuat sang anak panik juga bisa dilakukan untuk mengantisipasi dampak negative ang lebih besar.

Erlinda dan KPAI mengimbau para orang tua, lembaga perlindungan anak lainnya dan kementerian untuk memberikan perhatian khusus terhadap kasus ini mengingat maraknya kejadian serupa di lapangan

peran masyarakat untuk tidak dengan sangat mudah menyebarkan video dan fenomena semacam ini hingga menjadi viral di dunia siber. Sebab dengan beredar luasnya video seperti ini akan memberikan pengaruh buruk buat psikologis anak-anak. Dengan tidak menyebarkan video sejenis, maka kita telah memberikan perlindungan kepada anak tersebut.

Sekilas Tips

Kesadaran orang tua untuk meminimalisir terjadinya berbagai kejahatan di dunia siber dengan mengaplikasikan OCP dapat direalisasikan melalui Aplikasi Parental Control. Berikut beberapa aplikasi yang bisa anda gunakan untuk melindungi anak anda di dunia maya:

Qustodio



Program parental controls yang bisa digunakan sebagai filter dan monitor aktivitas anak di internet. Qustodio juga bisa membatasi waktu anak saat melakukan aktifitas online. Dengan menggunakan fitur Internet Usage Schedule, Qustodio akan menetapkan jadwal yang secara otomatis mengaktifkan dan menonaktifkan internet pada device anak tertentu.

Qustodio juga bisa mengatur hal-hal sebagai berikut:

- Memblokir akses internet tapi mengizinkan penggunaan komputer.
- Blok akses intrnet dan mengunci komputer.
- Mengirim pesan saat batas waktu dilanggar oleh anak-anak.

K9 Web Protection



K9 Web Protection merupakan perangkat lunak komputer sebagai keamanan berselancar di dunia maya yang difungsikan sebagai pengawas anak-anak di internet.

Beberapa fungsi:

- penyaring konten yang dibuka maupun diunduh dari Internet
- pembatasan waktu untuk mematikan internet pada jam tertentu
- mengawasi aktivitas anak dengan mencatat web yang dikunjungi
- memblokir konten berdasarkan kata kunci

Selain menggunakan aplikasi-aplikasi pelindung anak dari bahaya dunia siber seperti yang dipaparkan di atas, penting juga bagi orang tua untuk selalu menjaga anak agar tetap aman dari pengaruh pornografi. Berikut adalah tips menjaga anak agar aman dari pornografi:

Dampingi anak saat mengakses internet

Dampingi anak-anak saat mereka berselancar di dunia maya. Jangan biarkan mereka mengakses internet sendirian. Batasi hal-hal yang tidak wajar diakses karena berbahaya.

Berikan pengertian yang baik kepada anak

Orang tua harus memberi tahu anak, tentang mana yang boleh dibuka dan tidak. Pengetahuan ini sangat penting agar anak terhindar dari situs internet yang tidak layak untuk mereka. Orangtua juga harus berhati-hati dan memberikan contoh yang baik untuk buah hatinya.

Jangan biarkan anak akses gadget di kamar

Jangan letakkan gadget, laptop, atau komputer di dalam kamar pada saat tidak bersama orangtua. Hal ini membuat anak semena-mena mengakses situs apapun yang diinginkannya. Beberapa kali bahkan orangtua kecolongan. Orangtua harus mencegah itu supaya anak nyaman dan mendapatkan informasi dari internet sesuai usia.

Hapus history di gadget

Segera hapus history. Karena gadget bisa saja dibuka oleh anak-anak yang seharusnya tidak mengetahui situs internet yang cocok untuk orang dewasa. Jangan biarkan mereka tahu history situs yang baru kita buka karena Mereka lebih peka dan rasa penasarannya tinggi

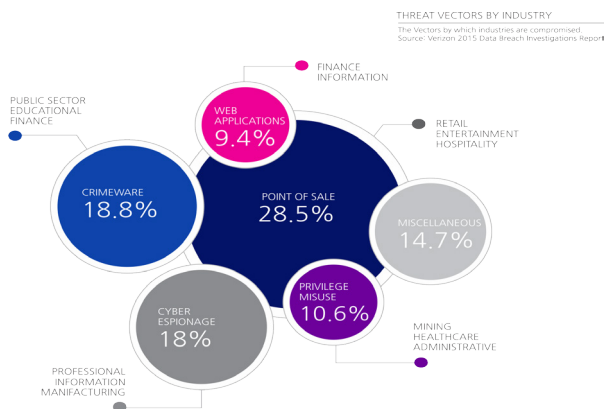
Buat profil safety mode

Bedakan situs internet yang dikunjungi oleh anak dan orangtua. Khusus anak, pakailah safety mode dengan memasukkan usia anak saat mendaftar sebuah akun. Hal ini sangat penting supaya anak tidak bisa mengakses situs internet yang negatif. Satu platform biasanya menyaring situs apa saja yang tidak boleh diakses anak-anak saat berselancar di dunia maya. Hal ini juga berlaku dengan model game yang aman untuk dimainkan anak.

Setelah menyelami sekilas beberapa ruang lingkup dari keamanan siber, setidaknya kin kita dapat lebih memahami berbagai macam kemungkinan dimana kejahatan siber dapat terjadi dan hal-hal apa yang bisa kita lakukan untuk mengantisipasi jika serangan siber terjadi. Untuk membawa anda lebih dekat dengan keamanan siber, pembahasan selanjutnya akan lebih mengeksplor berbagai upaya aplikatif dari kewanaman siber yang dapat dilakukan untuk menjadi pengguna internet yang lebih bijak.

KEAMANAN SIBER DI INTERNET

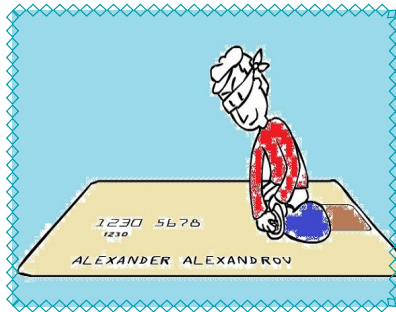
Kewanaman siber pada dasarnya bukan merupakan pilihan, tetapi sebuah kepastian. Dengan ketergantungan kita yang semakin tinggi terhadap internet, keamanan siber menjadi pagar yang berfungsi melindungi diri kita dari berbagai serangan yang mungkin akan terjadi. Sebab setiap kemajuan teknologi yang terjadi akan selalu ada pihak yang memanfaatkan hal tersebut untuk kepentingannya sendiri. Sekarang adalah saat yang tepat untuk kita bersiap diri menjadi pengguna internet dan masyarakat siber yang lebih bijak.



Sumber : ACS Cybersecurity Treats, Challenge, and Opportunities, 2016

Berbagai macam bentuk kejahatan siber telah dijelaskan pada pembahasan sebelumnya. Ancaman terbesar misalnya, datang dan berkaitan dengan kehidupan kita sehari-hari. Sistem yang sering kita gunakan saat bertransaksi di mini market, super market, atau restoran seperti mesin

kasir dan seperangkat komputer yang melengkapinya, ternyata merupakan salah satu gerbang ancaman terbesar dari terjadinya kejahatan siber. Penggunaan kartu kredit maupun debit pada sistem ini akan memberi akses terhadap informasi yang bisa saja di salah gunakan.



Sumber : Referensibebas.com, 2016

Kasus penyalahgunaan informasi dan data diperkirakan akan terus meningkat di tahun-tahun mendatang jika masyarakat tidak diberikan bekal pendidikan yang tepat tentang bagaimana mengamankan komputer, laptop dan perangkat lainnya dari kemungkinan terjadinya kejahatan ini. Selain melalui akses eksternal seperti yang telah disebutkan diatas, pencurian informasi juga dapat terjadi secara tidak kita sadari melalui diri kita sendiri. Misalnya melalui *cookie*.



Cookie adalah sejumlah data-data yang tersimpan di komputer atau perangkat lain kita yang tersambung ke internet. Saat kita mengakses berbagai informasi di internet, khususnya *website*. *Cookie* merupakan hal umum yang akan kita terima melalui browser kita. *Cookie* digunakan

untuk menyimpan data-data mengenai perilaku pengguna dalam mengakses website. Web Server dapat menggunakan data tersebut untuk mengolah informasi kembali sesuai dengan data dari *cookie* tersebut. (Hernawan, 2018).

Fungsi *cookie* sendiri adalah untuk mengidentifikasi siapa yang mengakses website. Contoh paling mudah adalah ketika kita membuka Facebook. Untuk pertama kalinya, kita akan diminta untuk memasukkan Email dan Password. Saat kita mencoba mengaksesnya kembali, kita tidak harus memasukkan data itu lagi dan anda langsung menuju beranda Facebook sebab *cookie*-mu telah merekam identitas kita.



Sumber : Lifewire.com, 2018

Cookie dapat menyimpan banyak sekali data seperti pengaturan, browser yang dipakai, lokasi, ketertarikan kita dan lain sebagainya. Informasi ini digunakan untuk meningkatkan pengalaman pengguna yang mengakses *website*. Dengan umunya yang tergolong pendek, pada dasarnya, *cookie* tidak berbahaya. Namun dapat menjadi boomerang jika dipegang oleh tangan yang salah.

Kecendrungan *cookie* menjadi boomerang yang besar sebenarnya tergolong kecil. Tidak terlalu sering *Cookie* dapat diretas oleh *hacker* atau *cracker* yang jahat. Hal paling buruk yang dapat terjadi adalah ketika seseorang dapat mengakses *Cookie* kita, lalu dia dapat mengakses akun-akun pada *website* tersebut. Namun jangan terlalu khawatir, sebab keamanan dari *Cookie* biasanya tergantung dari website dan browser

yang kita gunakan. Fitur enkripsi *Cookie* adalah salah satu contoh keamanan atas hal ini.

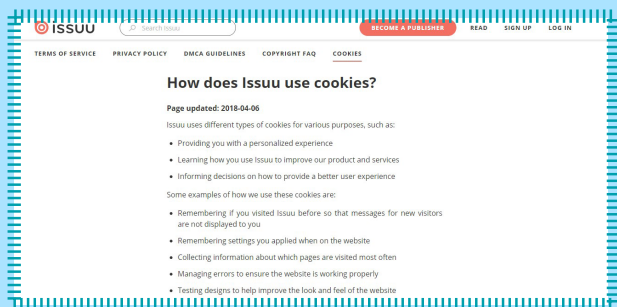
Hal yang mungkin dapat membahayakan adalah penyalahgunaan *cookie* yang dapat mengganggu ranah privasi kita. Kasus yang paling sering adalah adanya “*tracking cookie*”. *Cookie* jenis ini tidak digunakan untuk pengalaman pengguna, namun lebih digunakan untuk melihat kegiatan anda pada beberapa website. *Cookie* jenis ini dapat mengakses history browser anda, sehingga dapat digunakan untuk menampilkan iklan yang spesifik berdasarkan data-data tersebut (Hernawan, 2018).

Sekilas Info

Cookie tidak dapat mengetahui informasi tentang kita jika kita tidak memberikan informasi tersebut. Contohnya adalah ketika membuat akun di sebuah website. Jika kita tidak pernah memasukkan data alamat rumah anda, maka situs tersebut tidak akan mengetahuinya.

Selain itu, biasanya sebelum merekam, *cookie* akan meminta izin terlebih dahulu sebelum melakukan aksinya. Seringkali, sebuah website akan menunjukkan pilihan ketersediaan kita untuk direkam *cookie*-nya dalam *website* tersebut.

Bahkan beberapa *website* memberikan penjelasan lebih lanjut tentang bagaimana penggunaan *cookie* yang terekam dalam data mereka.



Sumber : Issuu, 2018

Tetapi, jika kita masih khawatir dengan keberadaan *cookie* ini, maka kita dapat memblokirnya dengan berbagai pengaturan yang ada di masing-masing browser. Selain memblokir semua cookies dari semua website, kita juga bisa memblokir cookies dari situs-situs tertentu saja. Namun jika kita ingin nyaman dalam mengakses internet, maka sebaiknya tetap mempertahankan cookies dari situs-situs yang kita percayai dan hanya memblokirnya dari berbagai situs asing yang mungkin akan berbahaya (Plimbi, 2013).

Penyalahgunaan *cookie* mungkin tidak begitu signifikan. Tetapi *cookie* menjadi salah satu asset berharga khususnya bagi dunia periklanan. Kemungkinan akan adanya campur tangan penggunaan data ini untuk kepentingan pihak tertentu bisa saja terjadi di masa yang akan datang. Oleh karena itu, kita perlu mengantisipasi berbagai kemungkinan yang akan terjadi melalui lini ini.

Jika seorang hacker pada akhirnya menyalahgunakan data informasi pribadi kita yang bisa ia dapatkan dari internet, ada beberapa tujuan yang mendasarinya:

- Menggunakan informasi tersebut untuk membuka rekening kartu kredit menggunakan nama, login perbankan, email dan password.
- Membuat duplikat kartu kredit yang kita miliki dan menggunakannya untuk membeli sesuatu secara online.
- Menggunakan virus Komputer yang disebut malware yang membuat pencuri dapat merekam ketikan keyboard anda sehingga mereka tau situs yang kita kunjungi beserta passwordnya.
- Dengan mendapatkan nomor jaminan sosial kita, hacker dapat meniru kita untuk mengajukan permohonan demi memperoleh asuransi, berlaku untuk properti atau pembelian properti sewa yang harus kita bayar tetapi tidak kita nikmati.

- Beberapa penipu dapat menggunakan kartu debit kita untuk berbelanja online.
- Pencuri dapat menggunakan virus ransomware untuk mengenkripsi file komputer kita. Mereka akan melakukan enkripsi file hanya jika kita membayar uang tebusan kepada mereka.
- Hacker dapat memperoleh akses ke ponsel kita ketika terhubung ke jaringan Wi-Fi publik. Demikian pula, ketika Wi-Fi di rumah tidak memiliki keamanan yang baik, hacker dapat menggunakannya untuk mendapatkan akses melalui perangkat lunak.

Untuk dapat menerapkan keamanan siber dalam konteks ini, kita bisa melakukan beberapa hal:

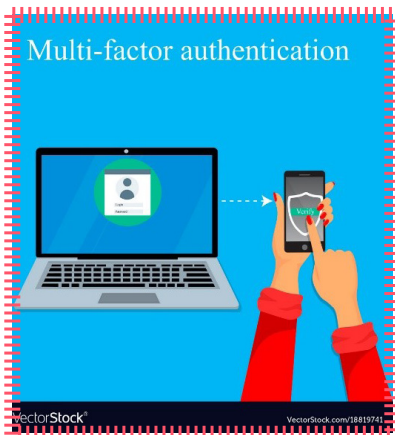
Langkah 1 - Gunakan Enkripsi



Sumber: Information Security Buzz, 2018

Enkripsi seperti yang sudah dijelaskan sebelumnya, merupakan sebuah metode untuk melindungi data. Biasanya digunakan untuk menyimpan informasi pribadi yang digunakan dalam transaksi online atau berbelanja online. Ada banyak bentuk enkripsi yang digunakan pada berbagai tahap ketika menangani informasi digital.

Langkah 2 - Otentikasi Komputer Anda



Sumber: Vectorstock.com

Otentikasi adalah keamanan tambahan untuk komputer kita. Ini adalah salah satu langkah yang paling penting untuk melindungi data privasi dari komputer untuk mengurangi risiko pencurian identitas.

Misalnya Double otentikasi membantu membuat password kita menjadi lebih aman karena cara ini memanfaatkan telepon pengguna untuk login, jadi dibutuhkan lebih dari sekedar password. Mereka akan mengirimkan kita nomor verifikasi dan para hacker harus memiliki akses ke telepon kita agar dapat mencuri akun milikmu.

Banyak komputer bisnis saat ini juga menggunakan slot-in smartcard yang memberikan keamanan ekstra. Anda dapat menemukan teknologi ini pada gadget yang lebih kecil seperti ponsel dan tablet. Metode otentikasi lainnya adalah biometrik, yaitu dengan cara mengidentifikasi wajah atau sidik jari seseorang. Namun, hanya laptop yang telah dilengkapi dengan perlengkapan tertentu yang dapat menggunakan cara ini.

Langkah 3 - Ubah Pengaturan Browser



Sumber : Depositphotos, 2018

Kebanyakan browser menyimpan password, email dan nama pengguna. Sementara ada pilihan untuk menonaktifkan ini, banyak orang memilih untuk menyimpan password mereka demi kenyamanan. Jika laptop kita dicuri atau di hack maka semua informasi yang tersimpan di browser dapat digunakan oleh pencuri identitas.

Seperti browser, email juga memiliki informasi pribadi kita dan dengan demikian harus lebih mudah diamankan. Para ahli menyarankan menggunakan password yang kuat (sering 12 karakter dan dengan angka, simbol, dan huruf besar dan huruf kecil) untuk membuat pencuri sulit untuk membuka semua akun yang kita miliki.

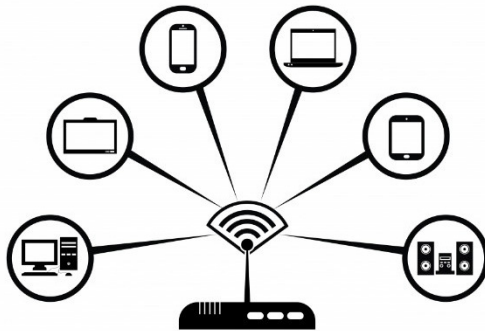
Langkah 4 - Update Anti Virus / Program Anti Malware

Tidak peduli apakah kita mengakses internet melalui komputer, laptop, atau smartphone. Sebuah perangkat lunak keamanan yang baik dapat melindungi kita setiap saat dari berbagai macam serangan seperti phishing, hacking, malware dan virus.



Malware dan virus dapat masuk ke sistem melalui berbagai cara untuk menyerang perangkat kita. Cara terbaik untuk memastikan kita terlindungi adalah dengan menginstal program anti virus dan anti malware yang akan melindungi komputer. Namun kita perlu memilih antivirus dan anti malware yang sesuai.

Langkah 5 - Lindungi Koneksi Nirkabel



Sumber: Digital Unite

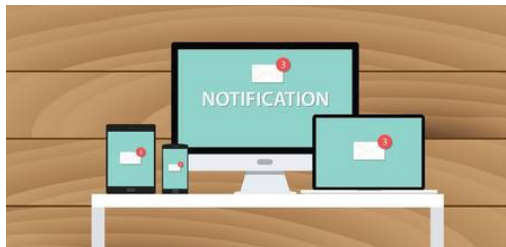
Pencuri data dapat menggunakan Wi-Fi untuk masuk ke komputer dan perangkat seseorang atau paling tidak melihat data transfERNYA. Jika tidak dienkripsi, koneksi Wi-Fi kita dapat dengan mudah digunakan sebagai alat untuk memata-matai hampir semua yang kita lakukan secara online.

Bila menggunakan koneksi jaringan nirkabel yang bersifat publik seperti di kafe, hotel, dan bandara maka pastikan bahwa semua informasi pribadi kita dilindungi (tidak mengakses rekening keuangan atau account penting ketika pada Wi-Fi publik).

Saat kita berada di rumah juga penting untuk mengenkripsi dan membuat password pada Wi-Fi keluarga). Banyak hacker menggunakan Wi-Fi untuk memperoleh profil rinci kita dan keluarga dengan hanya menganalisis dan melihat situs web yang kita kunjungi.

Sebagian besar situs melakukan enkripsi informasi yang kita berikan kepada mereka, namun masih ada situs lain yang tidak menyediakan enkripsi login yang akan mengamankan informasi milikmu. Salah satu cara dapat melindungi koneksi nirkabel adalah dengan menggunakan sandi yang kuat.

Langkah 6 - Gunakan Sistem Notifikasi



Sumber: 123RF, 2018

Salah satu cara untuk mengamankan informasi pribadi yang ada di komputer atau di perangkat manapun adalah dengan sistem notifikasi. Dengan sistem ini kita akan mendapat peringatan saat login ke sebuah akun, misalnya saja notifikasi SMS dan sebagainya. Dengan cara tersebut akan mudah mengetahui jika ada yang masuk ke akun kita selain dirimu sendiri.

Sebagai contoh, sistem peringatan identitas Lifelock memonitor berbagai aplikasi di komputer seseorang. Hal ini memberikan laporan lengkap dan monitoring layanan nirkabel, kartu kredit, hipotek dan banyak lagi. Ketika sistem mendeteksi risiko dalam identitasmu, ia akan mengirimkan peringatan melalui email, telepon atau sms.



Di zaman sekarang, semua sudah menjadi serba digital. Termasuk di sektor finansial seperti perbankan. Kita sebagai nasabah dapat melakukan transaksi perbankan dimana saja dan kapan saja, melalui internet (e-banking), telepon selular (m-banking), telepon (phone banking), ataupun lewat sms (sms-banking). Ini tentunya memudahkan kita sebagai nasabah dalam melakukan transaksi keuangan, tetapi di sisi lain dapat membuka peluang terjadinya penyalahgunaan. Berikut beberapa tips untuk mengamankan diri dari kejahatan siber dibidang perbankan.

1. Penipuan lewat telepon

Penipuan ini dilakukan melalui komunikasi telepon. Biasanya, pelaku kejahatan akan menelepon kita dengan memberi kabar-kabar tertentu seperti menapat hadiah, keluarga mengalami musibah atau menyatakan minat atas barang yang kita iklankan. Kemudian, si menelepon akan memandu kita untuk menuju ATM untuk melakukan apa yang mereka inginkan sesuai dengan instruksi yang diberikan ke kita.

Bagaimana Cara Menghindarinya?

Hal pertama yang harus kita lakukan adalah cek identitas si menelepon dan lakukan pengecekan atas informasi yang kita terima. Pada

umumnya perusahaan penyelenggara undian tidak meminta pemenang untuk mentransfer sejumlah dana kepada perusahaan penyelenggara.

Jika kita menerima telepon yang mengabarkan bahwa keluarga kita mendapat musibah, jangan panic dan jangan mengikuti perintah apapun yang diberitahukan oleh si penelopon. Lakukan hal yang sama dengan menanyakan identitas dan melakukan pengecekan.

Jika kita memasang iklan, berhati-hatilah dengan si penelopon yang tertarik dengan iklanmu dengan sangat mudah untuk setuju dengan harga yang kita tawarkan dan berjanji akan mentransfer sejumlah uang sebagai “tanda jadi atau uang muka”. Jangan mudah terpengaruh jika diminta mengecek saldo ke ATM. Segera tutup telepon kita.

2. Penipuan lewat email

Penipuan juga dapat terjadi melalui email kita. Email tersebut seolah-olah berasal dari bank resmi sehingga kelihatan asli. Pelaku kejahatan biasanya akan meminta kita untuk memasukkan nomor rekening dan nomor PIN. Modus serupa juga dilakukan dengan membuat website alamat bank kita yang seolah-olah asli tetapi sebenarnya adalah website palsu. Di website tersebut, kita juga akan diminta hal serupa ini dengan alasan untuk memperbarui data pribadi kita.

Bagaimana Cara Menghindarinya?

Jika mendapat email seperti ini yang mencurigakan, jangan pernah membalas dengan mengisi nomor rekening (atau user-id) dan nomor PIN karena bank seharusnya sudah memiliki data kita. Jika kita masuk ke website bank untuk melakukan transaksi perbankan, pastikan alamat website bank sudah benar dan kita memiliki prosedur keamanan tambahan seperti token, di samping user-id dan password.

3. Penipuan melalui penawaran investasi dengan imbalan bunga yang sangat tinggi

Modus ini biasanya mengatasnamakan perusahaan yang menawarkan investasi dengan janji imbalan bunga yang sangat tinggi. Kita harus berhati-hati dengan penawaran seperti ini karena terdapat sejumlah penawaran yang terbukti tidak dapat memenuhi imbal hasil sebagaimana dijanjikan.

Bagaiman Cara Menghindarinya?

Kita harus bersikap kritis dalam mempertimbangkan penawaran seperti ini. Apakah wajar? Segera lakukan pengecekan terhadap kredibilitas perusahaan yang menawarkan investasi dan pastikan kita terlindungi dari sisi hukum sebelum memutuskan untuk melakukan suatu investasi.

4. Penipuan dengan menggunakan kartu kredit di Internet

Sekarang ini semakin banyak toko atau merchant yang menawarkan produk dan jasa melalui telepon ataupun internet, dengan kemudahan pembayaran menggunakan kartu kredit. Biasanya, kita hanya diminta untuk menyebutkan nomor kartu kredit, masa berlaku (expiry date) dan 3 (tiga) digit kode rahasia yang tertera di bagian belakang kartu kredit kita, dengan demikian transaksi pun dapat terjadi.

Bagaimana Cara Menghindarinya?

Ketika kita mendapat tawaran seperti ini, kita harus mengerti tentang produk dan jasa yang ditawarkan dari toko atau merchant tersebut, dan juga memahami tentang syarat & ketentuan dari barang atau jasa yang ditawarkan. Jangan pernah memberikan nomor kartu kredit, masa berlaku dan 3 (tiga) digit kode rahasia yang terletak di bagian belakang kartu kredit kita kepada siapapun, kecuali untuk beberapa keperluan tertentu di mana kita telah menyetujuinya.

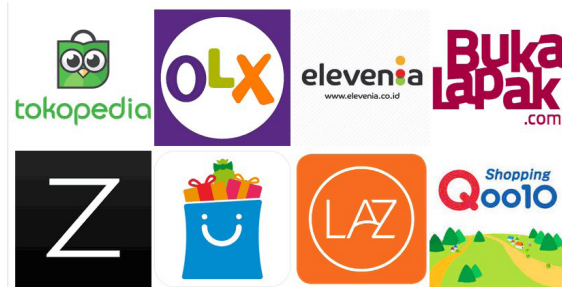
5. Pemalsuan nomor telpon call center bank kita

Modus ini termasuk yang paling sering terjadi. Pelaku kejahatan akan membuat seolah-olah mesin ATM bank kita rusak dan kartu kita tertelan. Otomatis kita menjadi panik dan tanpa sadar akan menghubungi nomor call center "palsu" yang ada di sekitar mesin ATM. Kemudian kita akan diminta penerima telepon untuk menyebutkan nomor PIN dan dijanjikan bahwa kartu ATM pengganti akan segera dikirimkan. Padahal, itu adalah cara mereka untuk mengambil uang kita dengan mengetahui PIN dan kartu kita.

Bagaimana Cara Menghindarinya?

Pastikan kita mengetahui nomor call center resmi bank kita. Jika perlu, catat nomor telepon 24 jam bank kita. Jika Anda menghubungi nomor tersebut, pada umumnya kita akan dijawab oleh mesin penjawab otomatis dan diminta untuk memasukkan pilihan jasa tertentu, bukan oleh suara penerima telepon secara langsung. Perlu kita ingat juga, jangan pernah memberikan nomor PIN karena bank tidak akan pernah meminta nomor PIN nasabahnya.

Sebagai tambahan agar dapat mencegah kejadian tersebut, kita juga dapat membuat pin ATM, m-banking, e-banking yang kemungkinan orang lain tidak mengetahuinya dan mudah diingat, dan juga membuat salinan dokumen pribadi jikalau terjadi pencurian data. Segera batalkan transaksi jika kita menemukan hal-hal yang mencurigakan seperti memasukkan data yang sensitif ketika mendaftarkan sebuah transaksi. Itulah beberapa tipe kejahatan siber di bidang perbankan dan tips bagaimana cara mengatasinya jika kita mengalami kejadian-kejadian tersebut.



Kita pasti suka kan berbelanja? Apalagi, sekarang ini banyak toko online atau ecommerce yang tersedia semakin mempermudah kita mengakses produk maupun barang yang kita butuhkan tanpa harus mendatangi tokonya. Tetapi, berbelanja secara online juga harus dilakukan secara hati-hati. Karena, maraknya praktik jual-beli online juga meningkatkan kasus-kasus penipuan. Berikut sejumlah tips untuk menghindari penipuan ketika berbelanja secara online.

1. Jangan Tergiuir dengan Barang yang Murah

Jangan Tergiuir Harga Murah via blogspot.com

Harga barang yang sangat murah menjadi salah satu strategi penipuan untuk memancing korbannya. Hal ini yang perlu kita waspadai. Jangan muda tergiur dengan tawaran harga yang sangat murah atau tidak masuk akal. Kita harus terlebih dahulu memastikan produk dan penjual yang menawarkan barang tersebut. Akan lebih baik lagi jika kita dapat memilih penjual yang memang sudah terpercaya sehingga transaksi yang kita lakukan benar-benar tidak berisiko. Situs polisionline.com juga tersedia untuk membantu kita dalam memilih toko online, jika nantinya

terjadi penipuan oleh pihak toko online maka pihak polisionline lah yang akan bertanggung jawab karena mereka bertugas untuk memverifikasi toko online yang sudah terdaftar.

2. Simpan dengan Baik Segala Bukti dan Transaksi

Ada baiknya jika kita menyimpan segala bukti yang berkaitan dengan transaksi online seperti bukti percakapan melalui SMS atau juga bukti transfer kita. Kita disarankan untuk menyimpan segala bukti tersebut hingga barang yang kita pesan sudah berada di tangan kita sehingga kita dapat mengantisipasi apabila seandainya menjadi korban penipuan.

3. Jangan Berpatokan pada Testimoni



Jangan Mengandalkan Testimoni via health.com

Melihat testimoni memang menjadi salah satu jawaban agar kita dapat memilih toko atau penjual yang terpercaya. Tetapi, saat ini juga sulit untuk mengandalkan testimoni. Para pelaku kejahatan sekarang mulai pintar membuat testimoni palsu sehingga calon korban mereka akan mudah terlena dan dapat ditipu. Jadi kita harus lebih cermat lagi dalam mencari testimoni.

4. Minta Foto Barang Asli

Pengiriman barang yang tidak sesuai dengan aslinya juga menjadi salah satu cara penipu dalam menjebak korbannya. Bahkan, dalam beberapa kasus si penipu tersebut tidak mengirimkan barang yang di pesan dan hanya mengirimkan kardus kosong kepada si pembeli. Maka dari itu, kita sangat perlu memeriksa gambar dari barang yang akan kita beli dengan meminta foto barang asli lebih dari satu. Karena, penipu bias saja mengambil gambar tersebut dari Google.

5. Selalu Utamakan COD (Cash on Delivery)



Usahakan Melakukan COD via wordpress.com

Cash on Delivery (COD) menjadi salah satu metode transaksi online yang sangat disarankan. Ketika berbelanja online, usahakan kita dapat mencari toko atau penjual yang dekat dengan lokasi kita. Dengan demikian, kita dapat melakukan COD atau bertemu langsung dengan si penjual sehingga kita juga dapat mengecek barang yang kita beli dan meminimalisir tindak penipuan.

6. Menggunakan Jasa Pihak Ketiga

Jika melakukan COD memang tidak memungkinkan bagi kita, maka sebaiknya kita menggunakan jasa pihak ketiga untuk memfasilitasi transaksi kita dengan penjual. Pihak ketiga yang dimaksud di sini adalah jasa Rekening Bersama atau yang biasa kita sebut dengan Rekber. Jasa rekber nantinya akan berfungsi untuk menjaga transaksi kita tetap aman, namun tentu saja dalam menggunakan jasa ini Anda perlu mengeluarkan sedikit biaya. Dengan melakukan transaksi melalui Rekber, transaksi kita dapat menjadi lebih aman karena uang yang kita bayarkan akan ditahan terlebih dahulu oleh pihak rekber dan dicairkan kepada penjual apabila barang telah kita terima. Tokopedia adalah salah satu contoh dari rekber ini.

7. Meminta Nomor Resi Pengiriman



Mintalah Resi Pengiriman Pesanan Anda via momycozy.com

Nomor resi adalah bukti nomor barang yang akan dikirimkan kepada kita melalui jasa ekspedisi pengiriman barang. Kita dapat meminta secara langsung nomor resi kepada penjual ketika mereka telah mengirimkan barang yang kita beli. Kita dapat segera mengeceknya di situs jasa ekspedisi yang digunakan oleh penjual dan mengeceknya secara berkala

hingga barang tersebut sampai di tangan kita. Jika penjual tidak dapat memberikan nomor resi tersebut, maka kita wajib mencurigai penjual tersebut sebagai penipu karena perilaku tersebut juga merupakan ciri-ciri seorang penipu. Biasanya penipu akan berdalih dengan sejuta alasan untuk mengulur-ulur waktu pengiriman resi lalu akhirnya menghilang.

8. Minta Rekomendasi Teman Kita

Kita juga dapat meminta rekomendasi rekan atau kerabat yang sudah berpengalaman dalam berbelanja online. Dengan begitu, teman kita akan memberitahukan toko online mana saja yang terpercaya berdasarkan pengalaman teman kita ketika berbelanja online sebelumnya.

9. Meminta Nomor Rekening Bank Berbeda



Kita dapat memastikan penjual atau toko online memiliki beberapa nomor rekening dengan nama yang sama untuk menghindari penipuan dalam berbelanja online. Sebagai contoh, jika penjual memberikan nomor rekening BCA, kita dapat menanyakan nomor rekening lain dan mengeceknya apakah memiliki nama pemilik yang sama. Apabila berbeda, kita patut mencurigainya.

Setelah meminta beberapa nomor rekening yang berbeda, periksa nomor rekening tersebut apakah pernah melakukan penipuan. Caranya

adalah dengan mengetikkan nomor rekening dan juga nama pemilik rekening tersebut di Google. Bila nomor rekening tersebut pernah terindikasi melakukan penipuan, kita harus membatalkan transaksi tersebut.

10. Waspada Metode pembayaran Tak Lazim

Contoh modus lain dari kasus penipuan belanja online adalah metode pembayaran yang tidak lazim. Apabila kita menemui penjual yang menawarkan metode pembayaran seperti membayar dengan pulsa, atau menggunakan jasa pos, lewat bitcoin wallet, dan semacamnya, segera batalkan transaksi tersebut. Karena, hal tersebut sangat mencurigakan dan kita juga berpotensi menjadi korban penipuan. Selalu gunakan metode transaksi yang terpercaya seperti yang sudah dijelaskan di atas.

KEAMANAN SIBER DI BIDANG FINTECH



Kemudahan dalam bertransaksi di zaman sekarang juga dilakukan secara digital. Hal ini yang sering dijumpai dengan “cashless transaction” atau transaksi non-tunai. Melalui transaksi ini, kita tidak perlu repot-repot mengambil uang tunai di ATM. Biasanya kita hanya perlu mengisi ulang saldo ke akun pembayaran digital yang kita gunakan seperti GoPay, OVO, dan semacamnya. Sehingga, kita dapat melakukan transaksi secara online maupun offline dengan lebih mudah. Kendati demikian, segala tindak kejahatan tetap mengintai. Maka dari itu, kita perlu memper-

hatikan beberapa hal jika memiliki akun pembayaran digital. Berikut beberapa tipsnya.

1. Jangan beritahukan kode akses/nomor pribadi *Personal Identification Number* (PIN) kepada orang lain.
2. Jangan mencatat dan menyimpan kode akses/nomor pribadi *SMS banking* di tempat yang mudah diketahui orang lain.
3. Selalu periksa setiap transaksi yang kita lakukan secara teliti sebelum melakukan konfirmasi.
4. Setiap kali melakukan transaksi, tunggu beberapa saat hingga menerima respon balik atas transaksi tersebut.
5. Ketika melakukan transaksi, pastikan kita akan menerima pesan notifikasi atas transaksi berupa SMS atau email yang akan tersimpan di dalam *inbox* (*bukan spam*). Segera periksa ulang secara teliti isi dari notifikasi tersebut dan segera kontak ke pihak terkait jika terdapat hal-hal yang mencurigakan dalam transaksi.
6. Jika kita merasa PIN kita diketahui oleh orang lain, segera lakukan penggantian PIN.
7. Jika kita kehilangan SIM card, baik hilang/dicuri/dipindahtangkan kepada pihak lain, segera beritahukan ke pihak terkait dengan menghubungi call center resmi.
8. Hati-hati dengan aplikasi di internet yang merupakan *spam* atau *malware* yang mungkin dapat mencuri data-data pribadi kita untuk disalagunakan.
9. Kita disarankan tidak melakukan transaksi internet di tempat umum seperti warnet, WIFI gratis, dan semacamnya. Karena, data-data yang ada di gadget kita berpotensi dicuri oleh pihak

10. Jika diperlukan, jangan lupa melakukan proses *log out* setelah selesai melakukan transaksi digital dengan akun-akun khusus seperti transaksi *internet banking*.
11. Jika berganti ponsel, pastikan bahwa semua data-data kita sudah dihapus untuk menghindari penyalahgunaan oleh pihak lain yang menggunakan ponsel tersebut di kemudian hari.

Indonesia adalah salah satu negara dengan pengguna internet terbesar. Berdasarkan penelitian yang dilakukan oleh We Are Social, orang Indonesia menghabiskan 3 jam 23 menit dalam sehari

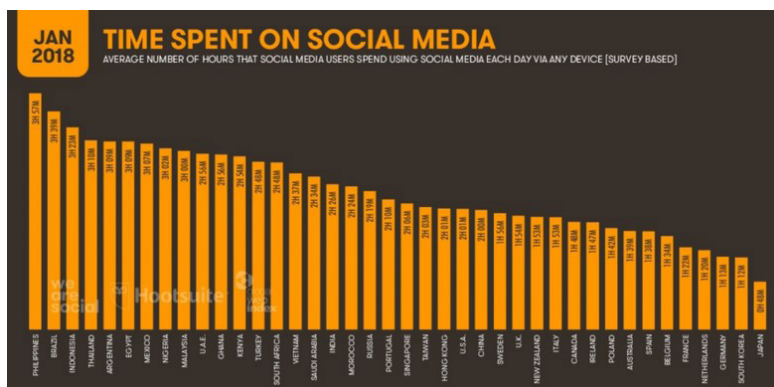


Persentase rata-rata orang Indonesia menghabiskan waktunya untuk mengakses media sosial

69

Media sosial menjadi primadona tersendiri bagi masyarakat Indonesia. Aplikasi media sosial yang paling banyak diunduh adalah Whatsapp, Facebook, Instagram, dan Line. Facebook merupakan media sosial paling banyak dikunjungi dengan capaian lebih dari 1 miliar juta pengunjung per bulan. Rata-rata pengunjung Facebook menghabiskan waktu 12 menit 27 detik untuk mengakses jejaring sosial tersebut. 92 persen mengakses Facebook menggunakan perangkat mobile dengan persentase gender 56 persen pria dan 44 persen wanita. Pengguna Facebook didominasi golongan usia 18-24 tahun. Total pengguna aktif Instagram bulanan di Indonesia mencapai 53 juta dengan persentase 51 persen pria dan 49 persen wanita. (Kompas.com, 2018)

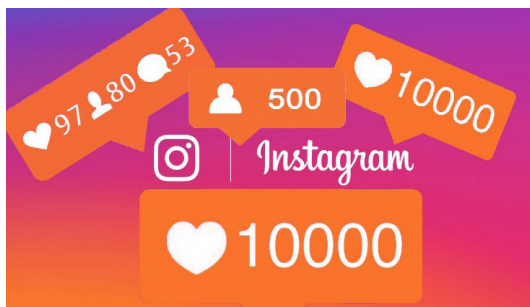
Bahaya yang mengintai pengguna media sosial di Indonesia



ilustrasi: jurnas.com

Orang Indonesia yang keranjingan media sosial banyak yang tidak menyadari pentingnya menjaga keamanan. Jika tidak memperhatikan keamanan, maka akan banyak potensi celah yang dapat dimanfaatkan penjahat siber untuk memperoleh keuntungan. Inilah hal yang kurang diperhatikan pengguna media sosial di Indonesia. (Genmuda.com, 2016)

1. Menerima Followers atau Permintaan Pertemanan dari Orang Tak Dikenal



Ilustrasi: alona.co.id

Menambah *followers* atau mencari teman baru adalah hal yang wajar. Tetapi perlu diperhatikan itu sama saja mengizinkan orang asing untuk mengakses informasi pribadi media sosial. Survei dari Kaspersky Lab menyatakan 31 persen pengguna akan menerima koneksi dari orang yang mereka tidak kenal. Hal itu jelas akan membuka kemungkinan terhadap lebih banyak orang yang tidak dikenal, bahkan pelaku kejahatan dunia maya untuk masuk ke dalam kehidupan.

2. Tidak hati-hati dalam mengklik tautan



Ilustrasi: mediababe.net

Berbagi tautan gambar dan video lucu memang terbilang wajar di kalangan pengguna media sosial. Meski begitu, kita harus tetap waspada ketika menerima tautan dari orang yang tidak begitu dikenal dan terlihat mencurigakan. Riset dari Kaspersky Lab juga mengatakan bahwa 26% pengguna akan langsung membuka tautan yang mereka terima tanpa ragu.

3. Membagi informasi Pribadi



Ilustrasi Newsketstech.com

Menurut Kaspersky Lab, 30 persen pengguna jejaring sosial yang terlibat dalam riset ternyata sudah pernah berbagi postingan, check-in, dan informasi lainnya tidak hanya kepada teman-teman mereka, tapi juga ke semua orang yang online. Hal itu tentu akan membuka pintu bagi pelaku kejahatan dunia maya untuk melancarkan aksinya tanpa disadari oleh pengguna tersebut.

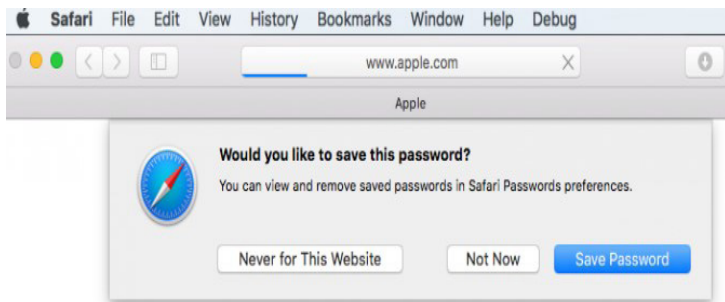
4. Mengesampingkan Aturan Privacy



Ilustrasi: wonderboustours.com

Meskipun 78 persen pengguna internet memiliki akun media sosial, survei menunjukkan kurangnya kesadaran di antara pengguna media sosial. Satu dari sepuluh (9%) responden survei tidak berpikir orang di luar daftar teman-teman mereka bisa melihat halaman dan posting mereka, sehingga mudah bagi informasi pribadi mereka jatuh ke tangan yang salah, atau bahkan digunakan oleh penjahat untuk pencurian identitas dan penipuan keuangan. Jika ada rincian, foto, status, atau informasi lain yang kita tidak ingin orang-orang tahu, pastikan kita memakai pengaturan privasi yang disediakan masing-masing media sosial. Jika tidak mengerti, pastikan membaca FAQ yang tersedia dalam masing-masing media sosial.

5. Password yang sama dan disimpan web browser



Ilustrasi: laptopmag.com

Memiliki password yang sama dalam setiap media sosial membawa kemudahan dalam mengingat. Dalam setiap web browser juga disediakan fitur untuk mengingat password. Hal ini tentu akan membantu aktivitas media sosial agar lebih mudah. Akan tetapi, perlu diperhatikan juga bahwa web browser kita dapat dihack oleh orang yang tak bertanggung jawab. Oleh karena itu perbarui password secara berkala dan jangan simpan di web browser. Bagaimana cara membuat password yang aman? Hal tersebut sudah dibahas pada bab sebelum ini.

Jadilah pengguna media sosial yang cerdas dengan tidak membuka profil dan informasi pribadi kita. Termasuk juga harus berhati-hati dengan siapa saja yang dikenal melalui media sosial. Karena namanya manusia, kita tidak pernah tahu orang punya niat apa saja.

Berbagai Kejahatan yang ada di media sosial

1. Penipuan berkedok jual beli online



Penipuan jual beli tidak hanya terjadi di dunia nyata, tetapi terjadi juga di dunia maya. Penipuan yang dilakukan lewat media sosial sudah sangat umum terjadi.

Modus:

Harga barang sangat murah

Menawarkan produk yang belum tersedia di pasaran

Memuat nomor resi palsu

Memuat testimoni palsu

Sekilas Cerita

Melvi seorang warga Kelurahan Rejosari, Pekanbaru kesal karena keinginannya memiliki lemari pakaian jati kandas. Kejadiannya bulan Juli lalu. Saat itu ia memesan lemari jati melalui akun jual beli online di media sosial Facebook. Namun setelah uang ditransfer sebesar Rp 2,7 juta, lemari yang ia pesan tidak kunjung datang. Ia tergiur karena penawarannya cukup meyakinkan. Setelah saling berkomunikasi melalui chat di Facebook, ia pun mentransfer uang sesuai harga ditambah dengan biaya pengiriman.

Melvi mulai khawatir karena barang yang dipesan tidak kunjung datang. Ia pun menelusuri keberadaan akun Facebook tersebut dan ternyata sudah banyak yang mengaku menjadi korban. Anehnya, akun tersebut tetap eksis dan terus menawarkan produk baru, seakan tak takut dan berdosa telah menipu banyak orang. Melvi kini hanya bisa pasrah. Ia memilih tak melaporkannya ke polisi. Sebab ia yakin alamat di akun Facebook tempat ia memesan lemari itu palsu.

Sekilas Tips

Teliti harga dan barang. Jika barang yang ditawarkan jauh lebih murah dibandingkan harga normal, lebih baik tidak dibeli. Karena berpotensi kualitas barang tidak baik atau bahkan penipuan.

Cari penjual toko online yang terpercaya, dengan review asli yang positif

Gunakan marketplace yang menawarkan rekening bersama. Artinya uang tidak langsung masuk ke penjual

Usahkan melakukan Cash on Delivery (COD) untuk lebih puas mengecek barang agar tidak merasa tertipu

2. Pembajakan akun media social



Ilustrasi: pymnts.com

Pembajakan atau pembobolan akun media sosial merupakan kejahatan siber yang sudah sering terjadi. Biasanya hal ini dilakukan oleh orang yang memiliki kemampuan IT yang tinggi dan targetnya bukan orang biasa, tetapi artis, pejabat, akun resmi pemerintah, pemimpin perusahaan, dan lainnya. Tujuan pembajakan akun media sosial ini biasanya untuk meminta tebusan sejumlah uang atau hanya untuk mengambil alih akun media sosial tersebut sehingga pembajak bisa leluasa menebar propaganda melalui akun media sosial yang berhasil mereka bajak.

Sekilas Cerita

Pada 5 Juni 2016, CEO Facebook Mark Zuckerberg menjadi target pembajakan. Pelaku pembajakan yang menyebut dirinya OurMine Team ini menemukan kata kunci akun Twitter dan Pinterest milik Zuckerberg dari pembobolan data LinkedIn. Lucunya, walau Facebook menyarankan menggunakan berbagai macam kombinasi huruf dan angka sebagai kata kunci, Zuckerbergh malah hanya memakai kata “dadada” sebagai kunci akunnya sendiri.

Tak lama setelah peristiwa itu, perusahaan keamanan Symantec melaporkan adanya peretas yang membajak akun-akun Instagram dan mengubah profil penggunanya dengan gambar sensual. Tujuannya untuk menarik pengguna lain ke situs kencan dewasa dengan iming-iming dibagikan foto bugil perempuan dan ditawarkan seks kilat. Tautan yang ada di profil pengguna yang dibajak akan mengarahkan pengguna lain ke situs perantara yang telah dikendalikan scammer.

Instagram akhirnya membuat otentikasi dua faktor atau two-factor authentication untuk para penggunanya. Fitur keamanan akun ini berfungsi untuk mencegah scammer mengambil alih akun. Sayangnya, walau berbagai macam perlindungan telah diterapkan Facebook maupun Instagram, pembajakan-pembajakan akun media sosial masih sering terjadi. Yang sedang marak adalah pembajakan akun-akun para selebgram dengan ribuan pengikut.

Sekilas Tips

1. Gunakan kunci ganda yang disediakan dengan verifikasi melalui email atau telepon
2. Perhatikan url ketika login, bisa aja itu berupa phishing
3. Jangan sembarang memasukan login dan password
4. Gunakan alamat email dan password yang berbeda
5. Ganti password secara berkala dan kombinasi password seperti yang sudah dijelaskan pada bagian sebelum ini

3. Penculikan dan Pemerkosaan



Ilustrasi:merdeka.com

Aksi penculikan atau pemerkosaan tidak bisa terjadi secara langsung di media sosial tetapi media sosial menjadi perantara dalam melakukan aksi kejahatan tersebut. Modus yang digunakan pelaku kejahatan bervariasi, misalnya saja dengan menghubungi pengguna media sosial lain dengan maksud berteman, atau menawarkan pekerjaan atau imbalan sehingga korban pun merasa tertarik dan terbujuk hingga sampai mereka bertemu langsung dan si penjahat pun bisa dengan mudah melakukan aksinya.

Sekilas Tips

Kejadian penculikan yang berujung pemerkosaan dengan perantara sosial media bukan satu dua kali terjadi. Kasus seperti ini biasanya diawali dengan perkenalan melalui media sosial tertentu. Menjalinkan hubungan di media sosial hingga akhirnya bertemu di dunia nyata. Identitas yang tidak dapat 100% dipastikan dari hasil perkenalan di media sosial ini akhirnya berujung pada tindak penculikan hingga pemerkosaan.

Berkaca dari kasus terkait, masyarakat membutuhkan kewaspadaan yang lebih seiring berkembangnya teknologi. Dengan teknologi semua urusan lebih mudah dan cepat. Bahkan untuk urusan bertemu jodoh.

Namun, masyarakat harus lebih bijak dalam menggunakannya. Hal ini dikarenakan kemudahan yang ditawarkan tersebut juga sering dilihat sebagai kesempatan oleh para pelaku kejahatan. Salah satu bentuk kejahatan yang menggunakan kesempatan ini adalah penculikan dan pemerkosaan.

Oleh karena itu, saat kita berkenalan dengan seseorang melalui media sosial, ada baiknya kita lebih berhati-hati. Telusuri lebih lanjut tentang identitasnya sebelum kita memutuskan untuk bertemu secara langsung. Saat pertama kali bertemu, ada baiknya kita mengajak teman saat menemui orang yang baru kita kenal tersebut.

3. Prostitusi Online



Ilustrasi: 123rf.com

Prostitusi online adalah salah satu kejahatan melalui media sosial yang sempat menghebohkan media sosial di Indonesia. Modus yang digunakan pun bervariasi dan dengan cara yang bermacam-macam, misalnya mengupload foto vulgar atau dengan menggoda pengguna media sosial lain dengan kata-kata manis dan rayuan sehingga pengguna media sosial lain pun tertarik dan masih banyak lagi modus-modus lainnya. Pelaku kejahatan

prostitusi online juga beragam, bahkan salah satu kasus terpopuler menyangkut sederet artis papan atas.

Sekilas Tips

1. Perlunya pendidikan seksual sejak dini
2. Pemerintah bangun pusat kreativitas agar bakat tersalurkan
3. Pendidikan bermedia sosial agar tak sebar konten porno
4. Penyempurnaan Undang-undang yang melarang prostitusi, terutama prostitusi online
5. Sosialisasi Internet Sehat

4. Cyber bullying

Bullying merupakan salah satu tindak kejahatan yang sering terjadi baik disadari maupun tidak disadari. Perilaku ini dapat berupa tindakan fisik maupun verbal yang berakibat menurunkan semangat belajar pada seseorang bahkan bisa berujung pada tindakan yang fatal. Dengan perkembangan teknologi yang maju, kita tidak perlu bertatap muka dengan seseorang karena kita mampu berkomunikasi dengan cepat dan praktis. Akan tetapi, hal tersebut sering disalahgunakan dan membawa hal negatif yaitu cyberbullying (Cahyani, 2018).



Pelaku cyberbullying memanfaatkan teknologi informasi yang memungkinkan mereka untuk langsung menjangkau korbannya. Tidak perlu bertatap muka dan sulit dilacak kembali. Perilaku cyberbullying dapat dilakukan oleh siapa saja dan dimana saja. Cyberbullying bisa dilakukan dengan mudah oleh seseorang yang kerap berkomentar negatif lewat media sosial. Tetapi sayangnya memiliki efek yang besar karena kemajuan teknologi memungkinkan informasi yang diterima secara cepat dan luas (Cahyani, 2018).

Adapun faktor penyebab seseorang melakukan *cyber bullying* adalah:

1. Kesal

Perasaan kesal terhadap seseorang membuat orang tersebut melakukan bully melalui media sosial.

2. Karakter seseorang

Seseorang yang mudah untuk mengungkapkan amarahnya akan dengan mudah juga melontarkan kata-kata kasar atau negatif melalui media sosial.

3. Adanya akses

Cyberbullying melalui media sosial diperlukan akses berupa koneksi internet dan akun media sosialnya termasuk Instagram, Facebook, Twitter, sampai Snapchat. Semakin mudah seseorang mendapatkan dan mengakses hal tersebut, maka semakin besar juga kesempatan seseorang untuk melakukan cyberbullying.

4. Ikut-ikutan

Hal ini kerap terjadi karena pergaulan lingkungan sekitar yang sering melakukan cyberbullying yang mengakibatkan orang tersebut menjadi terpengaruh untuk melakukan hal yang sama.

Sekilas Info



Sumber : Serambi Indonesia 2018

Kasus *cyberbullying* kembali ramai belakangan ini. Nama Bowo Alpenliebe mungkin sudah tidak asing di telinga kita. Bowo Alpenliebe adalah anak 13 tahun yang mulai dikenal setelah aksinya melalui aplikasi Tik Tok dengan pengikut mencapai 700 ribu orang. Dalam video Tik Tok, Bowo terlihat ganteng dan menggemaskan. Gambaran ini membuat banyak remaja perempuan yang tergila-gila dengannya.

Popularitas Bowo Alpenliebe di Tik Tok mendorong Bowo menggelar Meet and Greet yang berujung pada komentar negatif netizen yang menyerang akun sosial media-nya dengan kata-kata yang tidak pantas diucapkan.

Kejadian penindasan di sosial media seperti yang terjadi pada Bowo bisa menjadi sangat membahayakan karena kita tidak tahu perkataan atau komentar yang ditujukan hanya bercanda atau bullying sekedar marah dan gimmick belaka. Sebab bullying memberikan efek yang tidak baik pada korban. Mungkin saat kita secara sengaja atau tidak sengaja melakukan *bullying* di media sosial, kita tidak merasakan dampaknya secara langsung terhadap korban. Tetapi hal tersebut sangat beresiko mengganggu keadan psikis mereka.

Sekilas Tips

Beberapa tips untuk mencegah dan menghentikan cyberbullying:
(Cahyani, 2018)

1. Jangan bereaksi

Pelaku bullying selalu menunggu reaksi korban. Maka jangan terpancing untuk merespons aksi pelaku agar mereka tidak merasa diperhatikan.

2. Jangan membalas aksi pelaku

Membalas apa yang dilakukan pelaku cyberbullying akan membuat kita ikut menjadi pelaku

3. Segera blokir aksi pelaku

Jika pengganggu muncul dalam bentuk pesan, teks, atau komentar profil, gunakan tool privasi untuk memblokir pelaku.

4. Selalu berperilaku sopan di dunia maya

Berperilaku yang baik layaknya di dunia nyata. Perilaku buruk yang dilakukan, seperti membicarakan orang lain, bergosip, atau memfitnah, akan meningkatkan risiko seseorang menjadi korban cyberbullying.

5. Jangan hanya diam

Ikut meneruskan pesan fitnah atau hanya diam dan tidak berbuat apa-apa akan menyuburkan aksi bullying dan menyakiti perasaan korban. Suruh pelaku menghentikan aksinya, atau jika pelaku tidak diketahui bantu korban menenangkan diri dan laporkan kasus tersebut ke pihak berwenang.

Kiat-Kiat Keamanan di Sosial Media:

Kiat-Kiat Keamanan di Whatsapp



Mematikan Laporan Dibaca

Memilih apakah seseorang dapat melihat jika Anda telah membaca pesan orang tersebut.



Menghapus dan Melaporkan Spam

Melaporkan spam dari dalam aplikasi.



Meminta Info Akun

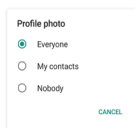
Mendapatkan laporan informasi dan setelan akun WhatsApp Anda.

[Pelajari selengkapnya](#)



Membersihkan Pesan di Dalam Chat

Menghapus semua pesan di dalam chat dari individual atau grup, atau semua chat sekaligus.



Mengendalikan Setelan Privasi Anda

Menyetel foto profil, terakhir dilihat, dan info, agar dapat dilihat oleh semua orang, hanya kontak, atau tidak seorang pun.



Memblokir Pengguna yang Tidak Diinginkan

Menghentikan seseorang untuk menghubungi Anda secara langsung dari dalam chat.



Meninggalkan Grup

Keluar dari grup kapan saja.

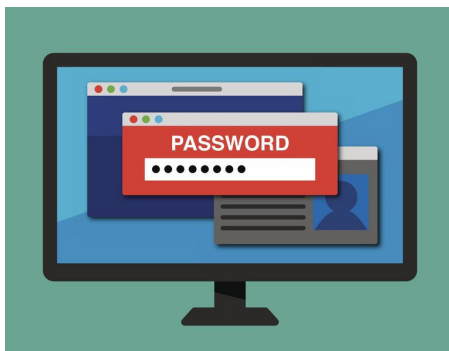
[Android](#) | [iPhone](#) | [Windows Phone](#)



Mengaktifkan Verifikasi Dua Langkah

Membuat pin enam digit untuk mengaktifkan keamanan tambahan.

Kiat Keamanan di Facebook



Sumber: Open Data News Wire 2018

nama kita dan kata-kata umum lainnya. Pelajari cara membuat *password* yang kuat dengan mengkombinasikan berbagai macam karakter dari huruf, angka, hingga tanda baca

1. Lindungi Password

Jangan pernah gunakan *password* Facebook milikmu untuk akses *online* lainnya dan jangan pernah sekalipun membagikannya ke orang lain. *Password* yang kita miliki harusnya sulit untuk ditebak. Hindari penggunaan

2. Jangan pernah membagikan informasi *login* kita

Penipu bisa saja membuat website palsu yang menyerupai facebook hanya untuk mendapatkan informasi *email* dan *pass-word* kita. Selalu cek kembali URL atau halaman website yang tengah kita buka sebelum kita memasukkan informasi login. Jika kita ragu, ketik langsung www.facebook.com ke browsermu untuk menghindari terjadinya *phising*.



Sumber: Yahoo Safety 2018

3. *Log out* dari Facebook saat kita menggunakan komputer bersama

Jika kita lupa untuk keluar dari akunmu di komputer milik bersama, kita masih bisa keluar dari komputer tersebut dengan jarak jauh.

Jangan mereima pertemanan dari orang yang kita tidak kenal

Penipu bisa saja membuat akun palsu yang sewaktu waktu bisa saja memberi peluang untuk memanfaatkanmu dan menjadikan kita korban kejahatan siber.



Sumber: Dreamstime 2018



Sumber: Lifewire 2018

4. Hati-hati dengan perangkat lunak berbahaya

Kenali tanda dari komputer atau perangkat yang terinfeksi virus atau perangkat lunak berbahaya. Selalu *update* perangkat browsermu dan hapus aplikasi yang mencurigakan.

5. Jangan pernah meng-klik tautan yang mencurigakan

Meskipun tautan tersebut berasal dari teman atau perusahaan yang kita kenal. Kita harus lebih cermat memahami dan menerka apa isi didalamnya. Perlu diingat bahwa Facebook tidak akan pernah meminta kata sandi kita dalam bentuk email. Jika kita melihat tautan mencurigakan di Facebook, laporkanlah.



Sumber: Mythemeshop, 2018

6. Gunakan fitur keamanan ekstra

Misalnya, kita dapat memperoleh pemberitahuan tentang proses masuk yang tidak dikenal, menyiapkan autentikasi dua faktor, atau memilih teman untuk menjadi kontak tepercaya kita. Jika kita masuk ke Facebook melalui komputer, kita juga dapat menggunakan Pemeriksaan Keamanan untuk meninjau pengaturan keamanan yang kita miliki.

Selain dengan menerapkan kiat-kiat keamanan di platform seperti Whatsapp dan Facebook diatas, kita juga perlu memperhatikan konten yang kita posting. Desy Widya Ningrum melalui inet.detik.com membagikan 7 hal yang pantang kita posting di media sosial:

1. Informasi pribadi yang bisa mengarah ke pencurian identitas

Ingatkan teman, anak, dan siapapun yang kita kenal untuk tidak memajang semua informasi pribadi, seperti tanggal lahir secara lengkap, termasuk alamat rumah dan nomor telepon. Karena dapat mengundang pencurian identitas.

2. Informasi keluarga

Masalah keluarga seharusnya tidak perlu diumbar ke publik. Nama lengkap ayah dan ibu, begitupun dengan berbagai informasi terkait keluarga kita, akan lebih baik jika kita simpan di ranah privat.

3. Masalah Pribadi

Hidup dengan segala masalah persahabatan dan drama percintaan adalah hal yang biasa. Tapi tidak tepat jika masalah itu diumbar ke media sosial, karena seluruh dunia bisa membacanya. Jangan sampai kesedihan dan gundah gulana kita justru dimanfaatkan orang lain dan menjadi boomerang bagi kita sendiri.

4. Foto dengan geotag

Remaja saat ini suka narsis dengan berfoto selfie. Demam selfie ini sayangnnya tidak disertai kesadaran bahwa pada foto-foto sering terdapat data tentang lokasi foto diambil. Karena itu pastikan kita menonaktifkan opsi GPS tag dalam pengaturan kamera sebelum memposting foto pribadi ke publik.

5. Di rumah sendirian

Jangan posting info seperti ini secara online. Jangan pula memposting rencana pribadi tentang kemana kita akan pergi dan bersama siapa karena bisa saja hal ini mengundang kejahatan.

6. Foto-foto yang tidak pantas

Terkadang kita sering memposting foto-foto narsis yang tidak layak dikonsumsi publik, misalnya yang mengandung unsur seksualitas, atau foto yang menggambarkan mereka yang terlibat dalam perilaku yang tidak pantas. Foto-foto hasil korban kecelakaan juga selayaknya tidak kita posting di sosial media, loh ya!

7. Komentar kasar

Gunakan kata-kata yang baik saat mengomentari postingan orang lain, jangan pernah memposting sesuatu yang dapat menyakiti orang lain.

BAB III

Cara Pintar untuk Aman di Dunia Siber

Kedekatan kita dengan internet saat ini mengharuskan kita untuk dapat berperilaku dengan pintar agar tetap aman di dunia siber. Dari berbagai penjelasan di atas setidaknya kita dapat mengklasifikasikan cara pintar untuk aman di dunia siber melalui tiga perspektif, yakni dari segi pengguna, perangkat dan akses.

CARA PINTAR UNTUK PENGGUNA

Dalam beraktivitas di dunia siber, ada beberapa hal yang tidak dapat dilewatkan sebagai pengguna internet. Saat kita mencoba masuk dan menggunakan sebuah aplikasi, mengakses mobile banking, berselancar di sosial media, permintaan terhadap email dan password pasti akan menjadi syarat utama sebelum kita masuk sebagai pengguna. Oleh karena itu, menjadi pengguna yang pintar juga berarti menjadi pengguna yang paham dengan betul mengenai dua gerbang utama di dunia siber, memahami penggunaan password dan email.



Memperkuat Password

Keamanan password merupakan salah satu hal penting dalam keamanan berinternet. Password berasal dari kata pass yang berarti izin, dan word yang berarti kata. Maka dari itu



password adalah kata yang digunakan untuk izin dalam melewati sesuatu. Berdasarkan istilah dalam teknologi informasi, password dapat diartikan sebagai deretan karakter yang dimasukan untuk mendapatkan akses terhadap fisik aplikasi ataupun sistem komputer. Sampai saat ini belum ada teknologi yang dapat menggantikan password. Oleh karenanya, menjaga password agar selalu aman dan rahasia adalah sebuah keharusan.

1. Panjang minimal delapan karakter yang merupakan kombinasi huruf besar, kecil, angka, serta karakter khusus yang tidak berurutan atau mengandung makna umum yang mudah ditebak. Hindari penggunaan nama dan tanggal lahir.

Contoh:

17Agustus1945 memenuhi syarat aman tapi mudah ditebak

54!auystge77 memenuhi syarat aman dan sulit ditebak

2. Ganti password secara rutin minimal selama 3 bulan sekali dengan pola unik yang dipahami sendiri
3. Gunakan password yang berbeda untuk setiap aplikasi layanan. Karena sulit untuk mengingatnya, maka wajib menggunakan aplikasi password management, seperti

- KeePassX: Tersedia untuk GNU Linux, Windows dan Mac OS X.
 - [KeePassDroid](#): Tersedia untuk Android.
 - [MiniKeePass](#): Tersedia untuk iPhone.
 - [KeePass](#): Tersedia untuk Windows dan GNU/Linux.
 - [1Password](#): Tersedia untuk Mac OS X, Microsoft Windows, iPhone dan iPad.
4. Jika layanan atau aplikasi yang digunakan menyediakan fitur two factor authentication, baik menggunakan code via SMS ke nomor telepon atau aplikasi token, aktifkan dan selalu gunakan.
 5. Wajib memiliki dan gunakan alamat email khusus yang dirahasiakan untuk keperluan password recovery
 6. Saat ini kecenderungannya satu aplikasi seperti google, facebook dan twitter menjadi layanan *open authentication* juga. Sehingga aplikasi tersebut digunakan sebagai akun universal untuk login ke aplikasi dan layanan lainnya. Jika memang menggunakan hal ini, maka syarat password yang kuat, two factor authentication dan email konfirmasi cadangan rahasia adalah syarat mutlak yang harus dilakukan.

Salah satu kesalahpahaman bagi kebanyakan orang terkait password adalah mencoba mengaplikasikan komposisi password yang sederhana agar mudah diingat dan menggunakannya untuk beberapa situs, layanan, dan aplikasi sekaligus. Kebiasaan ini nyatanya memberikan peluang untuk menjadikan kita sebagai korban dari kejahatan siber, karena sekali peretas dapat mengakses satu akun pribadi milik kita, maka dia dapat mengakses berbagai akun dengan password yang sama. Oleh karena itu, menggunakan *password manager* agar dapat membuat *password* unik untuk tiap situs yang digunakan dan menggunakan *two factor au-*

thentication dapat menjadi solusi yang tepat untuk dapat memperkuat password agar dapat beraktivitas lebih aman di dunia siber.

Menggunakan Email

Email dapat dikatakan sebagai gerbang utama dalam berselancar di internet. Memiliki email seakan tiket yang harus dimiliki sebelum kita dapat mengakses berbagai layanan lain di dunia siber. Oleh sebab itu, menggunakan email dengan pin-tar juga harus menjadi agenda utama agar dapat tetap aman saat beraktivitas di dunia maya.

Salah satu tips dalam penggunaan email adalah dengan menggunakan layanan yang menyediakan perlindungan protokol akses yang aman (SSL/TLS) disertai anti-spam, anti-phising, dan antivirus. Penyedia layanan populer seperti GMAIL biasanya sudah memberikannya secara default, namun umumnya pengguna harus mengkonfigurasikannya secara manual (optional) terlebih dulu. Pastikan semua fitur in tersedia, terutama jika menggunakan email sendiri dari perusahaan atau organisasi.



Menghindari Phishing

Salah satu jalur penipuan yang sering terjadi di dunia siber adalah *phishing*. Metode ini cenderung lebih sederhana dari kejahatan siber lainnya, tapi cukup berbahaya. Disaat kejahatan siber lain, seperti peretasan, dapat dicegah

dengan implementasi keamanan yang baik, *phishing* lebih sulit ditangkal karena memanfaatkan kelalaian pengguna sekaligus korban. Pengguna yang menjadi korban *phishing* akan “dipancing” untuk memberikan data-data penting pada pelaku kejahatan. Bila sudah terjaring, pelaku dapat mencuri akses ke akun korban, menimbulkan kekacauan, bahkan kerugian materil.

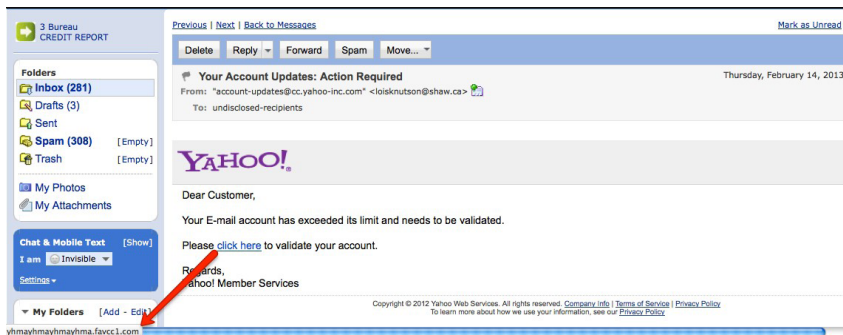


Sumber: Ambergis Today 2018

Pesan phishing biasanya memiliki ciri-ciri sebagai berikut (Mustofa, 2018):

- **Berasal dari sumber yang terlihat resmi.** Pelaku phishing akan mendesain pesannya sehingga tampak seolah-olah berasal dari perusahaan sungguhan.
- **Membangkitkan emosi.** Emosi ini bermacam-macam wujudnya. Bisa rasa panik, khawatir, gembira, bahkan kasihan.
- **Mengandung tautan atau lampiran.** Setiap kali kamu menerima pesan berisi tautan, jangan serta-merta mengkliknya sebelum yakin benar bahwa sumbernya terpercaya.
- **Meminta mengisi data tertentu,** misalnya username dan password, nomor kartu kredit, dan sebagainya.

Dari beberapa poin diatas, poin nomor dua adalah poin terpenting yang harus diawasi, karena pelaku *phishing* biasanya sangat pandai menciptakan kata-kata yang membuat korbannya tidak bisa berpikir jernih. Bila melihat pesan berbunyi, “Komputer Anda terjangkit virus xxxxx!” atau “Selamat anda memenangkan undian xxx” jangan langsung percaya. Agar dapat menghindari diri menjadi korban *phishing* Ayubb Mustufa melalui Tech in Asia menguraikan langkah-langkah pencegahan sebagai berikut:



Sumber: University of Delaware 2018

- **Jangan panik.** Begitu pula bila pesan yang di dapat menggem-birkan, jangan senang dulu. Tahan emosi agar bisa berpikir jernih. Jika pikiran sedang tidak jernih, segera tutup pesan dan membacanya lagi nanti.
- **Cek ulang pengirim.** Perhatikan gambar email phishing di atas. Pada kolom pengirim, tertulis “account-updates@cc.yahoo-inc.com”. Sekilas terlihat valid, bukan? Masalahnya, alamat ini tertulis pada bagian nama pengirim, bukan alamat pengirim. Hal seperti ini perlu di cek kembali dengan teliti. Demikian pula dengan SMS, jangan percaya bila ada orang mengirim pesan “resmi” tapi menggunakan nomor telepon berawalan +628XXXXXX.

- **Jangan mengeklik tautan dan lampiran apapun.** Misalkan email tersebut menyuruh mengisi data tertentu, jangan menggangginya lewat tautan yang disediakan. Buka situs resmi di tab baru, dan ganti data lewat tab itu.
- **Hubungi layanan konsumen resmi.** Jangan ragu-ragu mencari tahu ke sumbernya langsung apakah pesan yang didapatkan itu benar adanya
- **Cari informasi di internet.** Warganet suka membagikan cerita, termasuk cerita tindak kriminal. Bila sebuah praktik phishing sedang marak, kemungkinan ada orang lain yang juga mengalaminya. Sangat direkomendasikan untuk mencari pengalaman orang lain lewat Google untuk referensi agar tidak menjadi korban selanjutnya.

Bila kamu terlanjur terjerat oleh phishing, beberapa langkah yang bisa dilakukan adalah:

- Jangan panik
- Ganti seluruh password dari layanan yang terdampak
- Hubungi customer service resmi dari layanan yang digunakan
- Cek seluruh transaksi yang terhubung dengan akun terdampak

Sederhananya, cara utama menghindari *phishing* adalah dengan tidak mudah percaya pada apa yang dibaca di internet. Secara default, kita harus selalu menaruh rasa curiga terhadap setiap tautan dan lampiran yang diterima. Sesuatu yang terlihat terpercaya belum tentu benar-benar terpercaya. Ini memang terdengar seperti paranoid. Tapi secanggih apapun sistem keamanan, *human error* masih bisa terjadi. Lebih baik waspada, daripada menyesal di kemudian hari, kan?

Mengamankan Kartu ATM, Kartu Debit, dan Kartu Kredit

Berikut tips dan trik aman untuk menghindari kejahatan siber bagi pemegang kartu ATM, kartu debit dan kartu kredit:

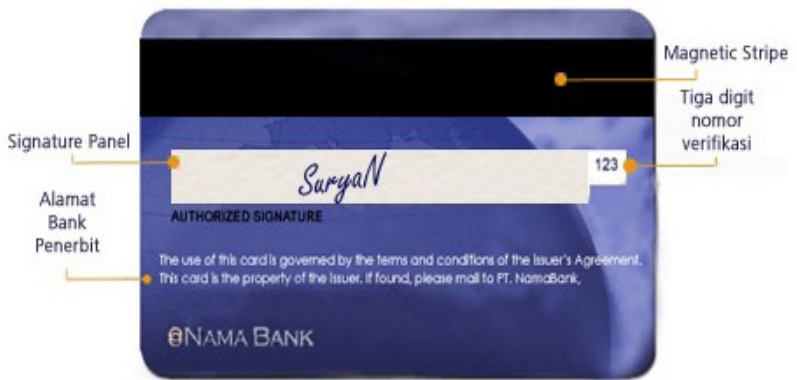
- a. Setiap bentuk fisik kartu ATM/debit/kredit telah menggunakan chip. Oleh karena itu, pastikan kartu debit/kredit telah terpasang chip, jika tidak segera mintakan ke Bank untuk diganti.



Sumber: PilihKartu.com

- b. Setiap kartu ATM/debit/kredit memiliki tiga digit nomor verifikasi di balik kartu yang disebut CVV2 code. Kode ini digunakan untuk melakukan transaksi *online* bersamaan dengan informasi lainnya seperti nomor, *expired date*, dan nama pemegang kartu. Akan tetapi, informasi yang tertera tersebut akan sangat mudah untuk di-*capture* orang lain sehingga mempertinggi risiko penggunaan kartu tersebut untuk transaksi *online* tanpa sepengetahuan pemilik kartu walaupun by default bank sudah mengaktifkan *two factor authentication* dengan mengirimkan kode token via SMS. Sebab, beberapa

merchant mungkin melakukan by pass ketika transaksi dalam jumlah di bawah *threshold* yang masih dijamin oleh asuransi sehingga kelemahan ini akan sangat mudah dimanfaatkan oleh para *hacker*. Oleh karena itu, sebaiknya tutup CVV2 code pada kartu ketika melakukan transaksi *offline*.



Sumber: PilihKartu.com

- c. Salah satu hal yang dapat dilakukan untuk menyimpan kode CVV2 adalah dengan mencatatnya ke dalam aplikasi *password manager* atau dengan menghafalnya.
- d. Ketika bertransaksi secara *offline*, jangan menggesek (*swipe*) kartu debit/kredit di mesin *cash register*. Pastikan selalu transaksi menggunakan otentikasi PIN.
- e. Ketika bertransaksi secara *online*, sebaiknya jangan menyimpan informasi kartu yang digunakan di dalam layanan transaksi *merchant* walaupun hal ini akan mempersulit proses transaksi di waktu lain karena harus mengisi kembali data yang wajib dimasukkan. Hal ini dilakukan

untuk melindungi dan menghindari dari adanya kemungkinan insiden kebocoran data dari *merchant* tempat bertransaksi.

- f. Gunakan perlindungan *anti-magnetic* pada dompet jika menyimpan kartu jenis prabayar/*e-money* bersama-sama atau memiliki kartu debit/kredit yang multifungsi seperti sebagai kartu *e-money* di dalam dompet.



- g. Gunakan kode PIN dengan pola yang unik untuk setiap kartu yang dimiliki. Jangan menggunakan *recycle* pada kode PIN di kartu yang berbeda dan pastikan PIN ini diketahui diri sendiri. Hal ini merupakan salah satu cara pengamanan terbaik dalam membedakan PIN masing-masing kartu

CARA PINTAR UNTUK PERANGKAT

Perangkat juga menjadi komponen penting yang harus diperhatikan agar kita dapat tetap aman di dunia siber karena kejahatan siber muncul dan berkembang pada komponen ini. Penggunaan ponsel genggam, ponsel pintar, laptop, tablet, dan *personal computer* sebagai perangkat untuk mengakses internet dengan bijak dapat lebih didalami melalui pembahasan kali ini.

Mengoptimalkan *Operating System*

Notifikasi untuk mengupdate *operating system* kadang cenderung mengganggu, tetapi jika hal ini diabaikan, bisa menjadi boomerang yang nantinya membuka peluang perangkat yang dimiliki menjadi korban dari kejahatan siber.

Mendownload *operating system* gratis yang legalitasnya dipertanyakan juga dapat menjadi ancaman tersendiri bagi keamanan kita di dunia siber.



Pengamanan *operating system* (OS) pada perangkat portable maupun mobility merupakan hal yang sangat perlu diperhatikan. Berikut tips yang dapat dilakukan terkait pengamanan OS:

a. **Gunakan selalu OS dan aplikasi yang legal.** Jangan menggunakan OS bajakan atau aplikasi yang tidak resmi, misalnya memasang aplikasi tambahan dari sumber selain pengembang resmi atau melakukan rooting/jailbreak perangkat smartphone kita. Hindari penggunaan OS versi tidak resmi atas dasar keingintahuan sekalipun karena akan meningkatkan risiko keamanan pada perangkat komunikasi.

b. **Pastikan telah mengaktifkan fitur enkripsi by default di semua OS dan perangkat komunikasi yang digunakan (laptop, tablet, smartphone, dsb.).** Aktivasi fitur enkripsi sangat mudah dilakukan dan hanya perlu sekali untuk digunakan selamanya. Fitur enkripsi ini gratis dan sama sekali tidak mengurangi performa. Umumnya, pengguna perangkat komunikasi tidak mengaktifkan fitur enkripsi karena tidak tahu atau khawatir dengan dengan mitos risiko yang dapat ditimbulkannya.

c. **Aktifkan pula fitur remote wipe dan lost device (phone) untuk perangkat mobility.** Fitur ini berfungsi untuk menghindari hal-hal yang tidak diinginkan ketika perangkat tersebut hilang. Penemu perangkat yang hilang tersebut tidak akan dapat mengakses atau membuka isi perangkat karena telah terenkripsi. Pemilik perangkat juga dapat melakukan penghapusan data dari jarak jauh (remote) sehingga data menjadi lebih aman sekalipun perangkatnya hilang.

d. **Terapkan rutinitias backup data sekaligus aktifkan enkripsi pada device backup.** Setidaknya terdapat 3 hal terkait backup yang perlu diperhatikan, yaitu:

i. **Device backup yang dilakukan rutin setiap hari.** Perangkat portable seperti laptop atau tablet dapat menggunakan external drive seperti flash drive atau portable HDD.

ii. **Backup yang dilakukan secara periodik misalnya dua hari sekali dan disimpan di tempat aman yang berbeda seperti di rumah.**

iii. **Fasilitas backup cloud yang digunakan dengan mode sinkronisasi instan.**

Memanfaatkan Cloud Storage

Keuntungan menggunakan layanan *cloud storage*?



Aman

Data tersimpan di server yang sudah dilengkapi enkripsi.



Mudah diakses

Data dapat diakses dari perangkat apa pun.

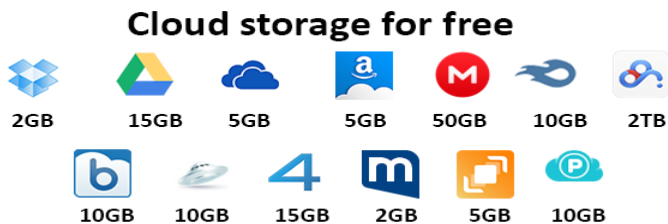


Mudah berbagi

Kemudahan berbagi data dengan orang lain sesuai keinginan pengguna.

Sumber: Tech in Asia 2018

Hampir semua OS resmi menyediakan layanan *cloud* secara gratis untuk penggunaanya. Contohnya, Windows OS menyediakan *one drive*, Google menyediakan Google Drive, Apple menyediakan iCloud dengan kapasitas masing-masing umumnya sebesar 5GB. Jika kekurangan kapasitas, pengguna juga dapat memperoleh tambahan layanan *cloud* secara gratis seperti MEGA yang menyediakan layanan berkapasitas hingga 50GB dan layanan lain seperti Dropbox yang kapasitasnya bervariasi. Ada juga layanan cloud spesifik seperti FLICKR yang disediakan untuk pengguna YAHOO! khusus untuk menyimpan foto dan video. Perlu diketahui bahwa semua layanan *cloud storage* ini menawarkan versi komersial jika membutuhkan kapasitas melebihi yang disediakan secara gratis.



Sumber: airexplorer.net

Hal yang terpenting adalah seluruh fitur *backup* telah disediakan *by default* oleh OS. Cara menggunakannya sangatlah mudah karena dilakukan secara otomatis dengan hanya satu kali konfigurasi, walaupun memang memang harus diaktifkan secara manual (*optional*). Kendalanya adalah pengguna seringkali mengabaikannya karena tidak tahu dan tidak pernah mencoba mengaktifkan atau menggunakan fitur ini.

Manfaat terbesar dari layanan *backup* ini adalah pengembalian data secara utuh dan mudah ketika terjadi insiden kehilangan perangkat maupun karena alasan alamiah seperti mengganti perangkat baru atau karena memiliki beberapa *device* berbeda yang digunakan secara bersamaan. Oleh karenanya, layanan *cloud* dapat membantu sinkronisasi semua data secara otomatis termasuk data *phone book*, *calender/event*,

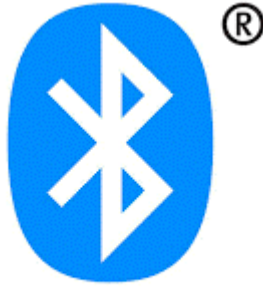
notes hingga aplikasi. Jangan lupa pula untuk mensinkronisasi layanan *cloud storage* agar terlindungi dengan enkripsi, baik dengan layanan enkripsi *online* dan aplikasi yang gratis maupun yang berbayar secara berlangganan.

Selanjutnya, END POINT SECURITY yang lengkap juga harus dimiliki pada perangkat komunikasi dengan fitur-fitur minimal, antara lain: personal firewall, antivirus, antimalware, antiransom-ware dan pilihan yang memiliki fitur tambahan seperti anti phishing dan ads blocker. Beberapa OS sudah menyediakan fitur end point security ini. Contohnya, Microsoft Windows (desktop) sudah dilengkapi firewall, antivirus dan antimalware. Namun demikian, kebanyakan OS belum melengkapi layanannya dengan fitur tersebut, khususnya perangkat mobility. Layanan end point security sebenarnya banyak tersedia secara gratis dengan berbagai pilihan, namun yang paling baik tentu saja yang berbayar karena memiliki fitur lengkap, paling update dan dapat melakukan otomatisasi pada banyak perangkat untuk membantu proteksi aktivitas di dalam jaringan online.

Penggunaan Perangkat Mobility

Sharing data melalui *perangkat mobility* memang merupakan sesuatu yang lumrah untuk dilakukan. Melakukan pertukaran data melalui Infrared, Bluetooth, dan Near Field Communication (NFC) seringkali dilakukan sebab prosesnya yang tergolong mudah. Sayangnya, kelebihan ini bisa menjadi peluang ancaman bagi keamanan siber dari perangkat yang dimiliki. Maka dari itu, menggunakan perangkat mobility dengan pintar juga perlu kita terapkan.

Untuk menjaga perangkat agar tetap aman, Dalam kondisi default, selalu matikan koneksi Infrared, Bluetooth, dan Near Field Communication (NFC). Hanya aktifkan jika ada kebutuhan koneksi dengan perangkat yang sudah dikenal. Jika ada permintaan akses dari perangkat lain yang belum dikenal, selalu tolak untuk menghindari adanya hacker yang mengakses smartphone.



Pada saat ini, ketergantungan atas penggunaan koneksi Bluetooth dan NFC semakin tinggi. Bluetooth banyak digunakan untuk kebutuhan transfer file, telepon dalam mobil, maupun entertainment seperti mendengarkan musik atau Google VR. Sedangkan NFC banyak digunakan untuk transaksi keuangan. Dua fitur ini jika secara tidak sengaja selalu on, akan berbahaya karena hacker dapat mengakses dari jarak 10 meter dengan perangkat yang tidak mencolok. Maka pastikan fitur ini selalu dimatikan jika tidak digunakan.

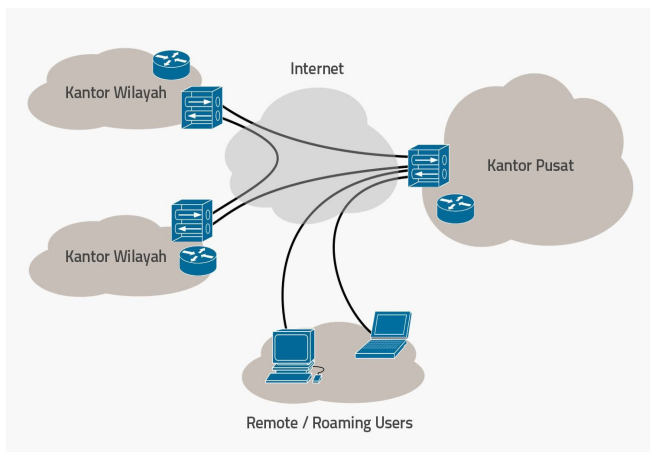
Komponen yang tidak kalah penting untuk diperhatikan untuk dapat pintar dalam keamanan siber adalah jembatan antara pengguna dan perangkat, yaitu akses. Tanpa akses maka kita tidak dapat terhubung ke dunia siber. Dalam mengakses internet, kita dapat melakukannya lewat berbagai macam jaringan baik yang dimiliki sendiri (pribadi) dan yang dimiliki bersama (publik). Jaringan pribadi jelas akan lebih aman dibandingkan jaringan publik, sebab akses yang kita lakukan bisa saja disalahgunakan oleh pemilik jaringan maupun pengguna yang tengah menggunakan jaringan yang sama. Oleh sebab itu, penting bagi kita agar dapat lebih pintar saat mengakses internet, khususnya saat menggunakan akses publik.

Akses di Tempat Publik

Salah satu hal yang perlu diperhatikan ketika melakukan transaksi secara *online* adalah masalah di tempat publik. Sebagai contoh, sangat disarankan untuk tidak melakukan transaksi sensitif apapun seperti *internet banking* ketika sedang terhubung dengan sambungan koneksi secara gratis atau WiFi di tempat publik. Jika hal ini harus dilakukan, terdapat alternatif untuk mengaktifkan Jaringan Pribadi Virtual atau VPN ketika hendak bertransaksi secara *online*. Memiliki VPN di setiap perangkat elektronik, baik *portable (laptop)* maupun *mobility (smartphone, tablet)*, sudah menjadi hal yang lazim terutama bagi *traveler*. Layanan VPN yang terbaik dan terpercaya umumnya dapat diperoleh dari perusahaan atau instansi terkait sebagaimana dijelaskan pada bagan di bawah ini.



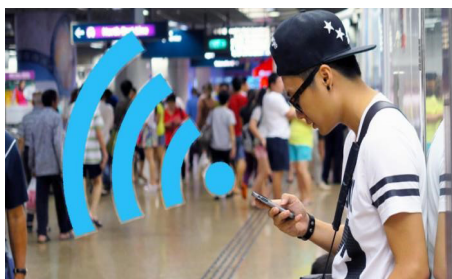
tif



Sumber: JejakWaktu.com

Akses di Terminal Publik

Perlu lebih berhati-hati jika menggunakan akses internet yang bersumber dari terminal publik seperti warnet atau terminal akses di bandara. Sangat tidak dianjurkan untuk melakukan transaksi apapun terlebih



yang mengharuskan untuk memasukkan data-data pribadi yang bersifat sensitif, misalnya identitas, username, atau password dan sejenisnya. Sebab, keylogger terdapat hamper di setiap sudut tempat publik. Jika ingin melakukan transaksi terkait perjalanan seperti check in, pastikan terminal akses yang digunakan adalah yang khusus digunakan untuk keperluan tersebut.

Apa itu *keylogger*?

Keylogger merupakan sebuah program yang dirancang untuk merekam atau mencatat penekanan tombol melalui *keyboard* ke dalam sebuah *log* (catatan). Akan tetapi, saat ini *keylogger* juga dapat merekam aktivitas *mouse*, *clipboard*, *web browser* dan *visual surveillance* (gambar yang tayang di monitor dan tertangkap secara otomatis).

Bagaimana cara mengatasi *keylogger*?

Gunakan aplikasi On Screen Keyboard dengan langkah-langkah berikut:

- Klik Start
- All Program
- Pilih Acessoris
- Acessibility
- Klik On Screen Keyboard

Gunakan password dengan cara *copy-paste* password yang sudah dipersiapkan pada *notepad software* pencatat lainnya.

Gunakan *Anti-Keylogger* yang memiliki antivirus khusus untuk mencegah program pada *keylogger* masuk ke dalam jaringan perangkat.

Sumber: KursusWebsite.org

DAFTAR PUSATAKA

- ACS, *Cybersecurity: Threats, Challenges, and Opportunities*, November 2016.
- Arifah, Dista Amalia, “Kasus Cybercrime di Indonesia”, *Jurnal Bisnis dan Ekonomi (JBE)* Vol. 18, No. 2, September 2011, Hal. 185 – 195.
- Andriyati, Handrini, “Cyber Security dan Tantangan Pengembangannya di Indonesia”, *Politica* Vol. 5, No.1, Juni 2014, Hal. 95—110.
- Cavelty, Myriam Dunn, *Cyber-Security*, ETH Zurich, 2012.
- Danuri, Muhammad dan Suharnawi, “Trend Cybercrime dan Teknologi Informasi di Indonesia”, *INFOKAM* No. 2 Th. XII, September 2017, Hal. 55 – 64.
- Pande, Jeetendra, *Introduction to Cyber Security*, Uttarakhand Open University, 2017.
- Wildan, Moh, “Konvergensi Simbolis dalam Komunikasi Ruang Siber”, *Jurnal Masyarakat Telematika dan Informasi*, Vol. 5, No. 2, November 2014, Hal. 209-232
- Antara, Agregasi, “Kasus Serangan Siber Terheboh di 2017, Apa Saja?”, *Techno Okezone*. 31 Desember 2017, (<https://techno.okezone.com/read/2017/12/31/207/1838109/kasus-serangan-siber-terheboh-di-2017-apa-saja>), diakses tanggal 7 Juli 2018.
- Asih, Antika, “Tahukah Kita Tentang Child Online Protection”, *Wantiknas*, 17 Oktober 2016, (<http://www.wantiknas.go.id/2016/10/17/tahukah-kita-tentang-child-online-protection/>), diakses 1 Juli 2018
- Baraniuk, Chris, “Bagaimana Berpikir ala Pakar Keamanan Siber?”, *BBC*, 1 Agustus 2017, (<http://www.bbc.com/indonesia/vert-fut-40772575>), diakses tanggal 8 Juli 2018.

Damar, Mario, *"Jutaan data pribadi pengguna Facebook diduga bocor lewat kuis"*, Merdeka.com, 21 Maret 2018, (<https://www.merdeka.com/dunia/jutaan-data-pribadi-pengguna-facebook-diduga-bocor-lewat-kuis.html>), diakses 1 Juli 2018

Erdianto, Kristian, *"Keamanan Siber Indonesia Tak Lebih Baik Dibandingkan Malaysia dan Singapura"*, Kompas. 21 November 2017. (<https://nasional.kompas.com/read/2017/11/21/20480051/keamanan-siber-indonesia-tak-lebih-baik-dibandingkan-malaysia-dan-singapura>) diakses tanggal 7 Juli 2018.

Falahuddin, Mochammad James, *"Sekilas Tentang Cyber Crime, Cyber Security dan Cyber War"*, Detik.com, 31 Agustus 2015, (<https://inet.detik.com/security/d-3005339/sekilas-tentang-cyber-crime-cyber-security-dan-cyber-war>), diakses tanggal 8 Juli 2018.

Family Online Safety Institute, *"Clean Up Your Digital Footprint"*, (<https://www.fosi.org/good-digital-parenting/clean-your-digital-footprint/>), diakses 1 Juli 2018

Google Consumer Barometer, Indonesia, diakses tanggal 1 Juli 2018 <https://www.consumerbarometer.com/en/graph-builder/?question=M6&filter=country:indonesia>

Hadid, M, *"Melindungi Privasi Mutlak Perlu di Era Internet of Things"*, Pemmzchannel.com, 3 Desember 2017, (<https://pemmzchannel.com/2017/12/03/melindungi-privasi-mutlak-perlu/>), diakses 1 Juli 2018

Hamdi, Putra, *"KPAI Sayangkan Viral Anak Kecil Tonton Video Porno di Samping Ibunya"*, Tribunnews.com, 15 Maret 2018, (<http://www.tribunnews.com/metropolitan/2018/03/15/kpai-sayangkan-viral-anak-kecil-tonton-video-porno-di-samping-ibunya>), diakses 1 Juli 2018

Hernawan, Achmed Islamic, "Apakah Cookie Dan Apa Dampak Privasi Yang Ditimbulkan?", Windowsku.com, 22 Mei 2018, (<https://windowsku.com/apakah-cookie-dan-apa-dampak-privasi-yang-ditimbulkan/>), diakses 23 Juli 2018.

Kania, Dewi, "5 Cara Melindungi Anak-Anak dari Konten Negatif Internet", Okezone, 7 Februari 2018, (<https://lifestyle.okezone.com/read/2018/02/07/196/1855941/5-cara-melindungi-anak-anak-dari-konten-negatif-internet>), Diakses 1 Juli 2018

Librianty, Andrina, "ID-COP Kawal Keselamatan Anak-anak di Dunia Maya", Liputan6.com, 17 September 2015, (<https://www.liputan6.com/tekno/read/2319823/id-cop-kawal-keselamatan-anak-anak-di-dunia-maya>), diakses 1 Juli 2018

Maulana, Risky. App Annie: Durasi Penggunaan Aplikasi Mobile di Indonesia Tertinggi di Dunia . TechinAsia. 23 January 2018 (<https://id.techinasia.com/app-annie-report-2017-indonesian-app-market-potentials>) diakses tanggal 1 Juli 2018.

Mustofa, Ayub. Cara Menghindari Penipuan Phishing di Internet, Tech in Asia. 5 Januari 2018, (<https://id.techinasia.com/cara-menghindari-phishing>) diakses tanggal 29 Agustus 2018.

Plimbi, Apakah Browser Cookie Berbahaya?, 4 Feb 2013, (<https://www.plimbi.com/article/28691/browser-cookie-berbahaya>), diakses 23 Juli 2018.

Plimbi.com, "Tips Menjaga Keamanan Data Pribadi di Internet", 13 Juli 2015, (<https://www.plimbi.com/article/160323/tips-menjaga-keamanan-data-pribadi-di-internet>), diakses 1 Juli 2018

Referensi Bebas, Cara Mengamankan Laptop Dari Pencuri Data, 2 Oktober 2016, (<https://www.referensibebas.com/2016/10/cara-men>

[gamankan-laptop-dari-pencuri.html](#)), diakses 23 Juli 2018.

Sulaiman, Fajar, “60% Kejahatan Cyber Perbankan Dilakukan Pegawai Sendiri”, *Warta Ekonomi.co.id*, 5 April 2016, (<https://www.wartaekonomi.co.id/read96016/waduh-60-kejahatan-cyber-perbankan-dilakukan-pegawai-sendiri.html>), diakses tanggal 7 Juli 2018.

Zaenudin, Ahmad, “Jejak Digital, Barang Berharga yang Dilupakan”, *Tirto.id*, 6 Januari 2018, (<https://tirto.id/jejak-digital-barang-berharga-yang-dilupakan-cCP7>), diakses 1 Juli 2018










Center for Digital Society

Faculty of Social and Political Sciences
Universitas Gadjah Mada
Room BC 201-202, BC Building 2nd Floor,
Jalan Socio Yustisia 1
Bulaksumur, Yogyakarta, 55281, Indonesia

Phone : (0274) 563362, Ext. 116

Email : cfds.fisipol@ugm.ac.id

Website : cfds.fisipol.ugm.ac.id

 ugm.id/digitalsociety  [@cfds_ugm](https://www.whatsapp.com/channel/0029va333333333333)  CfDS UGM  [@cfds_ugm](https://twitter.com/cfds_ugm)
 facebook.com/cfdsugm  [cfds_ugm](https://www.instagram.com/cfds_ugm)  Center for Digital Society (CfDS)