SAFEnet
SOUTHEAST ASIA FREEDOM OF EXPRESSION NETWORK

PANDUAN

KEBERSIHAN DIGITAL

UNTUK ORGANISASI MASYARAKAT SIPIL

DI INDONESIA

Panduan Kebersihan Digital Untuk Organisasi Masyarakat Sipil Indonesia

Disusun oleh:

Divisi Keamanan dan Keselamatan Daring

Southeast Asia Freedom of Expression Network/ SAFEnet

September 2020

PANDUAN INI DIPERGUNAKAN SEBAGAI BAHAN BACAAN PESERTA MENDAMPINGI SALINDIA PELATIHAN.

https://safenet.or.id

Dapat diunduh lewat: **s.id/panduankebersihandigital**

Daftar Isi

Pengantar 1

Bagian 1: Mengidentifikasi Ancaman Digital 4

1.1 Phishing 5

1.2 Spear Phishing 10

1.3 Malware 14

1.4 Spyware 18

1.5 Wi-Fi tidak aman 22

1.6 Menyadap jaringan 23

Bagian 2: Proteksi dan Pencegahan Serangan Digital lewat Kebersihan Digital 26

2.1 Menerapkan manajemen password yang baik 27

2.2 Menggunakan password yang sama itu berbahaya, gunakan Password Manager 29

2.3 Otentikasi dua langkah 31

2.4 Mengenali jika akun Anda disusupi 34

2.5 Peran Anda untuk menjaga agar pemili tetap aman 39

2.6 Mengamankan jaringan internet Anda di rumah 50

LAMPIRAN A: Cara aktivasi dan penggunaan LastPass **59**

LAMPIRAN B: Cara aktivasi dan penggunaan Google Authenticator pada akun Google **61**

LAMPIRAN B: Langkah-langkah pelaporan serangan digital melalui SAFEnet **63**

Pengantar

"A chain is only as strong as its weakest link. Computer security relies on a great number of links, hardware, software and something else altogether: people."

Dalam persiapan beberapa daerah di Indonesia untuk melaksanakan Pemilihan Kepala Daerah (Pilkada) 2020 di bulan Desember nanti, para pemangku kepentingan Pemilu dihadapkan pada tantangan untuk melaksanakan Pilkada secara efektif dengan segala kekurangan akibat pandemi COVID-19. Dalam setiap pelaksanaan proses pemilu dan demokrasi, organisasi masyarakat sipil memainkan peran penting dalam mendukung proses kelembagaan pemilu yang demokratis, serta mengurangi dinamika konflik terkait pemilu dan mendorong lingkungan pemilu yang damai.

Namun, belakangan ini organisasi masyarakat sipil di Indonesia harus berhadapan dengan serangan digital yang belakangan semakin kerap dialami oleh aktivis, jurnalis, perempuan dan kelompok rentan lainnya di Indonesia.

Bentuk serangan digital yang telah terjadi bermacam-macam, mulai dari *phising*, *malware*, akun peniru (*impersonator*), mengunggah informasi personal tanpa persetujuan (*doxing*), persekusi, penggunaan *fake news/ misinformasi/disinformasi* sebagai senjata (*weaponization of social media*), peretasan, hingga penyadapan ilegal (*unlawful breach and illegal surveillance*).

Intensitas serangan digital yang diarahkan kepada aktivis, jurnalis, perempuan dan kelompok rentan ini kerap berkaitan dengan momentum peristiwa sosial dan politik

yang terjadi di Indonesia, termasuk di antaranya aktivitas Pilkada maupun pemilihan nasional.

Panduan Kebersihan Digital (*Digital Hygiene*) ini dapat digunakan organisasi masyarakat sipil untuk membekali diri dengan kompetensi dasar melindungi diri untuk mengurangi risiko dari serangan digital.

Penyusunan panduan Kebersihan Digital ini ditujukan agar organisasi masyarakat sipil memiliki pengetahuan dan teknik dasar untuk mengidentifikasi dan mencegah menjadi korban serangan digital.

Panduan ini terdiri dari dua bagian, yaitu:

Bagian 1: Mengidentifikasi Ancaman Digital

Bagian 2: Memproteksi Serangan Digital lewat Kebersihan Digital

Di balik semua sistem teknologi dan prosedur keamanan yang ada, tetap terdapat faktor penting, yaitu: manusia. Bukan hanya dirimu, tapi yang perlu diperhitungkan adalah bagaimana jika orang-orang sekitarmu tidak memperkuat kapasitas keamanan digital mereka. Misalnya menggunakan kata kunci (*password*) yang mudah ditebak, atau menuliskannya di layar komputernya, lupa *logout*, atau dengan mudahnya memberikan akses kepada teman, rekan, kliennya, atau dikelabui dengan *phishing* dan berbagai *social engineering*? Tidak ada sistem yang tidak melibatkan interaksi manusia. Begitu pula keamanan digital bersifat menyeluruh, melibatkan semua orang, bukan semata bergantung pada kemampuan individu ataupun perangkat tertentu.

Tidak ada sistem keamanan yang tidak dapat dibobol, dan tiap orang memiliki kebutuhan dan solusi keamanan berbeda-beda. Kebutuhan dan solusi keamanan untuk anak kecil akan berbeda dengan seorang jurnalis, aktivis buruh. Namun, ada praktik-praktik keamanan dasar yang dapat dilakukan untuk mencegah data Anda di(salah)gunakan.

Maka gunakan panduan ini untuk dipraktikkan dalam kegiatan sehari-hari agar dijauhkan dari gangguan dan ancaman yang mengganggu kegiatan dalam mendukung proses kelembagaan pemilu yang demokratis, serta mengurangi dinamika konflik terkait pemilu dan mendorong lingkungan pemilu yang damai.

Bagian 1

Mengidentifikasi Serangan Digital

Ketika berada pada dunia siber, Anda tidak akan terbebas dari ancaman peretas dan kejahatan siber. Jika Anda berpikir Anda bukan siapa-siapa maka itu sama sekali salah. Jika Anda berpikir penjahat itu cuma satu orang iseng dengan kemampuan teknis peretasan (*hacking*) di depan komputer, maka Anda juga salah. Karena saat ini, kejahatan siber sudah menjadi bisnis serius yang terkoordinasi dengan baik.

Motif serangan digital bisa sangat beragam, tetapi pada dasarnya bisa dibagi tiga yaitu pribadi, ekonomi, dan politik. Motif serangan pribadi biasanya dilakukan dengan tujuan personal, misalnya balas dendam pribadi atau alasan hubungan tidak sehat (*toxic relationship*). Perilakunya adalah orang-orang dekat atau yang kenal secara pribadi dengan korban.

Motif ekonomi biasa dilakukan secara acak dengan metode lebih canggih, terutama menyasar korporasi atau lembaga tertentu dengan tujuan meminta imbalan atau mendapatkan keuntungan lain secara material. Salah satu contohnya adalah serangan ransomware WannaCry pada Mei 2017 yang menyasar perusahaan-perusahaan besar dan menagih sejumlah pembayaran dari korban.

Adapun motif politik saat ini semakin sering dilakukan terhadap kelompok kritis dan rentan, seperti jurnalis, akademisi, aktivis, masyarakat adat, kelompok LGBT, dan lainnya. Tujuannya untuk membatasi atau bahkan

membungkam suara-suara kritis terhadap negara atau bahkan campur tangan terhadap situasi politik sebuah negara. Pelaku serangan ini jauh lebih canggih, sistematis, dan terorganisir sehingga sulit sekali diidentifikasi serangannya kecuali ketika sudah ada korban.

Maka penting untuk mengetahui apa saja serangan digital yang mungkin Anda alami sebagai aktivis organisasi masyarakat sipil.

Ancaman serangan digital yang perlu dikenali adalah:

1. *Web-based threat*: *phising, spear phising*
2. *Application-based threat*: *malware, spyware*
3. *Network-based threat*: *unsecured Wi-Fi, network spoofing*

1.1. Phishing

Phishing adalah salah satu ancaman siber terbesar saat ini. Dari semua jenis serangan siber yang memanfaatkan manipulasi psikologis, *phishing* adalah yang paling terkenal dan paling berhasil.

Phishing adalah salah satu bentuk rekayasa sosial (*social engineering*). Dalam serangan rekayasa sosial, penyerang menggunakan interaksi manusia (keterampilan sosial) untuk mendapatkan atau membahayakan informasi tentang organisasi atau sistem komputernya. Seorang penyerang mungkin tampak sederhana dan terhormat, mungkin mengaku sebagai karyawan baru, petugas perbaikan, atau peneliti dan bahkan menyertakan dokumen-dokumen

untuk mendukung identitas tersebut. Namun, dengan mengajukan pertanyaan, dia mungkin dapat mengumpulkan informasi yang cukup untuk menyusup ke jaringan organisasi. Jika penyerang tidak dapat mengumpulkan informasi yang cukup dari satu sumber, dia dapat menghubungi sumber lain dalam organisasi yang sama dan mengandalkan informasi dari sumber pertama untuk menambah kredibilitasnya.

Kegiatan kerja dari rumah dan pandemi COVID-19 telah meningkatkan tingkat ancaman *phishing*.

Definisi:

Phishing adalah serangan siber yang berupaya mengelabui orang agar memberikan informasi seperti sandi, atau nomor rekening bank dan kartu kredit melalui email yang dibuat sedemikian rupa supaya seolah terlihat berasal dari sumber yang "tepercaya".

Serangan *phishing* yang paling sering terjadi adalah serangan *phishing* melalui email, tetapi sebetulnya semua jenis media dapat digunakan untuk melakukan serangan ini seperti melalui aplikasi pesan instan (Whatsapp), lewat Facebook, aplikasi video conference, maupun SMS.


SAFEnet
phishing
Phishing adalah serangan siber yang berupaya mengelabui orang agar memberikan informasi seperti sandi, atau nomor rekening bank dan kartu kredit melalui email yang dibuat sedemikian rupa supaya seolah terlihat berasal dari sumber yang "terpercaya".
APA YANG DIINCAR PELAKU PHISHING?
Kata Sandi
Data Keuangan
Data Pribadi
Uang
Data
MEDIA YANG DIGUNAKAN PELAKU PHISHING
Email
Pesan WhatsApp
Facebook
Video Conference
SMS
1 DARI 10 PERCOBAAN PHISHING BISA BERHASIL*
WASPADAI!
1. Ejaan atau tulisan dari pesan yang diterima
2. Nama pengirim
3. Isi email yang terlalu bombastis
4. Lampiran yang mencurigakan
5. Url atau tautan yang tidak biasa
* Stanford University

SMiShing:

Seperti penipuan *phishing*, penjahat siber berupaya mengelabui orang agar mengunduh perangkat lunak jahat, mengklik tautan berbahaya, atau mengungkapkan informasi sensitif. Serangan SMiShing diluncurkan melalui pesan SMS, bukan lewat email.

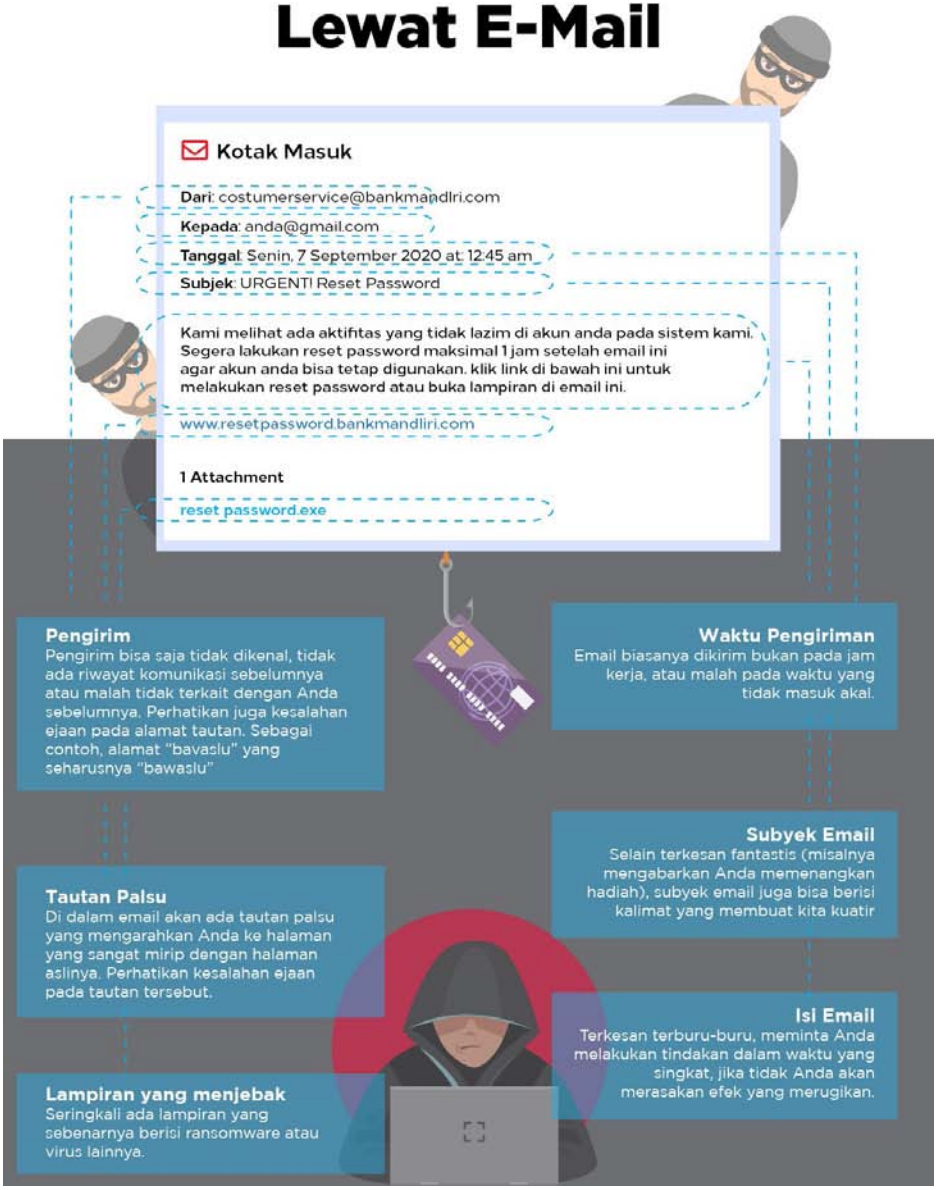
Phishing adalah ancaman besar bagi semua jenis organisasi, baik besar maupun kecil. Informasi yang berhasil didapatkan dari serangan *phishing* dapat digunakan untuk mengakses akun penting dan dapat mengakibatkan pencurian identitas, kerugian finansial, atau kerusakan reputasi.

Ciri-ciri umum *phising*

1. **Kabar Fantastis** – Memberi kabar yang menguntungkan dan pernyataan yang menarik seperti Anda telah memenangkan ponsel mewah, undian berhadiah, atau barang mewah. Jangan klik email yang mencurigakan ini.

2. **Serba Buru-buru** - Taktik favorit yang sering digunakan adalah Anda diminta untuk bertindak super cepat dalam waktu terbatas. Beberapa dari mereka bahkan akan memberi tahu bahwa Anda hanya memiliki beberapa menit untuk menanggapi. Saat Anda menemukan jenis email ini, sebaiknya abaikan saja. Terkadang, mereka akan memberi tahu Anda bahwa akun Anda akan ditangguhkan kecuali jika Anda segera memperbarui detail pribadi Anda. Jangan mengklik tautan di email.

Anatomi Phishing Lewat E-Mail



3. **Tautan Aspal** – Seringkali *phising* mencantumkan tautan yang terlihat asli, tapi sebenarnya palsu. Gunakan kursor untuk mengarah ke tautan, maka Anda akan diberitahu URL sebenarnya. Perhatikan juga atas kesalahan eja/ketik, misalnya www.bankmandliri.com - 'l' sebenarnya adalah 'i', jadi perhatikan baik-baik.

4. **Lampiran** - Jika Anda melihat lampiran di email semacam ini, jangan dibuka. Penjahat siber seringkali menyertakan file berisi muatan seperti *ransomware* atau virus lainnya. Satu-satunya jenis file yang selalu aman untuk diklik adalah file .txt.

5. **Pengirim Tidak Dikenali** - Apakah itu tampak dari seseorang yang tidak Anda kenal atau seseorang yang Anda kenal, jika ada sesuatu yang tampak tidak biasa, tidak terduga, di luar karakter atau hanya mencurigakan secara umum, jangan klik!

1.2. Spear-Phishing

Spear-Phishing adalah serangan siber yang terarah. Serangan ini secara spesifik menargetkan calon korban, penyerang telah terlebih dahulu menentukan siapa individu atau organisasi yang mereka incar (mereka melakukan riset pada target untuk merancang serangan yang lebih personal dan bisa meningkatkan kemungkinan target calon korban jatuh ke dalam perangkap mereka).

Email spear-phishing seringkali dibuat seolah-olah berasal dari teman, kolega atau atasan korban, atau terkadang bahkan layanan online yang digunakan

oleh korban (Gmail atau Bank).

Email yang dikirimkan oleh pelaku biasanya akan "memberitahukan" Anda bahwa ada beberapa hal atau masalah yang perlu Anda selesaikan. Email tersebut juga berisi tautan atau lampiran yang jika dibuka akan memungkinkan peretas mengakses akun dan informasi Anda.

Cara melindungi dari phishing dan spear-phishing:

Tidak ada cara yang 100 persen berhasil untuk menghindari serangan phishing, tetapi Anda bisa selamat dari serangan ini dengan melakukan beberapa tindakan pencegahan mendasar seperti berikut ini:

1. Selalu Waspada Sebelum Klik Tautan

Sebelum mengklik suatu tautan, selalu periksa lebih dulu.

- Kita sehari-hari terbiasa dengan mengklik tautan, entah itu ketika membalas email, melakukan pencarian online, maupun berselancar di dunia maya, Mengklik pada tautan sudah jadi semacam kebiasaan. Penjahat siber memanfaatkan kebiasaan tersebut – yang telah membuat menurunnya tingkat kewaspadaan – untuk membuat kita membuka tautan di email hanya karena isinya terlihat menarik. Anda harus selalu bertanya pada diri sendiri: siapa yang mengirimnya? kapan? apakah ada sesuatu yang mencurigakan?

- Meluangkan beberapa detik untuk mengarahkan

kursor ke atas tautan yang diberikan dan melihat kemana arah tautan tersebut. Hal sederhana ini dapat menyelamatkan Anda dari serangan *phishing*.

- Waspadalah, *phishing* tidak hanya dilakukan melalui email. Akun media sosial, pesan instan, layanan e-commerce, dan semua jenis alat komunikasi online dapat digunakan sebagai vektor serangan phishing.

2. Verifikasi Pengirim atau Legitimasi dari Situs Web

Penyerang biasanya akan menirukan tampilan situs web yang asli. Ada beberapa kegiatan verifikasi yang dapat Anda lakukan agar tidak terperangkap ke dalam serangan *phishing* yang umum dilakukan:

- Cek apakah pada sebuah email ada tautan yang tidak mengandung nama organisasi atau perusahaan yang digunakan untuk mengirim email.

- Salah satu rekomendasi yang sangat berguna adalah dengan mengetik tautan seluruhnya pada peramban dari pade mengklik langsung dari email yang Anda terima.

3. Gunakan Otentikasi Dua Langkah (2FA)

Praktik ini adalah cara terbaik untuk melindungi Anda dari *phishing* dan *spear-phishing* yang canggih. Jika seorang hacker berhasil mendapatkan password Anda, mereka tidak akan bisa login ke akun Anda jika mereka tidak memiliki "kunci kedua" Anda.

4. Selalu Perbarui Antivirus di Gawai

- Sebagian besar anti-virus sudah dilengkapi dengan fitur *anti-phishing* (terkadang disebut *Web-Shield*) yang secara otomatis terinstalasi di peramban Anda dan memblokir situs-situs phishing dari komputer Anda. Jangan *instalasi toolbar anti-phishing* yang Anda temukan secara sembarangan di internet! Seringkali *toolbar* tersebut justru mengandung *spyware* yang akan merekam dan mengirimkan semua situs yang Anda kunjungi ke pihak ketiga. Dalam hal ini, obatnya malah bisa lebih buruk dari penyakitnya.

- Jika lembaga Anda tidak menyediakan anti-virus untuk perangkat Anda, maka Anda disarankan untuk menggunakan anti-virus yang berbayar atau anti-virus gratisan yang telah dikenal luas olah masyarakat, misalnya Avast anti-virus. Pastikan hanya instalasi anti-virus yang diunduh dari website resmi pembuatnya.

5. Jangan Memberi Informasi Pribadi

Sebagai aturan umum, Anda harus selalu berhati-hati saat berbagi data pribadi maupun informasi keuangan di Internet.

- Rata-rata lembaga keuangan memiliki aturan ketat terkait dengan permintaan informasi data sensitif. Mereka tidak akan meminta data personal tanpa mengonfirmasi identitas Anda, dan Anda tidak boleh memberikannya tanpa mengonfirmasi identitas mereka.

- Kunjungi situsweb resmi, dapatkan nomor mereka dan hubungi mereka.

- Juga, berhati-hatilah dengan pertanyaan reset password: nama Ibu Anda, kota kelahiran Anda, dan sekolah pertama Anda bukanlah sebuah rahasia. Jadi data tersebut sebaiknya tidak dijadikan sebagai pertanyaan untuk pemulihan kata sandi.

1.3. *Malware*

Malware adalah kependekan dari *Malicious Sofware* (peranti lunak berbahaya). Istilah *malware* digunakan untuk menggambarkan suatu program atau *script* yang dicurigai bisa mengekspoitasi komputer atau informasi penting di dalamnya. Termasuk juga untuk menggambarkan program atau *script* yang bersifat berbahaya, merusak, mengganggu, mengusik, dan mencurigakan.

Target atau sasaran utama *malware* bervariasi tergantung dari keinginan pembuatnya. Misalnya untuk memata-matai seseorang, mencuri informasi atau data pribadi (rahasia) orang lain, membobol keamanan program dan masih banyak lagi. Intinya, *malware* bisa merugikan seseorang bahkan banyak orang.

Merujuk pada hasil riset terbaru Microsoft Security Endpoint Threat Report 2019, secara khusus serangan malware di Indonesia sendiri menempati peringkat tertinggi di kawasan Asia Pasifik, yaitu 10,68% pada 2019. Angka tersebut masih dua kali lebih tinggi dari rata-rata regional. Indonesia juga terdaftar memiliki tingkat kasus ransomware tertinggi ke-2 di seluruh

wilayah Asia Pasifik, yaitu 0,14%. Ini masih 2,8 kali lebih tinggi dari rata-rata regional. Sedangkan tingkat kasus penambangan cryptocurrency Indonesia berada di angka 0,10% pada tahun 2019, 2 kali lebih tinggi dari rata-rata regional dan global, dan tingkat kasus tertinggi ke-4 di seluruh wilayah.

Dalam beberapa hal, program yang akan berjalan di ponsel maupun di komputer PC dan laptop dideteksi oleh antivirus sebagai "malware" dikarenakan ada kode skrip tertentu yang dianggap mencurigakan oleh aplikasi pelindung tersebut.

Virus, spyware, adware, worm, trojan, rootkit, ransomware, dan cryptojackers adalah semua jenis malware, seperti juga beberapa serangan phishing. Beberapa jenis malware tersebar di Internet melalui email, pesan teks, laman web jahat, dan cara lainnya.

Beberapa menyebar melalui perangkat seperti stik memori USB yang digunakan untuk bertukar data. Sementara beberapa malware membutuhkan target yang tidak menaruh curiga untuk membuat kesalahan, yang lain dapat secara diam-diam menginfeksi sistem yang rentan tanpa korban melakukan apa pun.

Malware hadir dalam bentuk kode, skrip, surat, perangkat lunak dan bahkan program yang sah. Perangkat lunak perusak biasanya digunakan sebagai sarana untuk mengumpulkan statistik, data sensitif (nama, alamat, informasi kartu kredit), mengirim e-mail spam massal, data selundupan host, mengirim iklan, dan lain sebagainya.

Beberapa sumber penyebaran malware adalah :

(1) *Removable* media. Seperti USB flashdisk, media storage R/W Media penyimpanan eksternal yang dapat jadi tempat Malware menetap menjadikan media.

(2) Jaringan. Hubungan antara beberapa komputer secara langsung sangat memungkinkan suatu malware ikut berpindah saat terjadi pertukaran atau pengeksekusian suatu file/program yang mengandung malware.

(3) Situs web (internet). Sangat mungkin suatu situs sengaja ditanamkan suatu *malware* yang akan menginfeksi komputer-komputer yang mengaksesnya.

(4) Piranti lunak yang berkategori *freeware, shareware* atau bahkan bajakan. Banyak sekali malware yang sengaja ditanamkan dalam suatu program yang disebarluaskan baik secara gratis atau "trial version" yang tentunya sudah tertanam malware di dalamnya, apalagi mengunduh aplikasi bajakan (*crack*) dari situs internet.

(5) *Attachment* pada email, *transferring* file. Hampir semua jenis penyebaran malware akhir-akhir ini menggunakan *email attachment* dikarenakan semua pemakai jasa internet pastilah menggunakan email untuk berkomunikasi, file-file ini sengaja dibuat mencolok/menarik perhatian, bahkan seringkali memiliki ekstensi ganda pada penamaan filenya.

MALICIOUS SOFTWARE

Istilah untuk sebuah perangkat lunak (software) yang biasanya dipasang di website oleh *cybercriminals* dengan maksud untuk mencuri data atau menimbulkan kerusakan pada komputer korban

JENIS-JENIS MALWARE

Virus

Virus bisa menginfeksi korbannya, mengambil alih sebagian atau seluruh fungsi. Virus merusak data atau mencari hal-hal seperti password, nomor kartu kredit, atau informasi sensitif lainnya.

Worm

Virus yang tertinggal di memori komputer Anda dan mereplikasi dirinya dan menyebar ke komputer lain di dalam jaringan. Worm bisa membuat peladen menjadi kelebihan beban.

Spyware

Malware yang didesain untuk memata-matai kegiatan korban, mengumpulkan data pribadi seperti nama pengguna, kata sandi, atau kebiasaan dalam berinternet.

Adware

Iklan otomatis yang muncul tanpa persetujuan kita untuk memberikan promosi-promosi yang tidak kita inginkan. Ketika iklan diklik, kita kadang diarahkan ke website yang mencurigakan

Trojan

Malware yang menyamar seperti program yang lazim kita temui. Malware ini bisa masuk ke komputer kita dan membuka akses untuk mencuri data-data pribadi

Ransomware

Malware yang mengambil alih kuasa pada data Anda dan meminta tebusan dalam bentuk uang untuk mengembalikan kuasa pada data tersebut

MEDIA PENYEBARAN MALWARE

Media Penyimpanan seperti USB Flash Disk, CD, dll

Piranti lunak, utamanya yang berkategori *freeware*, *shareware*, atau malah bajakan

Jaringan

Lampiran pada email

Situs web

Cara melindungi diri dari malware adalah memasang perangkat lunak anti-malware dan anti-virus. Jika sistem sudah terinfeksi, maka *system restore* dan *formatting* bisa digunakan untuk memperbaiki komputer.

1.4. Spyware

Dari jenis malware yang mengirimkan aliran data ke penjahat siber, ada ancaman utama yang lebih berbahaya yaitu Spyware. Dalam banyak kasus, bukan malware dari penyerang tak dikenal yang harus dikhawatirkan pengguna, melainkan spyware yang dipasang oleh oknum untuk melacak keberadaan dan aktivitas mereka.

Spyware jenis ini juga dikenal dengan nama *stalkerware*; banyak dari aplikasi ini dirancang untuk dimuat di perangkat target tanpa izin atau sepengetahuan mereka.

Aplikasi TeamViewer, yang sejatinya digunakan untuk membantu mengakses gawai dari jarak jauh, kerap disalahgunakan menjadi *stalkerware*. Sebenarnya TeamViewer adalah perangkat lunak resmi yang digunakan untuk menghubungkan ke komputer jarak jauh, menyediakan dukungan jarak jauh, mentransfer file antara komputer yang berbeda, dan sebagainya, tetapi penipu menggunakan perangkat lunak ini untuk tujuan jahat. Mereka sering menipu orang agar menginstal TeamViewer menggunakan berbagai situs web penipuan. Salah satu contohnya adalah situs penipuan dukungan teknis yang mengklaim bahwa komputer pengunjung mungkin berisiko. Orang-orang

biasanya tidak mengunjungi situs web semacam ini dengan sengaja - mereka dibuka oleh aplikasi yang mungkin tidak diinginkan yang dipasang di peramban dan sistem operasi.

Upaya deteksi antivirus dan malware yang komprehensif harus menggunakan teknik pemindaian khusus untuk jenis program ini, yang memerlukan penanganan sedikit berbeda daripada malware lainnya karena cara ia masuk ke perangkat Anda dan tujuannya.

Spyware canggih belakangan kerap digunakan dengan tujuan mengumpulkan informasi (intelijen) dengan target aktivis, jurnalis, dan kelompok berisko. Beberapa versi spyware yang ekstrim dan invasif dapat melacak dengan tepat kunci yang Anda ketik. Penyerang juga dapat menggunakan spyware untuk tujuan jahat. Contoh spyware ini seperti FinFisher, HackingTeam, dan NSO Pegasus --- ketiganya sudah masuk dan digunakan di Indonesia --- perlu diwaspadai untuk melindungi aktivitas organisasi dan data pribadi Anda. Spyware semacam ini tidak mudah untuk dilacak keberadaannya dan dicegah dengan program antivirus, sehingga perlu kewaspadaan ekstra dalam mengantisipasinya.

Bagaimana Anda dapat mencegah spyware?

- **Jangan mengklik tautan di dalam jendela pop-up**. Karena jendela pop-up sering kali merupakan produk spyware, mengklik jendela tersebut dapat menginstal perangkat lunak spyware di komputer Anda. Untuk menutup jendela pop-up, klik ikon

Contoh-Contoh Serangan Spyware

Aktivis HAM Maroko Jadi Target Serangan Spyware

NEWS

Ilustrasi | Foto: freepik.com

Andi Nugroho

Konferensi Video Dating & Sedating / Webinar
Hemat Kendaraan / Kuota Internet
Pengembang Aplikasi Lokal Indonesia

jumpa.id

Cyberthreat.id Amnesty International mengatakan, sejumlah aktivis hak

Spyware Pegasus

Spyware Pegasus menyebar di bulan November 2019 yang lalu. Spyware ini menyebar melalui aplikasi pesan WhatsApp dan menargetkan sekitar 1.400 orang. Sebagian besar di antaranya adalah diplomat, wartawan, aktivis HAM, dan pejabat senior pemerintah.

RottenSys

Menyamar sebagai aplikasi bawaan dari beberapa *smartphone* terkenal, *malware* ini mampu terhubung langsung dengan server utama dan kontrolnya untuk mendapatkan daftar komponen sebenarnya yang berisi kode-kode berbahaya.

Pengintaian terhadap Ahmed Mansoor

Ahmed Mansoor adalah aktivis HAM dari UEA. Pada 10 dan 11 Agustus 2016, Mansoor menerima pesan teks SMS di iPhone-nya yang menjanjikan "rahasia baru" tentang tahanan yang disiksa di penjara UEA jika dia mengklik tautan yang disertakan

Oleh Citizen Lab, tautan itu diperiksa dan diketahui memiliki hubungan dengan NSO Group, sebuah perusahaan "perang dunia maya" yang berbasis di Israel yang menjual Pegasus, produk spyware "penyadapan yang sah menurut hukum" milik pemerintah

Sebelumnya, di tahun 2011 dan 2012 Ahmed Mansoor telah menjadi target dari usaha *spyware*

FinFisher di Indonesia

Citizen Lab juga telah melakukan penyelidikan di Indonesia, menelusuri internet, mencari *server* yang mengumpulkan informasi yang dicuri (password, percakapan Skype, rekaman audio/video) dari komputer yang terinfeksi FinFisher.

Citizen Lab menemukan delapan *server* FinFisher di Indonesia pada tiga penyedia jasa ISP yaitu: PT. Telkom, PT. Matrixnet Global, dan Biznet.

Temuan ini telah dilaporkan ke Kementerian Kominfo dan Kominfo berjanji akan mengambil tindakan tegas pada ISP yang terbukti melakukan penyadapan dan pengintaian.

Sumber: cyberthreat.id/ | telset.id/ | apnews.com/ | https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

"X" di bilah judul alih-alih tautan "tutup" di dalam jendela.

- **Pilih "tidak" saat ditanya pertanyaan tak terduga.** Berhati-hatilah dengan kotak dialog tak terduga yang menanyakan apakah Anda ingin menjalankan program tertentu atau melakukan jenis tugas lain. Selalu pilih "tidak" atau "batal", atau tutup kotak dialog dengan mengklik ikon "X" di bilah judul.

- **Berhati-hatilah dengan perangkat lunak yang dapat diunduh gratis.** Ada banyak situs yang menawarkan bilah alat ubahsuaian atau fitur lain yang menarik bagi pengguna. Jangan mengunduh program dari situs yang tidak Anda percayai, dan menyadari bahwa komputer Anda mungkin terpapar spyware dengan mengunduh beberapa program ini.

- **Jangan ikuti tautan email yang mengklaim menawarkan perangkat lunak anti-spyware.** Seperti virus email, tautan tersebut mungkin memiliki tujuan jahat dan justru memasang spyware yang diklaim telah dihapus.

Bagaimana Anda menghapus spyware?

- **Jalankan pemindaian penuh di komputer Anda dengan perangkat lunak anti-virus Anda.** Beberapa perangkat lunak anti-virus akan menemukan dan menghapus spyware, tetapi mungkin tidak menemukan spyware ketika memonitor komputer Anda secara real time. Atur perangkat lunak anti-virus Anda agar meminta Anda menjalankan pemindaian penuh secara berkala.

- **Gunakan produk resmi yang dirancang khusus untuk menghapus spyware.** Banyak vendor menawarkan produk yang akan memindai komputer Anda dari spyware dan menghapus perangkat lunak spyware.

- **Pastikan perangkat lunak antivirus dan anti-spyware Anda kompatibel.** Lakukan pendekatan bertahap untuk menginstal perangkat lunak untuk memastikan bahwa Anda tidak secara tidak sengaja menimbulkan

1.5. Wi-Fi Tak Aman

Kerap kali tanpa berhati-hati, aktivis mengandalkan jaringan Wi-Fi tidak aman, seperti di tempat umum, kafe, atau area sekitar tempatnya bekerja. Jaringan Wi-Fi gratis biasanya tidak aman karena dengan mudah penjahat siber melakukan penyalinan aktivitas Anda dengan *keylogger*.

Untuk lebih aman, gunakan Wi-Fi gratis seperlunya saja di perangkat seluler Anda dan jangan pernah menggunakannya untuk mengakses layanan rahasia atau pribadi, seperti mengakses media sosial, email, informasi perbankan atau kartu kredit. Selain itu, aktifkan VPN/*Virtual Private Network* untuk memintas jalan agar penjahat siber tidak mudah mengakses informasi sensitif yang Anda komunikasikan di internet. (Lihat cara kerja VPN di bagian kedua).

1.6. Menyadap Jaringan

Menyadap jaringan adalah saat penjahat siber menyiapkan titik akses palsu – koneksi yang terlihat seperti jaringan Wi-Fi, tetapi sebenarnya adalah jebakan – di lokasi publik dengan lalu lintas tinggi seperti kedai kopi, perpustakaan, dan bandara. Penjahat dunia maya memberi titik akses nama umum seperti "Wi-Fi Bandara Gratis" atau "Rumah Kopi" untuk mendorong pengguna agar terhubung.

Waspada juga pada teknologi pengawasan bernama StingRay (juga dipasarkan sebagai Triggerfish, IMSI Catcher, Cell-site Simulator atau Digital Analyzer), perangkat mata-mata portabel canggih yang dapat melacak sinyal ponsel di dalam kendaraan, rumah, dan gedung berinsulasi. Pelacak StingRay bertindak sebagai menara seluler palsu (*Fake BTS*), memungkinkan pelaku untuk menentukan lokasi seluler nirkabel yang ditargetkan dengan menyedot data telepon seperti pesan teks, email, dan informasi situs seluler.

Ketika target membuat panggilan telepon, Stingray menipu ponsel agar mengirimkan sinyalnya kembali ke pelaku sehingga mencegah sinyal tersebut kembali ke operator nirkabel target. Namun, tidak hanya melacak ponsel yang ditargetkan, StingRay juga mengekstrak data dari ribuan pengguna ponsel lain yang berada di daerah tersebut.

Dalam beberapa kasus lain, penyerang meminta pengguna membuat "akun" untuk mengakses layanan gratis ini, lengkap dengan sandi. Karena banyak

Cara Kerja Stingray

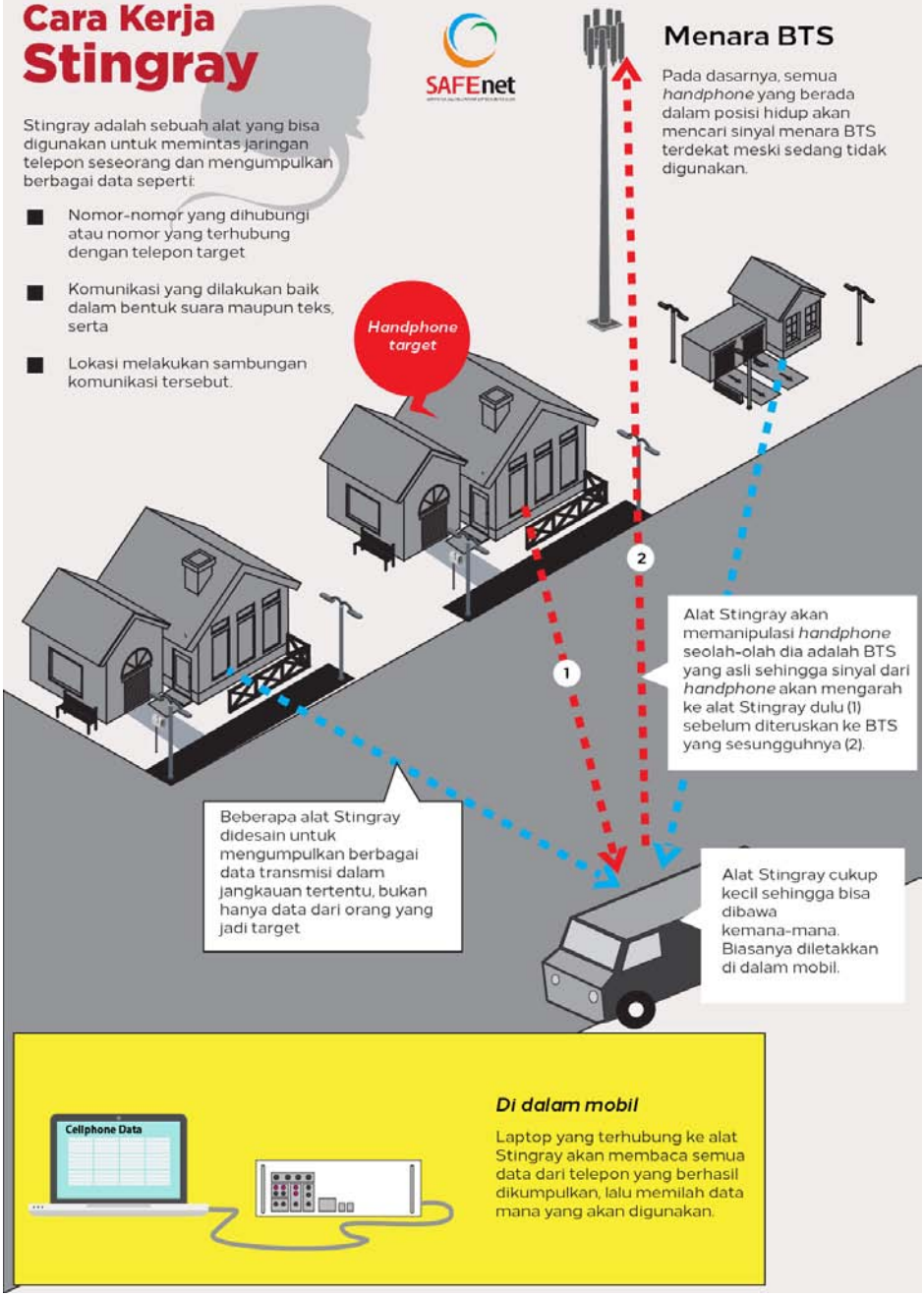
SAFEnet

Stingray adalah sebuah alat yang bisa digunakan untuk memintas jaringan telepon seseorang dan mengumpulkan berbagai data seperti:

- Nomor-nomor yang dihubungi atau nomor yang terhubung dengan telepon target
- Komunikasi yang dilakukan baik dalam bentuk suara maupun teks, serta
- Lokasi melakukan sambungan komunikasi tersebut.

Menara BTS

Pada dasarnya, semua *handphone* yang berada dalam posisi hidup akan mencari sinyal menara BTS terdekat meski sedang tidak digunakan.



Di dalam mobil

Laptop yang terhubung ke alat Stingray akan membaca semua data dari telepon yang berhasil dikumpulkan, lalu memilah data mana yang akan digunakan.

pengguna menggunakan kombinasi email dan sandi yang sama untuk beberapa layanan, peretas kemudian dapat menyusupi email pengguna, e-commerce, dan informasi aman lainnya.

Selain berhati-hati saat menghubungkan ke Wi-Fi gratis dan koneksi jaringan, jangan pernah memberikan informasi pribadi. Dan setiap kali Anda diminta untuk membuat login, baik untuk WiFi atau aplikasi apa pun, selalu buat kata sandi yang unik.

Bagian 2

Proteksi dan Pencegahan Serangan Digital lewat Kebersihan Digital

Kebersihan Digital sering dideskripsikan sebagai kebersihan dalam perilaku digital setiap orang. Kebersihan digital terlihat dalam hal yang sederhana semisal mengatur ikon-ikon di desktop, struktur folder setiap file, membersihkan file sampah dan kemungkinan malware dan virus, hingga penggunaan password dan keamanan jaringan ketika berselancar di dunia maya.

Munculnya istilah Kebersihan Digital adalah dalam rangka menyamakan semangat rutinitas yang waspada dan sadar dalam konteks keamanan di dunia siber di setiap hari. Sama halnya dengan kebersihan badan yang setiap hari kita lakukan.

Istilah Kebersihan digital juga kadang sama dengan istilah lain terkait yaitu **kebersihan siber** (*cyber hygiene*), **keamanan digital** (*digital security*), **kesadaran keamanan siber** (*cyber security awareness*), **internet sehat/aman** (*internet safety*) dan lainnya yang intinya merupakan pedoman keamanan dalam perilaku ketika terkoneksi dan berada di dunia digital –yang setiap orang tidak dapat hindari saat ini.

Jadi, kebersihan digital merupakan praktik keamanan dan kenyamanan dalam interaksi dan identitas Anda di dunia digital. Bagaimana kita mengelola kehidupan digital (*digital life management*) yang produktif dan memproteksi diri

dari kemungkinan tindakan yang berdampak merugikan kita baik secara daring maupun luring.

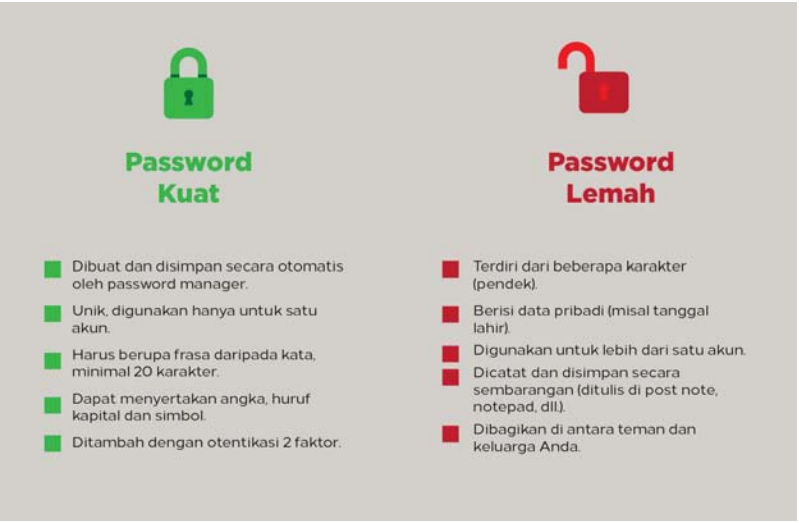
Kebersihan digital merupakan proteksi sederhana,l tetapi penting sebagai garis pertahanan awal untuk melawan ancaman digital yang terus berkembang.

Ancaman digital itu bisa datang dalam bentuk tidak terduga, seperti email atau pesan singkat, rekayasa sosial (*social engineering*), hingga teknik-teknik yang mengancam seperti pengelabuan, peretasan akun dan pencurian data pribadi.

Pada kenyataannya, mayoritas kejadian pelanggaran dan peretasan data disebabkan oleh kesalahan manusia. Saat pandemi seperti sekarang ini, Infosecurity Magazine mencatat serangan siber skala global meningkat drastis hingga 37% dari biasanya. Hal ini menambah tingkat pentingnya proteksi keamanan siber –yang tahun lalu berada di peringkat lima risiko global teratas menurut World Economic Forum pada Laporan Risiko Global 2019, bersama dengan perubahan iklim.

2.1. Menerapkan Manajemen Password yang baik

Penggunaan *password* (kata kunci) pada setiap aplikasi merupakan pada perangkat baik yang terkoneksi langsung dengan internet maupun mengetikkan password di Internet merupakan hal yang rutin kita lakukan.



Berikut ini tipsnya agar aman menggunakan password:

- **Hindari menggunakan password berupa tanggal lahir, nama orangtua, pacar, saudara, dan lainnya yang mudah diidentifikasi.** Termasuk hewan peliharaan, mobil kesayangan dan sejenisnya. Sebaliknya, gunakan password berupa kombinasi angka dan huruf/karakter yang unik dan tidak mudah diidentifikasi orang.

- **Hindari membuat password yang mudah diingat seperti "12345" "admin" "user" "default" "root"** dikarenakan menurut informasi, peretas bahkan tidak perlu menggunakan alat pembongkar password (password breaking tools) karena begitu mudah ditebak. Bahkan menurut ZDNET, angka 123456 muncul 23 Juta kali sebagai password yang sudah bocor.

- **Gunakan parafrase password (Passphrase).** Simpelnya buatlah jembatan keledai kata-kata personal yang selalu dapat diingat misalnya "Saya Pemilik PC Yang Ganteng Tiada Duanya" dengan disingkat menjadi "SayaPPCGT2Nya" yang tentu sulit ditebak. Atau "Sppgtyd!" dengan tambahan tanda "!" dan huruf kapital di awal. Walau panjang, dengan parafrase dan jembatan keledai, maka akan mudah diingat. Tentu gunakan kalimat panjang yang mudah diingat pula.

- Jangan gunakan password yang sama pada semua akun, terutama untuk situsweb finansial atau aplikasi keuangan. Perlakukan password yang berbeda, apabila dua-tiga akun Anda memiliki password yang sama (dan sudah melakukan tips parafrase). Untuk mengecek apakah password yang Anda punya saat ini telah pernah terdeteksi kebocoran, bisa dilakukan di **https://haveibeenpwned.com/Passwords**

2.2. Menggunakan password yang sama itu berbahaya, gunakan Password Manager

Faktor yang membuat password yang kuat juga membuatnya sulit untuk diingat; menggunakan password yang sama pada beberapa akun adalah hal yang berbahaya: jika satu akun diretas, maka penyerang memiliki akses ke semua akun digital Anda: email, internet banking, media sosial, penyimpanan cloud, dll. Meskipun tidak terlalu rumit untuk membuat password yang sesuai dengan kaidah

dasar pemilihan password, membuat satu password untuk satu akun akan sangat menyulitkan bagi Anda untuk mengingatnya. Di sinilah Password Manager berperan.

Password Manager memungkinkan Anda untuk untuk memastikan setiap password Anda adalah unik dan kuat (dihasilkan secara otomatis oleh software) dan menyimpannya dalam database yang aman sehingga Anda tidak perlu mengingatnya atau bahkan mengetiknya. Anda hanya akan perlu mengingat satu password: password untuk mengakses Password Manager itu sendiri.

Salah satu solusi Password Manager yang bisa digunakan adalah LastPass **(https://www.lastpass.com)**. Tata cara aktivasi dan penggunaan password manager LastPass dapat dilihat di lampiran A pada buku panduan ini.

Password manager lain yang bisa digunakan, terutama bila Anda mengelola banyak akun selain akun pribadi, adalah KeepPass **(https://keepass.info/).** KeePass adalah pengelola kata sandi *open-source* yang menyimpan semua data sensitif Anda secara lokal, tidak disimpan di cloud seperti LastPass. Di satu sisi, lebih aman, tetapi di sisi lain, kurang praktis. Anda dapat menyimpan semua kata sandi Anda dalam satu database, yang dikunci dengan kunci master. Jadi, Anda hanya perlu mengingat satu kunci master untuk membuka kunci seluruh database.

Password tidak boleh dibagikan ke orang lain, jika ingin berbagi akses terhadap sebuah akun software password manager bisa memfasilitasi hal tersebut tanpa perlu memberitahukan apa passwordnya.

2.3. Otentikasi Dua Langkah

Otentikasi dua langkah (2FA) adalah lapisan keamanan kedua untuk melindungi sebuah akun atau system saat login. Metode keamanan ini terdiri dari dua tahap otentikasi yang berisikan:

1. Tahap pertama adalah sesuatu yang Anda ketahui (misalnya password)

2. Tahap kedua adalah sesuatu yang Anda miliki (berupa kode yang dihasilkan lewat ponsel, SMS, maupun kode dari stik USB khusus).

Tahap kedua dari otentikasi bisa juga diri Anda sendiri, misalnya jari, wajah, maupun fitur biometrik lainnya.

Biometrik dan Kerentanannya:

Saat ini banyak ponsel menggunakan fitur otentikasi pengguna akan beralih dari sistem password menjadi biometrik. Namun, penggunaan biometrik berupa pengenalan wajah, finger print (sidik jari), yang lazim digunakan pada perangkat yang dibesut teknologi canggih, dalam hal ini bukan tanpa kerentanan. Akan lebih susah peretas jarak jauh untuk mendapatkan akses masuk tanpa mendapatkan data biometrik Anda.

Namun, penggunaan biometrik juga memiliki kelemahan. Penjahat dapat secara fisik menyerang Anda agar dapat memaksa mengakses pembukaan kode dengan menekan jari atau memaksa Anda menghadap ke perangkat untuk membuka kode

biometrik pengenalan wajah. Teknologi baru ini juga terkait dengan pelindungan data pribadi. Biometrik termasuk dalam subyek perlindungan data pribadi yang khas bagi setiap orang sebagai identifikasi.

Untuk itulah, beberapa aplikasi bawaan dari produsen ponsel mengenalkan penjaminan keamanan melalui aplikasi resmi yang bekerja sama maupun dikelola sendiri, misalnya Knoxx untuk Samsung. Jika Anda tidak yakin akan keamanan biometrik Anda dikelola pihak lain, maka tidak disarankan mengaktifkan mode ini.

Otentikasi dua faktor bisa juga berupa lokasi di mana Anda berada (misalnya, ponsel Anda yang mendeteksi bahwa Anda sudah di rumah dan secara otomatis menon-aktifkan kunci layar ponsel.

Tidak semua metode otentikasi dua tahap (2FA) menawarkan tingkat perlindungan yang sama:

- **Berbasis Aplikasi Authenticator**: Opsi ini menggunakan aplikasi yang secara berkala menghasilkan kode khusus di ponsel Anda. Google Authenticator adalah aplikasi yang sangat populer untuk ini; Alternatif lainnya adalah Microsoft Authenticator, Authy, dan FreeOTP. Setiap 30 detik, aplikasi akan menghasilkan 6-digit kode baru yang berlaku sekali pakai. Ini jauh lebih aman dan lebih direkomendasikan daripada otentikasi lewat SMS. Tata cara aktivasi dan penggunaan aplikasi otentikator dapat dilihat pada lampiran B di panduan ini.

- **Berbasis SMS:** Anda diminta menyediakan nomor ponsel saat aktivitasi. Ketika Anda akan login, Anda akan diminta memasukkan kode otentikasi yang secara otomatis akan dikirim ke ponsel Anda. Meskipun ini memberikan peningkatan yang signifikan dalam keamanan akun yang relatif hanya dengan nama pengguna dan password, ini tidak akan menghentikan penjahat siber yang termotivasi dan ahli karena dapat saja mencegah SMS masuk sebelum sampai ke Anda.

- **2FA berbasis push**: Beberapa layanan (Gmail contohnya) akan mengirimkan konfirmasi login ke ponsel Anda dimana Anda dapat menyetujui atau tidak sebuah aktivitas login ke akun Anda. Pemberitahuan ini akan menunjukkan bahwa seseorang (mudah-mudahan Anda) telah mencoba untuk login. Metode ini memberikan perkiraan waktu dan lokasi untuk selanjutkan dapat Anda periksa apakah benar Anda yang berusaha login.

- **Berbasis Kunci Keamanan (FIDO (Fast ID Online) U2F)**: Bukan merupakan mekanisme pengamanan yang sangat popular. Untuk penggunaannya pada suatu situs, Anda perlu mendaftarkan perangkat Anda terlebih dahulu. Setelah terdaftar, saat login situs akan meminta konfirmasi login lewat komputer atau telepon Anda. Perangkat U2F memang membutuhkan biaya, dari 20USD hingga 60USD per unit.

Metode ini disarankan untuk akun yang membutuhkan pengamanan lebih tinggi, seperti administrator TI.

2.4. Mengenali jika akun Anda telah disusupi

Password berubah

Hal pertama yang harus dilakukan adalah memastikan password yang dimasukkan adalah password yang benar, bahkan meskipun telah menggunakan password manager dan praktik pengelolaan password pun, masih memungkinkan terjadinya kesalahan pengguna. Jika tetap tidak bisa masuk, Anda bisa memulai proses pemulihan password.

Ada e-mail yang tidak wajar di folder terkirim Anda

Sering kali, penyerang hanya menggunakan akun Anda untuk mengumpulkan informasi tentang Anda, dan menyembunyikan aktivitas mereka. Mereka bisa saja secara diam-diam mengirimkan email orang-orang di dalam address book Anda dan meminta uang atas nama Anda dan tidak sepenuhnya menutup akses Anda terhadap email Anda.

Adanya email perubahan password secara tiba-tiba

Email setel ulang kata sandi yang tidak Anda minta harus diambil dengan kecurigaan. Jika permintaan tersebut sah dan berasal dari layanan yang sebenarnya Anda gunakan, penyerang mungkin mencoba mengambil alihnya.

Keluhan dari kontak Anda

Jika Anda mulai menerima pesan dari kontak Anda (kolega, keluarga, teman) yang memberitahukan bahwa mereka menerima email aneh dari Anda, ini bisa jadi pertanda seseorang telah menggunakan email Anda untuk mengirimkan email phishing.

Alamat IP, perangkat, dan/atau peramban yang tidak dikenal

Penyedia layanan email biasanya menyediakan fitur yang memungkinkan Anda untuk memeriksa aktivitas login dan lokasi dari mana perangkat Anda terhubung. Sebaiknya periksa fitur ini secara berkala dan lihat jika ada perangkat atau lokasi yang tidak dikenali.

Apa yang harus dilakukan jika Anda merasa akun Anda telah disusupi?

Ubah password Anda

Ini adalah praktik yang baik meskipun Anda hanya sebatas curiga terhadap kemungkinan akun Anda sudah diretas. Password yang dipilih haruslah

panjang dan unik dan gunakan password manager jika memungkinkan. Jika Anda sudah kehilangan akses ke akun Anda, lakukan proses pemulihan password. Jika tidak berhasil, satu-satunya pilihan Anda adalah menghubungi layanan pelanggan dari penyedia email tersebut. Proses ini mungkin akan memakan waktu beberapa hari dan tidak ada jaminan Anda akan mendapatkan akun Anda kembali.

Sekarang saatnya untuk memeriksa pengaturan pemulihan akun pada akun-akun yang Anda miliki. Anda diminta untuk mencantumkan alamat email dan nomor telepon pemulihan ketika Anda membuat akun tersebut, periksa apakah alamat email dan nomor telepon pemulihan sudah benar, jika tidak, segera ubah.

Siapkan otentikasi dua langkah (2FA)

Jika sebelumnya Anda tidak menggunakan autentikasi dua langkah, maka sekarang Anda harus mengaktifkannya. Sebagian besar penyedia layanan email mendukung opsi untuk login dengan otentikasi dua langkah. Unduh dan instalasi Google Authenticator atau Authy, keduanya mudah disiapkan.

Beritahu teman dan keluarga Anda

Beberapa dari mereka mungkin sudah memberitahu Anda tentang adanya aktivitas yang mencurigakan dari akun Anda. Anda pun harus sesegera mungkin memberitahu yang lain agar mereka tidak menjadi

mangsa serangan phishing yang menggunakan nama dan alamat email Anda.

Periksa penerusan akun, balasan otomatis, dll.

Penerusan otomatis dan balasan otomatis bukanlah fungsi umum digunakan sehari-hari. Untuk mengakses pengaturannya juga terkadang rumit dan berbelit tapi Anda harus memeriksa apakah fitur ini aktif atau tidak. Anda bisa saja telah mengubah password Anda, tetapi jika fitur penerusan akun dan balasan otomatis dalam keadaaan aktif, maka semua informasi yang dikirim ke email Anda akan dikirimkan juga ke email penyerang.

Periksa opsi keamanan tambahan

Cari opsi keamanan lain yang disediakan oleh penyedia layanan email Anda, atau opsi keamanan lain yang secara spesifik disediakan oleh perangkat Anda. Opsi ini bisa berupa peringatan jika ada aktivitas login dari perangkat atau lokasi baru, atau opsi untuk menghapus perangkat atau akun dari jarak jauh jika hilang atau dicuri. Pilih opsi yang dibutuhkan, dan aktifkan.

Periksa apakah ada akun lain yang terpengaruh

Karena adakalanya email Anda digunakan untuk mengamankan akun lain, maka penting untuk memeriksa apakah ada akun lain yang terpengaruh. Pastikan Anda dapat masuk ke akun lain tersebut,

dan pertimbangkan untuk merubah password dari akun itu. Jika Anda menghadapi kesulitan mengakses salah satunya, segera ambil tindakan untuk mereset password atau menghubungi layanan pelanggan penyedia layanan.

Jalankan antivirus dan bersihkan perangkat Anda

Penyerang mungkin telah memperoleh akses ke akun Anda melalui malware atau celah keamanan yang ada pada perangkat Anda. Jika Anda menjalankan proses pemulihan akses ke akun email Anda, pastikan Anda terlebih dahulu menjalankan antivirus untuk mendeteksi dan menghapus spyware, keyloggers, dan jenis malware lainnya.

Meminta bantuan

Anda tidak sendiri. Saat ada yang menyerang akun Anda ini bisa sangat menegangkan. Jangan ragu untuk bertanya kepada teman atau kolega.

Bila mendapat serangan digital dan membutuhkan bantuan, Anda bisa menghubungi:

SAFEnet
Formulir: s.id/laporserangan
Email: aduan@safenet.or.id
Hotline: 08119223375

Untuk penjelasan lebih lengkap tentang pelaporan serangan digital akan dijelaskan dalam Lampiran C di halaman akhir.

2.5. Peran Anda untuk menjaga agar pemilu tetap aman

Perbarui software dan sistem operasi semua perangkat Anda

Menjaga sistem operasi, antivirus, dan software lain tetap mutakhir adalah hal yang sangat penting untuk memastikan keamanan perangkat Anda, dan pemeriksaan rutin untuk memastikan bahwa fungsi pembaruan otomatis berfungsi dengan baik dan benar harus senantiasa dilakukan.

Perbarui Sistem Operasi Anda dan software lain secara berkala

Sistem operasi dan software lainnya perlu diperbarui secara berkala untuk menutup celah kerentanan dan memastikan data Anda terlindungi.

Yang harus Anda lakukan: Perusahaan pengembang software secara teratur merilis tambalan *(patch)* dan pembaruan, terutama ketika mereka menemukan adanya celah keamanan pada software tersebut. Segera instalasi tambalan dan pembaruan yang disediakan untuk menjaga perangkat Anda aman dari ancaman terbaru. Sangat disarankan untuk mengaktifkan pembaruan otomatis sehingga proses pembaruan berlangsung secara teratur.

Setelah periode waktu tertentu, sistem operasi akan mencapai apa yang disebut sebagai akhir masa hidup komputer *(computer end-of-life)*. Ini adalah fase di mana pabrikan/pengembang software akan berhenti

memberikan dukungan, termasuk menyediakan pembaruan maupun tambalan keamanan.

Anda harus hati-hati mempertimbangkan risiko yang ditimbulkan atas penggunaan komputer yang sistem operasinya sudah tidak disokong lagi oleh pabrikan, karena penyerang biasanya menyasar mesin-mesin yang masih menggunakan system operasi ini.

Misalnya, dukungan untuk Windows XP berakhir pada 8 April 2014, setelah 12 tahun Microsoft tidak lagi menyediakan pembaruan keamanan untuk sistem operasi ini. Microsoft Windows 7 mencapai akhir masa pakainya 14 Januari 2020 dan harus ditingkatkan ke Windows 10 juga.

Untuk ponsel Android, waktu dukungan sebenarnya jauh lebih pendek dan patch keamanan biasanya berhenti didistribusikan setelah 3 hingga 4 tahun.

Memastikan antivirus Anda aktif dan up-to-date

Antivirus garis depan pertahanan komputer Anda terhadap malware. Tidak perlu menginstal beberapa antivirus sekaligus dalam sebuah perangkat (mereka mungkin saling mengganggu). Instalasi satu saja yang efektif dan Anda percayai.

Yang harus Anda lakukan: Menginstal antivirus saja tidak cukup, penting untuk memperbarui antivirus secara rutin.

Amankan Perangkat Mobile Anda

Telpon seluler (ponsel) telah menjadi "sahabat" terbaik banyak orang saat ini, memang sangat bermanfaat

tapi juga mendatangkan risiko. Pasalnya, saat ini telpon genggam bukan saja sebagai alat komunikasi dan penyimpan data, tapi juga berfungsi sebagai dompet dan pusat jaringan sosial pengguna. Dengan fungsi-fungsi tersebut, menjaga keamanan ponsel pun menjadi semakin penting. Jika keamanan ponsel berhasil ditembus oleh peretas, maka yang terdampak bukan saja pemilik ponsel tersebut, namun juga lembaga tempat dia bekerja.

Berikut adalah tips untuk mengamankan dan menghindari peretasan pada ponsel.

- Update ponsel secara berkala baik sistem operasi maupun aplikasi yang diinstall
- Lakukan update berkala untuk memastikan sistem operasi ponsel, program serta aplikasi yang terpasang di ponsel senantiasa yang paling terkini.
- Pasang pengunci layar (lockscreen, sidik jari, pengenalan wajah) untuk mencegah akses orang lain
- Langkah ini adalah "pagar" pertama untuk menjaga ponsel Anda, aktifkan lockscreen baik berupa PIN, pattern, sidik jari, pengunnci wajah pada ponsel. Jangan aktifkan pengaturan agar ponsel masuk mode standby dan terkunci secara otomatis setelah periode waktu tertentu (missal 30 detik).
- Hindari terhubung dengan jaringan Wi-Fi publik
- Koneksi pada Wi-Fi publik (café, hotel, mal, dsb)

seringkali tidak aman karena tidak terlindungi dan dapat disusupi serangan *Man-in-the-middle* yang memungkinkan akses terhadap arus komunikasi dan bahkan ponsel Anda.

- Jangan *root/jailbreak* ponsel untuk mengurangi resiko peretasan. *Root* atau *jailbreak* adalah proses menghilangkan batasan yang diberlakukan pada ponsel Android dan Apple. Melakukan root/jailbreak pada ponsel Anda akan memungkinkan aplikasi pihak ketiga untuk mengakses ponsel tersebut. Hal ini berpotensi membuat pihak lain mengetahui semua informasi yang tersimpan dan dikirimkan pada ponsel itu, bahkan untuk memata-matai aktivitas Anda.

- Hanya instalasi aplikasi dari sumber resmi Play/Playstore. Aplikasi yang ada Google Play (Android) atau Apple Appstore (iOS) lebih aman karena keduanya adalah layanan store resmi terpercaya yang memiliki aturan ketat untuk mencegah aplikasi jahat.

- Aktifkan enkripsi data/SD Card. Enkripsi data adalah solusi dasar dalam melindungi informasi yang disimpan di ponsel Anda. Dengan enkripsi data, maka data di ponsel Anda akan diacak dengan kunci tertentu, jika ponsel Anda hilang, orang lain tidak bisa membaca data dalam ponsel tanpa *decryption key*.

- Aktifkan Find dan Wipe My Device. Ketika ponsel hilang atau dicuri, Anda dapat mengunci ponsel dan bahkan menghapus data pada ponsel

tersebut dari jarak jauh. Dengan cara ini, akses illegal terhadap informasi sensitif milik Anda dan organisasi Anda bisa terjaga.

- Aktifkan *phone backup* dan *folder backup*. Untuk mengantisipasi serangan malware yang berakibat pada hilangnya data atau ketika ponsel tersebut hilang, buatkan backup data di tempat lain sehingga data tetap bisa diakses dan diperbarui. Mengaktifkan fitur backup otomatis di layanan cloud akan sangat membantu Anda saat pemulihan paska insiden. Baik Google (Drive) dan Apple (iCloud) menyediakan fitur backup data di cloud. Pastikan perangkat Anda terhubung dan dibackup pada layanan tersebut.

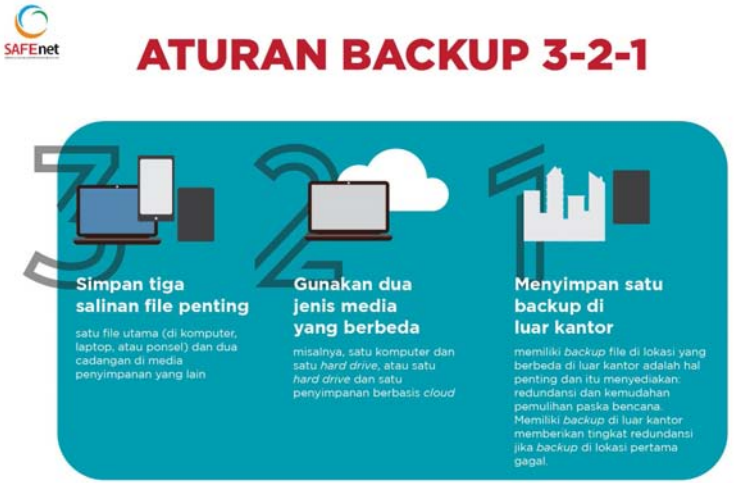
Waspadalah dengan software bajakan dan tidak berlisensi

Software bajakan dapat secara diam-diam tanpa sepengetahuan Anda menginstal malware ke perangkat Anda yang akan menyebabkan masalah pada perangkat tersebut. Dalam situasi tertentu mungkin sulit untuk mendapatkan software berlisensi, dalam situasi tersebut, Anda sebaiknya mencari software alternatif yang bersifat open source dan gratis, dan berkoordinasi dengan bagian Anda untuk menganggarkan software berlisensi.

Selalu instalasi software dari situs web resmi. Ada banyak sekali situs web yang menyediakan Salinan file instalasi software, tapi banyak dari mereka yang tidak jelas keamanannya.

Strategi backup yang baik dimulai sekarang

Pilih media penyimpanan backup, bisa berupa perangkat penyimpanan fisik (stik USB, hard drive portable/eksternal), sistem jaringan internal (biasanya dikelola oleh lembaga, ini adalah tempat di mana Anda dapat meletakkan file Anda di jaringan organisasi Anda), atau sistem berbasi cloud (misalnya Dropbox atau Google Drive).



Untuk file Anda yang paling penting, coba ikuti aturan 3-2-1:

3 - Simpan tiga salinan file penting, satu file utama (di komputer, laptop, atau ponsel) dan dua cadangan di media penyimpanan yang lain.

2 - Gunakan dua jenis media yang berbeda; misalnya, satu komputer dan satu *hard drive*, atau satu *hard drive* dan satu penyimpanan berbasis *cloud*.

1 - Menyimpan satu backup di luar kantor, memiliki *backup file* di lokasi yang berbeda di luar kantor adalah hal penting dan itu menyediakan: redundansi dan kemudahan pemulihan paska bencana. Memiliki *backup* di luar kantor memberikan tingkat redundansi jika *backup* di lokasi pertama gagal.

Idealnya file Anda dibackup secara otomatis untuk mengurangi masalah keharusan mengingat untuk melakukan backup. Tapi Anda perlu memeriksa apakah backup otomatis berfungsi sebagai mana mestinya.

Pada suatu titik, Anda akan membutuhkan *backup* data Anda. Entah itu karena kerusakan perangkat atau karena serangan siber. Memang membutuh waktu, tenaga, dan dana yang tidak sedikit untuk membuat backup secara benar, namun usaha yang dikeluarkan jauh lebih sedikit daripada yang Anda perlukan untuk membuat ulang file Anda yang hilang, itu pun jika dimungkinkan.

Risiko perangkat USB

Satu hal yang pasti, ketika sebuah perangkat USB hilang, maka hilang juga data yang ada di dalamnya. Kehilangan perangkat USB yang berisi data sensitif perusahaan dapat berujung pada pengumuman telah terjadi insiden keamanan, penyelidikan internal, dan mungkin teguran - atau bahkan hilangnya pekerjaan dan tuntutan atas Anda di pengadilan.

Apa yang harus Anda lakukan: Berhati-hatilah agar perangkat USB Anda tidak hilang, tetap jaga agar tetap aman dan dalam kendali Anda. Jika memungkinkan gunakan password atau enkripsi pada perangkat USB tersebut. Segera hapus file yang sensitive setiap kali Anda selesai mentransfer file dan jangan simpan dalam USB stik tersebut.

Sebuah penelitian menunjukkan bahwa hampir 50 persen orang yang menemukan flashdisk USB akhirnya memasukkan perangkat tersebut ke komputer mereka tanpa melakukan tindakan pencegahan apa pun. Dibutuhkan pakar keamanan dengan PC yang aman dan peralatan keamanan khusus untuk memeriksa apakah flash-drive USB yang ditemukan adalah aman. Jangan mencoba membukanya di laptop Anda.

Yang harus Anda lakukan: Jika Anda menemukan flash drive USB, biarkan saja, atau taruh di tempat sampah. Jangan memasangnya di computer Anda. Jangan langsung menggunakan *flash-drive* USB gratisan yang disediakan selama konferensi (materi acara bisa dikirimkan lewat email).

Penting untuk menjaga dan menyimpan perangkat stik USB Anda, begitu juga menjaga reputasi Anda. Keamanan dan privasi dapat dilanggar dengan cara yang sangat memalukan jika Anda meminjamkan stik USB ke kolega yang ternyata di dalam stik USB tersebut ada file-file personal Anda.

Apa yang harus Anda lakukan: Pertimbangkan memiliki area penyimpanan khusus untuk menjaga perangkat penyimpanan pribadi Anda terpisah dari yang Anda gunakan untuk bekerja, dan berhati-hatilah untuk memeriksa isi dari sebuah drive sebelum menyerahkannya kepada siapa pun.

Risiko Bermedia sosial

Apa pun platform layanan media sosial yang Anda gunakan, pertimbangkan jenis informasi yang Anda bagikan dengan orang lain pada platform media sosial tersebut. Berikut adalah risiko umum terkait dengan penggunaan media sosial:

- Batasi berbagi informasi sensitif pribadi. Berhati-hatilah tentang seberapa jauh informasi pribadi (seperti nama lengkap, alamat, tanggal lahir, nomor telepon, atau tempat lahir Anda) yang Anda tampilkan di situs jejaring sosial. Semakin banyak informasi yang Anda posting, semakin mudah bagi penyerang atau orang lain untuk menggunakan informasi tersebut untuk mencuri identitas Anda, mengakses data Anda, atau melakukan kejahatan lain seperti menguntit.

- Memasang konten/postingan yang meragukan: dapat berupa gambar, video, atau opini yang mungkin membuat Anda tampak tidak professional, kasar, dan dapat merusak reputasi Anda. Ingatlah bahwa apa yang diunggah di internet tidak akan pernah sepenuhnya terhapus, bahkan ketika Anda sudah menghapus konten tersebut.

- Stop berbagi lokasi Anda. Banyak platform media sosial memungkinkan Anda untuk menggunakan fitur *check in* dan membagikan lokasi Anda, atau secara otomatis menambahkan lokasi Anda ke foto dan postingan. Tiba-tiba, informasi yang Anda bagikan kepada publik bahwa Anda sedang menghadiri sebuah konferensi dapat digunakan untuk membuat email phishing terarah yang berisi tautan berbahaya kepada Anda.

- Awas terjebak hoaks. Anda bisa jadi korban atau Anda bisa jadi penyebar hoaks bila tidak berhati-hati ketika menerima informasi di media sosial. Karenanya Anda perlu untuk memverifikasi informasi dari kedua belah pihak yang bertarung di pilkada, atau bila Anda tidak yakin dengan kebenaran informasinya, lebih baik informasi itu tidak diedarkan lagi dan berhenti di Anda.

Salah satu tempat untuk melakukan pengecekan fakta, adalah lewat situs Cekfakta.com yang dikelola oleh media-media yang tergabung untuk melakukan pemeriksaan fakta atas klaim atau informasi yang beredar di media dan media sosial.

8 Tips
Bijak Menggunakan Media Sosial

01

Tidak ada tombol "delete" di internet

Pikirkan baik-baik apa yang Anda posting di internet. Meski postingan telah Anda hapus namun bisa saja orang sudah terlanjur melakukan *screenshot* atau tangkapan layar pada postingan tersebut.

02

Jangan sebarkan lokasi Anda

Fitur check in atau geo tagging bukan fitur yang aman digunakan. Orang bisa dengan mudah mengetahui lokasi Anda, apalagi bila dia adalah penguntit. Orang pun bisa tahu dengan mudah Anda tidak ada di rumah.

03

Hanya terhubung atau berkomunikasi dengan orang yang Anda percaya

Waspadalah dan hanya lakukan koneksi dengan orang yang benar-benar Anda kenal. Orang bisa menjadi siapa saja di dunia maya dan tidak bisa benar-benar dipercaya.

04

Perhatikan keberadaan Anda di dunia maya

Jika memungkinkan, batasi informasi tentang Anda di dunia maya. Gunakan fitur pengaturan kerahasiaan dan keamanan di media sosial yang Anda gunakan.

05

Pastikan beberapa hal tetap rahasia

Ada beberapa informasi yang sebaiknya tidak dibagikan di media sosial. Misalnya, tanggal lahir dan foto-foto keluarga yang sensitif. Ini bisa memudahkan pencurian data dan informasi sosial.

06

Hargai privasi orang lain

Hanya posting tentang orang seperti orang lain memposting tentang Anda

07

Sampaikan apabila postingan tentang Anda membuat tidak nyaman

Sampaikan jika ada orang lain yang memposting sesuatu yang membuat Anda tidak nyaman.
Di sisi lain Anda juga harus berpikiran terbuka jika ada orang lain yang mengutarakan ketidaknyamannya terhadap postingan Anda

08

Bertanggung jawab pada isi media sosial Anda

Anda bisa saja secara tidak sengaja menyebarkan berita yang ternyata tidak benar. Bila itu terjadi, segera koreksi postingan tersebut.
Bertanggungjawablah pada apa yang sudah Anda sebarkan di media sosial

Apa yang harus dilakukan bila akun media sosial Anda diambil alih/diretas?

- Melaporkan peristiwa tersebut ke platform teknologi. Setiap platform teknologi memiliki dashboard online untuk melaporkan gangguan dan serangan digital yang Anda alami.
- Memberitahukan segera kawan-kawan dan organisasi kalau akun media sosial Anda telah diretas dan dikuasai oleh penyerang.
- Meminta kawan-kawan dan organisasi mewaspadai dan mengeluarkan akun media sosialmu dari grup-grup yang bersifat *case-sensitive*.
- Begitu akun media sosial berhasil dipulihkan dan dikembalikan, segera tingkatkan keamanan digital. Instalasi ulang aplikasi dengan update terbaru dan langsung aktifkan fitur keamanan 2FA-Otentifikasi Dua Faktor.

2.6. Mengamankan jaringan internet Anda di rumah

Organisasi dan perusahaan dari baik skala besar, menengah, maupun kecil telah mengadopsi praktik kerja dari rumah untuk memastikan kelangsungan bisnis selama pandemi COVID-19. Perubahan dalam kegiatan usaha selalu memiliki dampak risiko keamanan. Cara kerja baru membutuhkan langkah-langkah keamanan baru; tetapi biasanya risiko ini seiring waktu akan berhasil dikelola dengan hati-

hati. Sayangnya, penjahat siber telah terlebih dahulu melihat peluang di tengah pandemi, dan telah melancarkan serangkaian serangan.

(Email phishing telah melonjak lebih dari 600% sejak akhir Februari dengan upaya untuk mengelabui pengguna agar menyerahkan informasi login dan informasi keuangan mereka, dan/atau secara tidak sengaja mengunduh malware ke komputer mereka).

Percakapan Instan (Chat)

Aplikasi chat telah menjadi alat yang nyaman untuk mentransfer file, menyimpan catatan, dan dapat berfungsi sebagai penyimpanan berbasis cloud; oleh karena itu, keamanan chat merupakan komponen penting untuk mengamankan komunikasi. Indonesia pernah mengalami serangan siber yang menirukan akun chat pejabat penyelenggara pemilu di masa lalu. Bentuk serangan ini bisa jadi akan digunakan lagi di masa yang akan datang.

Apa yang harus Anda lakukan:

- **Hati-hati terhadap serangan phishing di melalui aplikasi chat, seseorang dapat berpura-pura sebagai kolega atau atasan Anda. Bagikan informasi seperlunya dan gunakan media lain jika Anda ragu.**

- **Aktifkan fitur otentikasi 2 langkah (2FA) jika memungkinkan. Setiap aplikasi chat saat ini sudah dilengkapin dengan fitur keamanan 2FA. Aktifkan PIN/2FA pada akun Whatsapp, Line, Telegram Anda.**

Konferensi video

Terlepas instruksi untuk kerja dari rumah akan menjadi tren jangka panjang atau tidak, konferensi video secara online telah menjadi aktivitas normal dan kemungkinan besar akan tetap menjadi metoda pelaksanaan kursus pelatihan, rapat online, dan komunikasi reguler. Kesimpulannya: Kebutuhan konferensi video akan selalu ada.

Ada beberapa risiko yang harus diperhatikan saat menggunakan layanan konferensi video:

- *Zoom-Bombing* terjadi ketika peserta yang tidak diundang menggunakan konferensi video online untuk menyebarkan konten yang tidak pantas. **Apa yang harus Anda lakukan: Pastikan Anda merahasiakan kata sandi, buat ruang tunggu sehingga Anda dapat mengizinkan peserta sebelum rapat dimulai.**

- Kerentanan keamanan masih ditemukan di Zoom, Microsoft Teams, dan pada dasarnya terus ditemukan. **Yang harus Anda lakukan: Perbarui software dan atur ke pembaruan software otomatis jika memungkinkan.**

- Gunakan aplikasi yang direkomendasikan oleh lembaga Anda. Ini penting karena beberapa percakapan Anda mungkin sensitive.

- Beberapa aplikasi konferensi video meminta Anda untuk mengunduh file .exe agar dapat bergabung dalam rapat online, pastikan file yang

diunduh berasal dari website resmi penyedia layanan konferensi video dan bukan dari website/ orang lain.

Mengamankan jaringan internet Anda di rumah

Bekerja dari rumah sebenarnya dapat menimbulkan risiko bagi lembaga. Di kantor biasanya ada bagian khusus uang mengurus soal keamanan siber. Tetapi ketika karyawan bekerja dari rumah, mereka harus mengurusnya sendiri. Dengan berkembangnya kebijakan bekerja dari rumah, kemungkinan rumah telah menjadi kantor kedua, risiko bertambah lagi ketikan karyawan menggunakan komputer pribadi mereka untuk pekerjaan.

Ada beberapa langkah penting untuk mengamankan wifi di rumah Anda, dan sebagian besar pengguna belum mungkin pernah mendengarnya, tetapi penting untuk memastikan bahwa tidak ada yang dapat mencegat jalur komunikasi rumah Anda atau mengalihkan kendali router rumah Anda kepada penyerang.

Keamanan Koneksi Wi-Fi Anda

Seperti halnya aturan password untuk semua akun, password haruslah panjang (minimal 20 karakter) dan sulit ditebak. Jika sudah kuat, Anda tidak perlu terlalu sering mengubahnya.

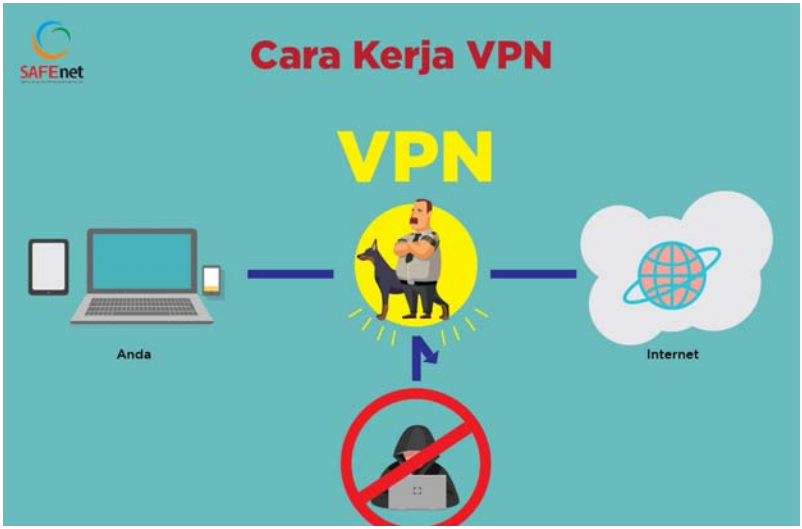
Periksa apakah Wi-Fi Anda menggunakan protokol enkripsi WPA2 yang sangat direkomendasikan.

Penggunaan WEP dan WPA1 tidak disarankan karena tidak aman.

Pengaktifan VPN

Sebagai aktivis, kita mungkin sempat berpikir bahwa bersembunyi di balik nama samaran dan mendaftar dengan akun email buangan sudah cukup melindungi, tapi ternyata hal tersebut masih bisa dilacak, terutama karena alamat *Internet Protocol* (IP) dapat dengan mudah dilacak.

Layanan Virtual Private Network/VPN dapat mengubah IP kita, atau, lebih baik lagi, memampukan kita pindah IP ke lokasi geografis yang jauh, memberi kita kebebasan untuk mengatakan apa pun di platform media sosial, bagian komentar atau forum.



Saat kita anonim, kita dapat mengakses situs web apa pun yang kita inginkan, dan tidak ada yang akan tahu kita pernah ke sana. Tidak ada yang akan dapat menarik catatan kita dan berkata, "Lihat, pada hari tertentu bulan lalu Kita telah mengunjungi situs web dewasa ini, belanja barang ini dari toko online dan menambahkan nama Kita dalam petisi ini."

Tabel: Perbandingan Keuntungan Menjadi Anonim dan Bisa Dikenali

Kategori	Keuntungan Menjadi Anonim	Keuntungan Dikenali
Hubungan sosial	Menghindari tidak disukai orang Terhindar dari komitmen pada komunitas Tidak ada halangan dalam hubungan baru Melindungi orang lain yang disayangi	Terhubung dengan teman sejati Hubungan sosial akan semakin menguat Mendorong lebih partisipasi
Reputasi dan kepercayaan	Memberikan nilai dan rekomendasi secara jujur	Bagus untuk membangun reputasi Memperoleh kepercayaan dari pengguna lain
Membangun citra	Punya kontrol atas citra diri Dapat menghindar dari rasa malu/penilaian/kritik	Menghindari kritik yang tajam Konsisten dengan citra diri

Manfaat emosional	Terasa santai dan nyaman Terasa keren dan seru	Terasa nyata, punya integritas Merasa lebih dekat dengan orang
Menyatakan pendapat	Terasa bebas saat menyampaikan pandangan	Terhindar dari tingkah laku yang tidak bertanggung jawab
Privasi	Lebih punya kontrol pada pengungkapan informasi pribadi	Terlihat polos
Keamanan	Melindungi keamanan diri Terhindar dari penuntutan hukum/spam/pengintaian	Tersembunyi dalam kerumunan
Kemudahan penggunaan	Butuh usaha untuk log in	Mudah mengingat akun

Menjadi anonim juga berarti kita dilindungi dari peretas, pengintai dan pengamat pada umumnya. Anonimitas melindungi kita agar tidak ada yang bisa mengetahui siapa kita, di mana kita tinggal, dan sebagainya. Anonimitas juga penting dalam hal keamanan data. Data pribadi kita mungkin tidak tampak begitu penting atau berharga bagi kita, tetapi tentu saja terlalu banyak "orang jahat" hanya menunggu kita untuk membuka informasi, bertransaksi, mengirim informasi.

Ada beberapa cara yang dapat membantu kita mencapai anonimitas penuh, dan salah satu yang paling efisien adalah VPN. Data kita akan dienkripsi dan lalu lintas Kita dilindungi. Lebih penting lagi, VPN menjamin anonimitas kita. VPN akan menutupi alamat IP asli kita dan dengan membuat terowongan terenkripsi tempat semua lalu lintas kita bergerak.

Pengaturan router Anda

Router kerap masih menyematkan username dan password standar bawaan pabrik (periksa situs web pabrikan, bisa jadi TP-Tautan, Cisco Tautansys, ZTE, Huawei).

Maka Anda perlu masuk ke halaman administrasi *router*, lakukan hal berikut ini:

Ubah *password* standar administrator *router* dan nama jaringan Wi-Fi. Jika Anda belum melakukannya, maka sangat penting bagi Anda untuk mengubahnya segera untuk menjaga router dari serangan. Ini karena nama jaringan Wi-Fi bawaan pabrik masih

menyertakan informasi merk dan model dari *router*, dan informasi tentang standar username dan password untuk masing-masing merk router banyak disediakan di internet.

Nonaktifkan akses jarak jauh. Terkadang pabrikan memberikan opsi untuk menghubungkan dan mengubah pengaturan *router* Anda dari jarak jauh. Meskipun hal ini praktis bagi tim teknis untuk perbaikan koneksi Anda dari jauh, ini juga memungkinkan penjahat siber untuk mengendalikan koneksi Anda dan pada dasarnya melakukan apa pun yang mereka inginkan dengannya.

Periksa pembaruan *firmware*. Sama seperti komputer, produsen *router* berusaha untuk menemukan celah kerentanan baru dan membuat tambalannya. Pada bagian administrator, ada menu khusus untuk melihat apakah ada pembaruan atas *firmware router* tersebut. Anda juga dapat merujuk ke situs web pabrikan untuk mengetahui *firmware* terkini.

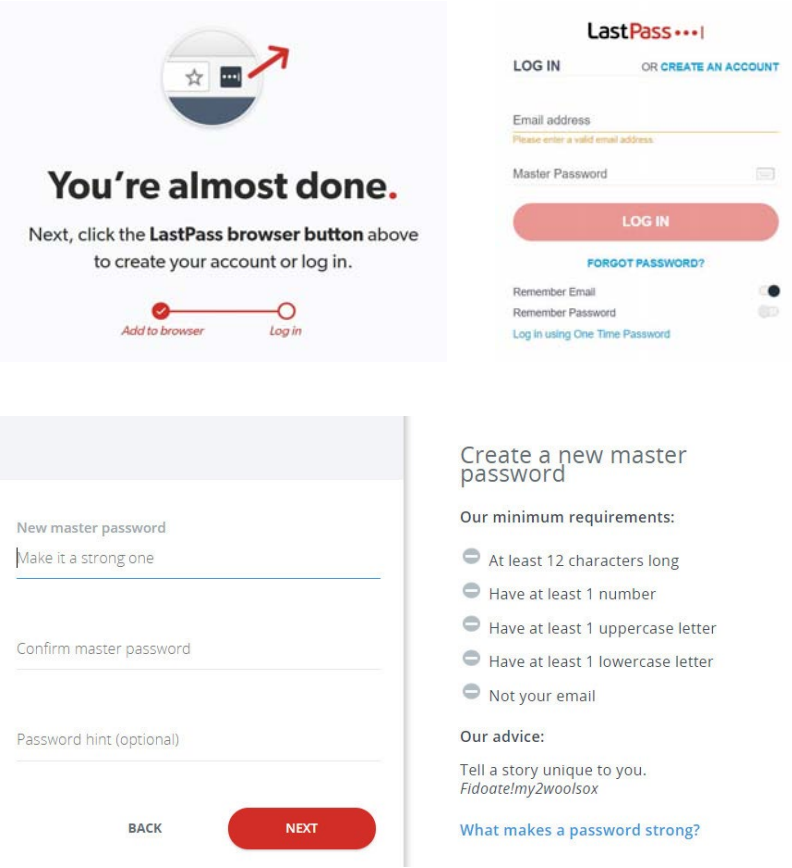
LAMPIRAN A

Cara aktivasi dan penggunaan LastPass

1. Unduh dan instalasi ekstensi LastPass di peramban Anda (Firefox, Chrome)
2. Setelah terpasang, akan muncul ikon LastPass di toolbar peramban (bagian kanan atas peramban).
3. Klik ikon LastPass.
4. Pilih 'Create an Account Now.'
5. Ketik alamat email dan buatlah password utama (master password) yang kuat.
6. Pada halaman utama, login menggunakan akun yang sudah dibuat.
7. Ketik username dan password.
8. Klik ikon Lastpass di dalam kolom password.
9. Klik 'Save credentials for this site.'

Anda juga bisa masuk ke berbagai layanan dan aplikasi yang Anda pakai, lalu menyimpannya di Lastpass saat muncul pemberitahuan. Setelah itu akun LastPass secara berkelanjutan menyimpan data Anda pada database penyimpanannya. Semua kata sandi dan informasi login Anda akan disimpan secara aman.

Ketika Anda mengunjungi website/layanan yang sudah didaftarkan di LastPass, maka secara otomatis LastPass akan memasukkan username dan password Anda.



Tampilan ekstensi LastPass pada peramban

Jika Anda membutuhkan LastPass di perangkat yang lain, silakan unduh dan instalasi dari Google Play atau Apple Appstore – sesuai perangkat yang Anda pakai. Nanti aplikasi akan melakukan sinkronisasi, sehingga Anda tidak perlu repot mengisi akun dan kata sandi di perangkat tersebut.

LAMPIRAN B

Cara aktivasi dan penggunaan Google Authenticator pada Akun Google

Mempersiapkan Google Authenticator

1. Unduh dan instalasi Google Authenticator dari Google Play Store (Android) atau Apple App Store (iOS) sesuai dangan ponsel Anda

2. Buka aplikasi Google Authenticator pada ponsel Anda dan log in ke akun Google Anda

Aktivasi 2FA dengan Google Authenticator pada akun Google

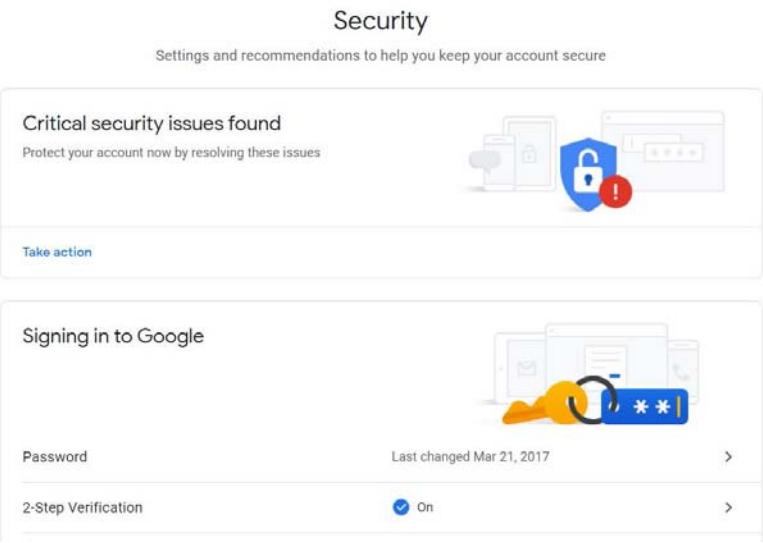
1. Pada laptop, buka Akun Google melalui myaccount.google.com.

2. Di bagian atas, di panel navigasi, ketuk Security/ Keamanan.

3. Di bagian "Login ke Google", ketuk Two Factor Authentication/ Verifikasi 2 Langkah. Anda mungkin akan diminta login.

4. Di bagian "Tambahkan langkah kedua lainnya untuk memverifikasi ini memang Anda", di bawah "Aplikasi Authenticator", ketuk Siapkan.

5. Ketika muncul pop up untuk memilih jenis perangkat Android atau iPhone, pilih perangkat yang Anda kehendaki. Sebuah kode barcode untuk perangkat tersebut akan ditampilkan.



Tampilan pengaturan security pada myaccount.google.com

6. Buka Aplikasi Google Authenticator pada ponsel Anda dan pilih scan barcode.
7. Dari ponsel, scan barcode yang ditampilan pada laptop (langkah no. 5). Setelah scan, akan muncul kode (6 digit) lalu klik tambah akun.
8. Kembali lagi ke laptop, jika sudah menambah akun, klik selanjutnya/next, akan muncul kotak untuk mengisi kode 6-digit dari Google Authenticator.
9. Masukan kode 6-digit yang ditampilkan oleh Google Authenticator pada kotak tersebut.
10. Klik verify dan selesai.

LAMPIRAN C

Langkah-langkah Pelaporan Serangan Digital Melalui SAFEnet

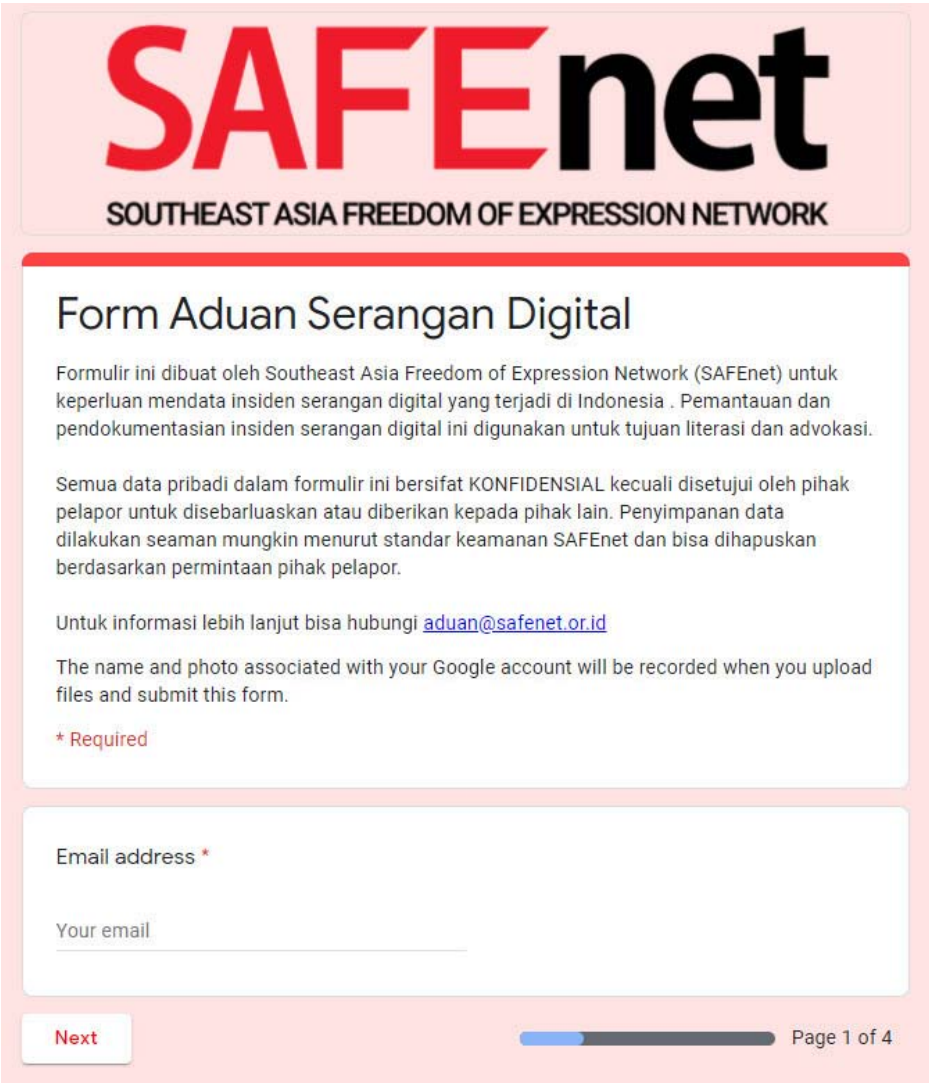
Jika menjadi korban serangan digital, Anda bisa melaporkan ke SAFEnet. Sebelum melaporkan, siapkan informasi berikut:

- Identitas Anda (nama dan nomor kontak) untuk verifikasi
- Jenis platform yang diserang (medsos, aplikasi pesan ringkas, dll)
- Kronologi dan bukti serangan
- Dukungan yang diharapkan dari SAFEnet

Laporkan ke SAFEnet melalui salah satu saluran berikut:

- Mengisi form daring di s.id/laporserangan
- Mengirim email ke aduan@safenet.or.id
- Mengontak hotline, WhatsApp, atau Telegram di +62 8119223375
- Mengabari langsung lewat Direct Message ke IG atau Twitter @SAFEnetVoice

Tim Reaksi Cepat (TRACE) SAFEnet akan menghubungi untuk memverifikasi dan memberikan respon sebagaimana yang dibutuhkan berdasarkan informasi ke saluran aduan SAFEnet.



Halaman form pengaduan SAFEnet

SOUTHEAST ASIA FREEDOM OF EXPRESSION NETWORK

2020