

**TULAR
NALAR**

PERLINDUNGAN DATA PRIBADI



PERLINDUNGAN DATA PRIBADI

PENULIS	: Novi Kurnia
PENYUNTING	: Giri Lumakto, Dwitasari Teteki Bernadeta, Niken Pupy Satyawati
PENYELARAS KATA	: Dwitasari Teteki Bernadeta, Axel Gumilar
DESAIN & PENATA LETAK	: Ken Zachary, Seto Prayogi
SUPERVISI	: Santi Indra Astuti

Buku ini diterbitkan di bawah lisensi CC BY-NC-SA 4.0. Anda dapat menyalin, menyebarkan kembali, mengubah, dan membuat turunan dari materi ini untuk kepentingan apapun, termasuk kepentingan komersial, selama Anda mencantumkan nama yang sesuai, mencantumkan tautan terhadap lisensi, dan menyatakan bahwa telah ada perubahan yang dilakukan (jika ada). Apabila Anda mengubah, mengubah, atau membuat turunan dari materi ini, Anda harus menyebarkan kontribusi Anda di bawah lisensi yang sama dengan materi asli.

Penjelasan lisensi: creativecommons.org/licenses/by-sa/4.0/deed.id

Buku Perlindungan Data Pribadi diterbitkan dengan dukungan dari Google.org.

tularnalar@gmail.com

www.tularnalar.id



ORGANIZED BY:



lovefrankie

SUPPORTED BY:



Kata Pengantar

Tidak terasa, Tular Nalar bagi Warga Lansia yang berlangsung selama bulan Februari hingga September 2022 telah berakhir. Tular Nalar periode tersebut adalah waktu inkubasi, di mana kurikulum pembelajaran bagi warga digital dikonstruksi, dikembangkan, serta diuji cobakan. Hasilnya tidak mengecewakan. Melalui proses riset berupa focus group discussion, wawancara mendalam, observasi kelas pilot, akhirnya kurikulum awal Tular Nalar Lansia berhasil dibentuk dan dilaksanakan di 26 kota seluruh Indonesia. Pilot project ini melibatkan 9.072 target sasaran, yang didominasi oleh warga lansia (di atas 60 tahun), pra lansia (45 tahun hingga di bawah 60 tahun), dan pendamping lansia (di bawah 45 tahun).

Bukan hanya berkesempatan untuk mengujicobakan materi dan pendekatan guna mengajarkan literasi digital kepada warga lansia, Tular Nalar juga menemukan model Training of Trainers untuk mencetak para fasilitator handal, sebagai ujung tombak program. Sepanjang periode inkubasi, sebanyak 135 fasilitator telah berhasil dilatih oleh Tular Nalar. Para fasilitator berasal dari latar belakang yang beragam, namun diikat oleh cita-cita yang sama, yaitu berkontribusi bagi inklusi digital dengan merangkul lansia agar menjadi cakap digital. Modal pelatihan fasilitator ini adalah satu set paket TOT terdiri dari materi, modul, tools pelatihan, dan opsi-opsi pendampingan.

Berdasarkan pengalaman-pengalaman ini, Tular Nalar kini mengembangkan materi pelatihan pada kompetensi-kompetensi lainnya. Kompetensi tersebut bersifat tematik, disesuaikan dengan konteks kebutuhan warga lansia. Terdapat 10 (sepuluh) tema yang dikembangkan, di antaranya mencakup Keamanan dan Perlindungan Data Pribadi, Aplikasi Percakapan Sosial, Ekonomi Digital, Hiburan di Ruang Digital, hingga Virtual Meeting untuk memfasilitasi ruang maya sebagai ajang silaturahmi lansia. Dengan adanya penambahan ini, maka Tular Nalar bagi Warga Lansia bertransformasi menjadi "Akademi Digital Lansia." Tujuannya tetap terfokus pada peningkatan kapasitas lansia agar cakap digital, sesuai dengan perkembangan teknologi dan kebutuhan warga lansia.

Seiring dengan penambahan tema-tema tersebut, tentunya diperlukan penambahan tools atau alat bantu pembelajaran. Modul berikut ini adalah salah satu tools tersebut. Isinya merangkum tema-tema kompetensi digital yang baru bagi warga lansia, sesuai dengan alur kurikulum Tular Nalar. Tentu saja, terminologi kurikulum dan alat bantu versi Tular Nalar, tidak bisa disandingkan atau disamakan dengan terminologi sejenis di lingkungan institusi pendidikan, karena tujuannya berbeda dan sasarannya juga sangat khas.

Tular Nalar berterima kasih kepada Tim Pakar yang telah mengembangkan modul, kurikulum dan alat bantu ini. Apresiasi sebesar-besarnya kepada Novi Kurnia, Ph.D. (FISIPOL Universitas Gajah Mada), Dr. Mario Anton Birowo (FISIP Universitas Atma Jaya Yogyakarta), Dr. Sri Astuty (FISIP Universitas Lambung Mangkurat Banjarmasin), dan Gilang Adikara, MA. (FISIPOL Universitas Negeri Yogyakarta), peletak dasar kurikulum dan materi Tular Nalar bagi Warga Lansia. Tidak lupa, terima kasih kepada Tim Kurikulum Tular Nalar yang digawangi oleh Giri Lumakto, M.A., beserta anggota tim Niken Pupy Setyowati, M.Si, Bernadeta Dwitasari Teteki Bernadeta, M.Hum, dan Axel Gumilar. Tanpa komitmen dan kolaborasi tim yang luar biasa ini, Tular Nalar belum tentu sekaya ini.

Modul "**Perlindungan Data Pribadi**" adalah sebuah awal, masih jauh dari sempurna. Karena itu, kritik dan saran kami harapkan. Semoga, modul ini dapat menambah khazanah materi pemberdayaan lansia di ruang digital, yang terus-terang saja masih sangat

minim. Besar harapan kami, para pembaca berkenan untuk memanfaatkan modul ini sesuai kebutuhan. Ini semua tentu menjadi bukti nyata kepedulian kita pada lansia sebagai kelompok rentan digital yang perlu dirangkul bersama.

Salam literasi,
Santi Indra Astuti
Program Manager Tular Nalar

00

Identitas Buku	i
Kata Pengantar	ii
Daftar Isi	iv

01

MEMAHAMI KEAMANAN DAN PRIVASI DI RUANG DIGITAL	1
---	---

Keamanan di Ruang Digital	2
---------------------------	---

02

MEMAHAMI DATA PRIBADI	5
------------------------------	---

Mengapa Perlu Memahami Data Pribadi?	6
--------------------------------------	---

Mengapa Data Pribadi Perlu dilindungi?	7
--	---

03

MELINDUNGI DATA PRIBADI	9
--------------------------------	---

Bagaimana Memperkuat Sandi?	10
-----------------------------	----

Bagaimana Cara Disiplin Menjaga Data Pribadi?	12
---	----

Bagaimana agar tidak segan meminta bantuan orang lain terkait data pribadi?	13
--	----

04

MENGATASI KEBOCORAN DATA PRIBADI	14
---	----

Mengapa perlu mengatasi kebocoran data pribadi?	15
---	----

Bagaimana cara memantau tindakan atasi kebocoran data pribadi?	16
--	----

05

LANSIA MANDIRI, LANSIA LINDUNGI DATA PRIBADI	17
---	----

Kawan Tular Nalar, dalam ruang digital, persoalan keamanan dan privasi sama pentingnya dengan di ruang nyata. Dalam kehidupan sehari-hari, kita berusaha menjaga rumah kita agar aman dan privasi kita terjaga dengan berbagai upaya terbaik yang bisa kita lakukan. Kita akan memasang kunci rumah yang bagus sehingga kita akan merasa aman ketika meninggalkan rumah maupun ketika kita ingin istirahat di dalam rumah. Kita juga mungkin akan lebih merasa tenang jika pagar rumah juga bisa terkunci dengan baik. Bahkan mungkin kita juga akan merasa lebih aman jika memasang kamera pengawas untuk mendokumentasikan apa yang terjadi di sekitar rumah kita. Semua upaya tersebut dilakukan tak hanya agar kita tenang dan merasa aman tapi juga menjaga segala kemungkinan buruk yang akan terjadi pada kita misalnya saja pencurian maupun kejahatan lain dari rumah rumah.

01

MEMAHAMI KEAMANAN DAN PRIVASI DI RUANG DIGITAL

Apa yang dimaksud dengan keamanan di ruang digital?

Kawan Tular Nalar, dalam ruang digital, persoalan keamanan dan privasi sama pentingnya dengan di ruang nyata. Dalam kehidupan sehari-hari, kita berusaha menjaga rumah kita agar aman dan privasi kita terjaga dengan berbagai upaya terbaik yang bisa kita lakukan. Kita akan memasang kunci rumah yang bagus sehingga kita akan merasa aman ketika meninggalkan rumah maupun ketika kita ingin istirahat di dalam rumah. Kita juga mungkin akan lebih merasa tenang jika pagar rumah juga bisa terkunci dengan baik. Bahkan mungkin kita juga akan merasa lebih aman jika memasang kamera pengawas untuk mendokumentasikan apa yang terjadi di sekitar rumah kita. Semua upaya tersebut dilakukan tak hanya agar kita tenang dan merasa aman tapi juga menjaga segala kemungkinan buruk yang akan terjadi pada kita misalnya saja pencurian maupun kejahatan lain dari rumah rumah.

Di ruang digital, kita juga harus melakukan upaya yang terbaik untuk menjaga agar keamanan dan privasinya terjaga. Kita tentu tidak mau ada hal buruk terjadi dari penipuan digital, kejahatan siber, maupun pencurian data pribadinya. Oleh karena itu, berbagai upaya untuk menjaga keamanan digital juga harus dilakukan sebaik-baiknya.

Terdapat beberapa indikator keamanan digital yang digunakan dalam Modul Aman Bermedia Digital yang merupakan kolaborasi Japelidi, Kominfo dan Siberkreasi pada tahun 2021.



Gambar 1.1 Lima Indikator Keamanan Digital

Pertama, kemampuan mengatur keamanan digital pada perangkat lunak maupun keras termasuk dalam mempraktikkan sandi yang kuat, aman, dan diganti secara berkala.

Kedua, memaksimalkan perlindungan data pribadi baik data diri sendiri maupun data pribadi orang lain (keluarga, teman, atau kolega) yang dititipkan.

Ketiga, mengantisipasi berbagai modus penipuan digital sehingga tak hanya bisa mencegah namun juga bisa mengatasinya.

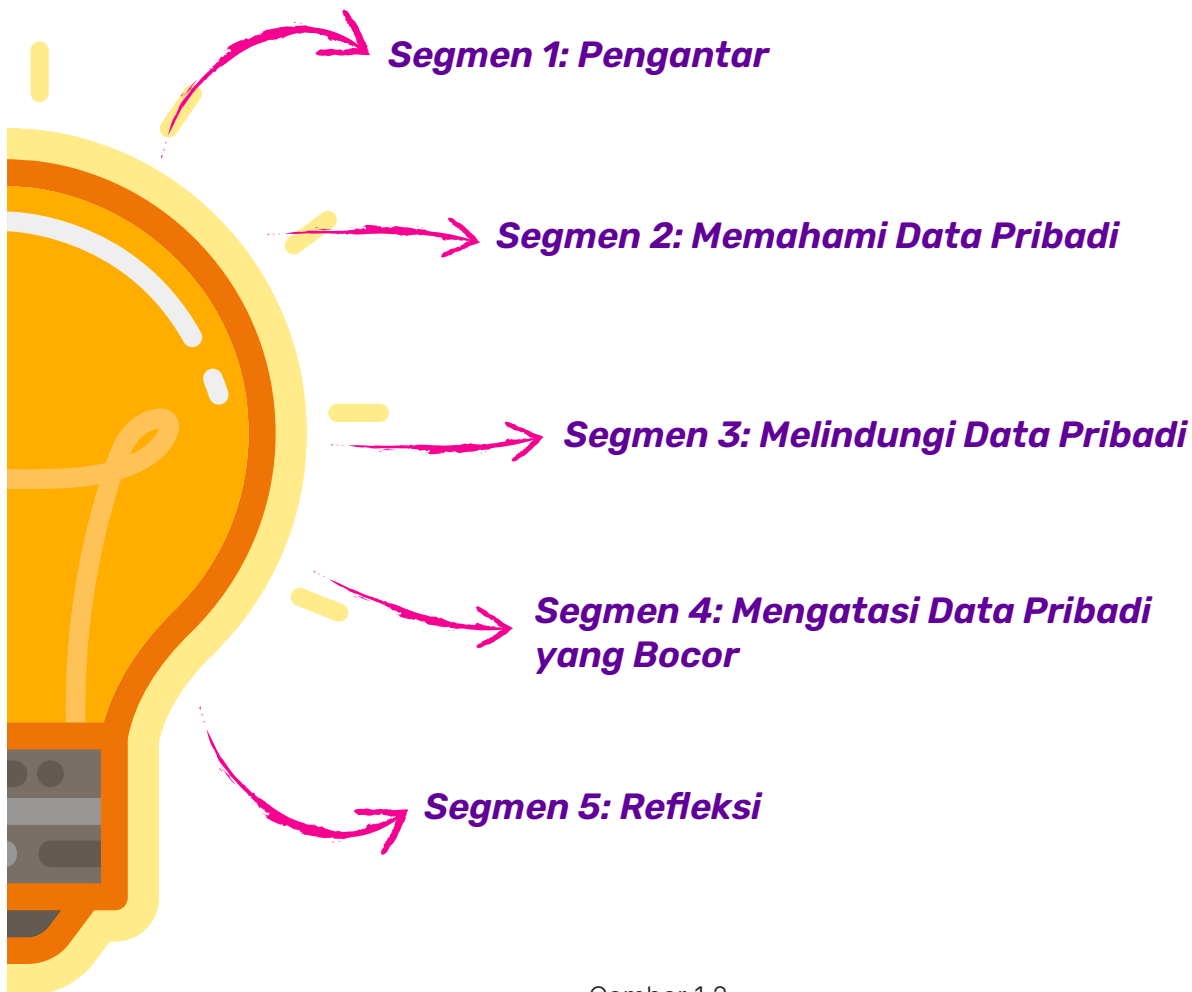
Keempat, menomorsatukan rekam jejak digital yang baik sehingga bisa melindungi diri dari berbagai potensi kejahatan siber,

Kelima, merangkul dan mendampingi, asah dan asuh, kelompok rentan digital seperti

perempuan, anak, lansia, difabel, warga dengan akses internet terbatas dan berbagai kelompok rentan lainnya.

BAGAIMANA PENGGUNAAN MODUL INI?

Modul ini memfokuskan pada indikator memaksimalkan perlindungan data pribadi untuk mengajak lansia memahami sekaligus mempraktikkan kemampuan melindungi data pribadi yang terbagi dalam 5 segmen.



Gambar 1.2
Lima Segmen Modul Keamanan Digital

Segmen pertama, pengantar, segmen ini, menjelaskan pentingnya perlindungan data pribadi penting untuk menjaga keamanan digital lansia berikut penjelasan segmentasi modul maupun penggunaan modul.

Segmen kedua, memahami data pribadi, memaparkan pengertian dan jenis data pribadi sekaligus memberikan alasan-alasan mengapa penting melindungi data pribadi.

Segmen ketiga, melindungi data pribadi, memberikan beragam tips untuk melindungi data pribadi yang bisa digunakan lansia

Segmen keempat, mengatasi data pribadi yang bocor, menjelaskan berbagai langkah untuk mengatasi data yang bocor.

Segmen kelima atau terakhir, refleksi, menyimpulkan sekaligus mengajak lansia untuk mampu menjadi panutan dalam melindungi data pribadi diri maupun anggota keluarga dan warga lainnya di ruang digital.

Modul ini bisa langsung dimanfaatkan oleh lansia sebagai panduan melindungi data pribadi saat berinteraksi di ruang digital baik melalui aplikasi *chat*, media sosial, maupun *platform* digital lainnya. Selain itu, modul ini juga bisa dimanfaatkan oleh pegiat literasi digital maupun warga digital yang mendampingi lansia.

Kawan Tular Nalar, dalam kehidupan sehari-hari kita sering membagikan identitas kita pada orang lain baik disengaja maupun tidak. Saat berjumpa dengan orang yang baru kita kenal baik dalam pertemuan tatap muka maupun melalui media digital, kita biasanya membagikan nama juga nomor telepon kita.

02

MEMAHAMI DATA PRIBADI

MENGAPA PERLU MEMAHAMI DATA PRIBADI?

Pilihan untuk membagikan data pribadi ini adalah wujud keinginan kita bersikap ramah dalam membangun hubungan supaya komunikasi di waktu mendatang lebih lancar. Tujuannya tentu untuk memperluas pertemanan maupun jaringan baik untuk kepentingan personal maupun profesional.

Namun begitu, ada baiknya kita memahami data pribadi yang ragamnya sangat banyak untuk melindungi data pribadi diri, keluarga dan warga lainnya agar bisa menghindari kejahatan siber. Beberapa kejahatan siber yang bisa muncul akibat penyalahgunaan dan kebocoran data pribadi adalah: penipuan digital, pinjaman *online* ilegal, profiling pemasaran, profiling politik, pemerasan digital, kekerasan digital, dan lain-lainnya.

APA YANG DISEBUT DENGAN DATA PRIBADI?

Kawan Tular Nalar, data pribadi merupakan data atau serangkaian informasi yang privat dan unik sehingga bisa digunakan untuk mengenali seseorang sekaligus membedakannya dengan orang lain.

Sementara itu, dalam Undang-Undang nomer 27 tahun 2022 tentang Perlindungan Data Pribadi dalam Pasal 1 disebutkan bahwa data pribadi adalah "data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau non-elektronik."

Untuk aman bermedia digital, lansia perlu melakukan perlindungan data pribadi agar terlindung dari kejahatan siber, penipuan digital dan risiko lain

APA SAJA JENIS DATA PRIBADI?

Kawan Tular Nalar, ragam data pribadi banyak tapi pada umumnya terbagi atas dua kelompok yakni data pribadi yang bersifat umum dan data pribadi yang bersifat khusus.

Data pribadi yang bersifat umum misalnya nama lengkap, jenis kelamin, kewarganegaraan, agama, status pernikahan, tanggal lahir, alamat rumah, email, nomor telepon (rumah maupun handphone), nomor KTP/NIP, nomor pegawai, nomor kartu kredit dan lain-lain.

Sedangkan data pribadi yang bersifat khusus contohnya adalah data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data dan informasi keuangan pribadi, dan lain-lain.

Baik data pribadi yang bersifat umum dan khusus sama-sama perlu kita lindungi supaya kejahatan siber bisa terhindari.

MENGAPA DATA PRIBADI PERLU DILINDUNGI?

Kawan Tular Nalar, kita mungkin pernah membaca berita mengenai beberapa kasus penipuan digital yang menimpa lansia. Ada sepasang lansia yang kehilangan uang setelah ditelpon perihal anaknya yang di luar kota kecelakaan dan membutuhkan dana cepat untuk operasi. Tindakan sepasang lansia melakukan transfer tentu dilakukan karena kekhawatiran orang tua atas kesehatan anaknya sehingga tanpa berpikir panjang berusaha yang terbaik untuk anaknya. Tanpa tahu bahwa kekhawatiran itulah yang dimanfaatkan oleh pelaku penipuan berkedok krisis keluarga.

Kasus lain adalah terjebaknya seorang lansia menjadi korban penipuan pinjaman *online* ilegal yang 'diteror' untuk segera mengembalikan pinjaman. Padahal ia tak pernah sekalipun melakukan pinjaman *online* sama sekali. Namun, data pribadinya yang berupa KTP bocor ke pelaku sehingga dimanfaatkan penipuan pinjaman *online* ilegal. Memang, dalam kasus ini korban tidak kehilangan uang, tapi nama baiknya jadi tercoreng selain juga jadi ada beban psikologis akibat ditagih pinjaman yang bukan miliknya.

Dua kasus di atas menunjukkan bahwa data pribadi baik berupa nomor telepon maupun identitas diri seperti KTP patut dilindungi karena jika sampai jatuh ke tangan orang yang tidak bertanggung jawab bisa menimbulkan penipuan digital atau kejahatan lainnya.

Oleh karena itu, penting bagi lansia untuk memahami beberapa alasan pentingnya perlindungan data pribadi.

Pertama, data pribadi bersifat privat dan unik serta menjadi milik subjek data pribadi sehingga harus dilindungi untuk menghindari penyalahgunaan data pribadi untuk kepentingan yang tidak baik dari pelaku yang tidak bertanggungjawab.

Kedua, data pribadi dikumpulkan dan digunakan secara sah sehingga hanya pihak yang berkepentingan saja yang berhak menggunakannya sesuai kesepakatan dengan subjek pemilik data pribadi.

Ketiga, penggunaan data pribadi harus seijin subjek data pribadi yang datanya tersebut di dalamnya.

Keempat, kebocoran data pribadi bisa menimbulkan banyak risiko yang merugikan baik subjek pemilik data pribadi maupun pihak lain yang terkait.

Dari penjelasan di atas bisa diingat bahwa data pribadi yang perlu kita lindungi adalah data diri kita sendiri maupun data diri pihak lain (anak, cucu, teman maupun orang lain) yang "dititipkan" pada kita.

APA RESIKO KEBOCORAN DATA PRIBADI?

Kawan Tular Nalar, sebagaimana dijelaskan sebelumnya, salah satu alasan perlindungan data pribadi penting untuk dilakukan adalah untuk menghindari resiko kebocoran data

pribadi yang bisa beragam bentuk.

Pertama, pembobolan rekening bank yang bisa terjadi jika ada kebocoran beberapa data pribadi misalnya nama, nomer telepon, nama ibu kandung, nomer rekening, sandi internet banking, dan lain-lain.

Kedua, penyalahgunaan identitas untuk pinjaman *online* ilegal yang bisa terjadi jika kartu identitas diri seperti KTP, NIK, maupun KK bocor dengan sengaja maupun tidak sengaja dari pemilik data pribadi.

Ketiga, penipuan digital yang beragam seperti penipuan berkedok krisis keluarga, penipuan berkedok hadiah yang biasanya memanfaatkan nomer telepon calon korban sehingga pengiriman pesan dan atau telpon menjadi modus pelakunya.

Keempat, pemetaan profil pemilik data pribadi baik untuk kepentingan politik, ekonomi, maupun sosial. Misalnya data pribadi dikumpulkan untuk dijadikan target pemasaran produk tertentu.

Kelima, pemerasan *online* yang dilakukan oleh pelaku dengan memanfaatkan data pribadi yang sering kali spesifik dan sensitif terkait dengan calon korban. Misalnya data dan informasi kesehatan yang spesifik digunakan sebagai bahan pemerasan *online* oleh pelaku.

Dengan mengetahui berbagai resiko kebocoran data pribadi, perlu diingat bahwa lansia harus selalu waspada dan hati-hati. Kebocoran data pribadi misalnya nomor telepon bisa berakibat pada banyaknya sms penipuan digital berkedok hadiah ataupun krisis keluarga. Kebocoran nomor atau informasi KTP bisa mengakibatkan pemiliknya terseret pinjaman *online* ilegal.

Kawan Tular Nalar, beragam resiko kebocoran data pribadi adalah tantangan nyata yang dihadapi oleh sebagian warga lansia. Dimulai dari pembobolan rekening, penyalahgunaan identitas untuk pinjaman *online* ilegal, aneka jenis penipuan digital, pemetaan profil untuk berbagai kepentingan politik juga ekonomi dan sosial, hingga pemerasan *online* yang menimbulkan kerugian materi maupun non materi.

03

MELINDUNGI DATA PRIBADI

MENGAPA PERLU MELINDUNGI DATA DIRI?

Kesadaran perlindungan data pribadi sangat penting untuk meminimalisir resiko yang mungkin muncul. Kesadaran tersebut harus diwujudkan dalam praktik perlindungan data pribadi yang bisa dilakukan oleh lansia yang bisa dilakukan dengan berbagai macam cara sebagaimana nampak dalam gambar berikut.



Gambar 3.1
Lima Praktik Perlindungan Data Pribadi (tolong gambar sesuaikan)

Dengan mempraktekkan beberapa cara di atas, lansia bisa melakukan upaya terbaiknya untuk melakukan perlindungan data diri.

BAGAIMANA MEMPERKUAT SANDI?

Sandi atau *password* adalah kombinasi huruf, angka dan simbol lainnya yang kita gunakan sebagai pintu masuk ke akun media sosial maupun akun *platform* digital lainnya. Oleh karena itu, lansia perlu memperkuat sandi dengan membuat sandi yang kuat, rahasia, diperbarui secara berkala, dan berbeda setiap akun.

Sandi yang kuat adalah sandi yang terdiri dari kombinasi huruf baik besar maupun kecil, angka, dan simbol lainnya. Hindari sandi yang mudah ditebak misalnya menggunakan nama yang dikombinasi dengan tanggal lahir. Kedua data ini mudah ditemukan misalnya dari panggilan kita sehari-hari maupun perayaan ulang tahun yang kadang didokumentasikan baik oleh diri sendiri atau orang lain di media sosial.

Gunakan gabungan kombinasi huruf, angka, dan simbol yang tak mudah ditebak orang. Nama makanan kesukaan, nama kucing peliharaan pertama, nama bintang film favorit adalah beberapa contoh yang bisa digunakan. Tentu harus dikombinasi dengan angka dan simbol lain yang kita sukai. Bagaimana supaya tidak lupa? Gunakan *password manager* atau tempat penyimpanan sandi baik yang digital maupun manual. Banyak tempat penyimpanan sandi secara digital yang gratis bisa dimanfaatkan. Pilihan lain adalah mencatatnya secara manual tapi menggunakan bahasa rahasia yang hanya kita tahu sehingga keamanannya terjamin.

Sandi juga perlu dijaga kerahasiaannya jadi lansia perlu hanya menyimpannya sendiri dan tak perlu dibagikan pada orang lain terutama pada orang yang baru dikenal. Ibaratnya kita

pasti tidak mau menitipkan kunci rumah pada orang yang tidak atau belum kita percayai karena di dalam rumah banyak barang yang berharga yang perlu kita lindungi.

Sebaiknya sandi juga diganti secara berkala misalnya saja setiap 3-6 bulan sekali supaya benteng keamanan digital kita lebih terjaga. Tampaknya merepotkan tapi yang merepotkan biasanya akan lebih aman.

Sandi berbeda tiap akun juga sebaiknya diupayakan terutama jika kita berinteraksi dengan menggunakan lebih dari 1 akun media sosial maupun *platform* digital lainnya. Mengapa harus beda kan merepotkan? Ya, memang sedikit merepotkan tapi risikonya lebih kecil karena jika sandi sama ketika kebocoran terjadi akan mengenai beberapa akun yang akan lebih merugikan.

Bagaimana cara menggunakan dua langkah verifikasi?

Kawan Tular Nalar, dua langkah verifikasi atau disebut dengan *Two-Factors Authentication* (2FA) merupakan sistem keamanan digital yang melekat pada berbagai *platform* digital. Sistem dua langkah verifikasi atau pengulangan verifikasi ini dilakukan agar bisa memastikan pengguna yang sedang mengakses adalah pengguna sebenarnya, bukan orang lain yang mengatasnamakan pengguna tersebut.

Untuk menggunakan dua langkah verifikasi, terdapat beberapa komponen informasi yang biasanya digunakan dalam dua langkah verifikasi.

Pertama, informasi yang berisi pengetahuan yang hanya dimiliki oleh pengguna misalnya terkait dengan sandi maupun pertanyaan keamanan tambahan lainnya.

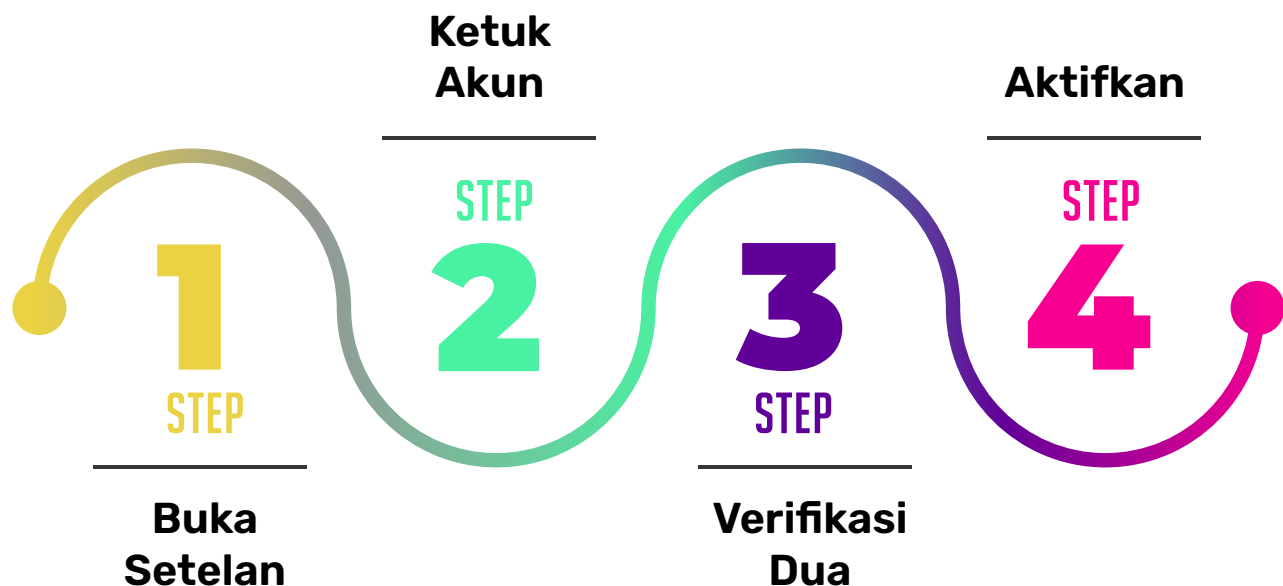
Kedua, informasi yang terkait dengan faktor kepemilikan seperti kartu identitas dan berbagai aplikasi lainnya.

Ketiga, informasi yang berupa biometrik misalnya dengan menggunakan teknologi sensor seperti sidik jari, wajah, suara, iris mata dan lainnya.

Keempat, informasi yang terkait dengan lokasi pengguna yang login dalam sistem yang bisa diidentifikasi.

Kelima, informasi yang terkait dengan waktu terbatas sehingga hanya pengguna yang akan bisa berinteraksi dengan *platform* yang akan digunakannya.

Sebagai contoh jika kita ingin melakukan dua langkah verifikasi di aplikasi percakapan WhatsApp, maka berikut adalah beberapa langkah yang bisa dilakukan:



Gambar 3.2.
Atur dua langkah verifikasi di WhatsApp

Untuk bisa mempraktikkan dua langkah verifikasi di *platform* digital dan aplikasi lainnya, pastikan informasi mengenai ini didapatkan secara detail sebab setiap *platform* digital atau aplikasi mempunyai sistem pengamanan yang berbeda satu sama lain.

BAGAIMANA CARA DISIPLIN MENJAGA DATA PRIBADI?

Kawan Tular Nalar, setiap kita berinteraksi dengan orang lain di dunia digital, melalui aplikasi *chat*, media sosial, aplikasi belanja dan berbagai aplikasi lainnya, sadar atau tidak sadar kita akan berbagi data pribadi kita. Setidaknya kita akan berbagi nama lengkap kita maupun nomor telepon kita pada orang lain.

Saat berbagi data pribadi, kita selalu mengutamakan prasangka baik bahwa orang yang menerima informasi tersebut tidak akan menyalahgunakan data pribadi kita. Sebagai contoh, saat kita menghadiri berbagai acara sosial kemasyarakatan, baik secara daring atau luring, sering kali kita dimintai mengisi presensi kehadiran. Dalam presensi ini biasanya kita harus menuliskan nama dan nomor telepon kita. Padahal, belum tentu data pribadi kita dikelola dan dijaga dengan benar. Oleh karena itu, penting bagi lansia untuk disiplin menjaga data pribadi dan hanya membagikannya pada orang atau pihak yang bisa dipercaya.

BAGAIMANA CARA TURUT MENJAGA DATA PRIBADI ORANG LAIN?

Kawan Tular Nalar, tak hanya menjaga data pribadi, lansia yang menjadi panutan juga mempunyai tanggung jawab untuk turut menjaga data pribadi orang lain. Biasanya data pribadi orang lain yang turut dijaga lansia adalah data pribadi keluarga, sahabat, kolega

atau warga.

Lansia biasanya mengetahui data pribadi anggota keluarganya dari anak, menantu, hingga cucu, maupun anggota keluarga lainnya. Oleh karena itu, perlu bagi lansia untuk turut menjaga data pribadi anggota keluarganya dengan selalu meminta persetujuan mereka jika ingin berbagi data pribadi mereka kepada pihak lain yang bisa dipercaya. Selain itu, lansia juga bisa mengingatkan anggota keluarganya untuk selalu disiplin melakukan perlindungan data pribadi.

Tak hanya berpartisipasi dalam turut menjaga data pribadi keluarga, lansia yang aktif biasanya juga turut menjaga data pribadi sahabat, kolega atau warga lain yang dititipkan padanya dan hanya membagikannya pada orang atau pihak yang bisa kita percaya.

BAGAIMANA AGAR TIDAK SEGAN MEMINTA BANTUAN ORANG LAIN TERKAIT DATA PRIBADI?

Kawan Tular Nalar, tantangan bagi lansia dalam perlindungan data pribadi adalah untuk mengikuti perkembangan teknologi, informasi dan komunikasi yang terus berkembang. Perubahan cepat ini juga terjadi dalam sistem keamanan digital terutama untuk selalu bisa melakukan pembaruan perangkat lunak dan perangkat keras yang digunakannya untuk berinteraksi di ruang digital.

Jangan segan meminta bantuan anggota keluarga maupun sahabat dan warga lain yang menguasai teknologi jika kesulitan mempraktikkan sandi yang kuat. Jangan ragu meminta pendampingan mereka apabila ingin mengatur dua langkah verifikasi maupun pengaturan pengamanan digital lainnya agar bisa melindungi data pribadi secara maksimal.

Kawan Tular Nalar, penting untuk diketahui meskipun lansia memberikan upaya terbaiknya untuk melakukan perlindungan data pribadi baik untuk data sendiri maupun data orang lain, kebocoran data pribadi masih bisa terjadi. Kebocoran bisa dilakukan oleh jika pihak lain yang mengelola dan memproses data pribadi kurang memperhatikan sistem keamanan digital sehingga bisa diretas.

04

MENGATASI KEBOCORAN DATA PRIBADI

MENGAPA PERLU MENGATASI KEBOCORAN DATA PRIBADI?

Jika kebocoran data pribadi tak bisa dielakkan, maka lansia tak perlu ragu untuk mengatasinya melalui beberapa langkah.



Gambar 4.1.
Beberapa langkah mengatasi kebocoran data pribadi (silakan ilustrasinya diimprovisasi)

Selain itu, lansia perlu memastikan langkah yang tepat untuk kasus kebocoran data pribadi. Jangan segan meminta bantuan anggota keluarga lainnya, sahabat, kolega, maupun warga yang lain jika mendapatkan kesulitan dalam mengatasi kebocoran data pribadi.

BAGAIMANA CARA LAPOR JIKA TERJADI KEBOCORAN DATA PRIBADI?

Kawan Tular Nalar, langkah pertama yang bisa dilakukan jika lansia mendapati data pribadinya bocor adalah dengan melaporkan pada *platform* digital atau aplikasi atau organisasi yang menjadi sumber kebocoran data pribadi. Dengan begitu maka *platform* digital atau aplikasi atau organisasi tersebut bisa segera mengambil langkah untuk mengatasinya maupun mengetakan sistem keamanannya.

BAGAIMANA MENGUBAH KATA SANDI JIKA TERJADI KEBOCORAN DATA PRIBADI?

Kawan Tular Nalar, ketika lansia mendapati data pribadinya bocor, sangat penting untuk segera mengubah sandi di mana kebocoran terjadi. Misalnya jika kebocoran terjadi di media sosial maka akun media sosial tersebut perlu segera diganti sandinya. Akan lebih baik jika email yang digunakan untuk mendaftar akun media sosial tersebut juga diganti. Dalam hal ini memang, kebutuhan untuk membuat sandi selalu diperbarui secara berkala ternyata penting.

BAGAIMANA CARA MENGAWASI AKTIVITAS KEUANGAN JIKA TERJADI KEBOCORAN DATA PRIBADI?

Kawan Tular Nalar, resiko yang sering muncul dari kebocoran data pribadi adalah pembobolan rekening bank dan aneka dompet digital atau alat pembayaran digital lainnya. Oleh karena itu, ketika lansia mendapatkan data pribadinya bocor, maka sangat penting untuk mengawasi aktivitas keuangan yang biasa dilakukan secara digital. Misalnya

apakah ada transaksi mencurigakan dalam e-banking atau dompet digital lainnya.

BAGAIMANA CARA MEWASPADAI AKTIVITAS PENIPUAN DIGITAL JIKA TERJADI KEBOCORAN DATA PRIBADI?

Kawan Tular Nalar, resiko lain yang acapkali muncul dari kebocoran data pribadi adalah penipuan digital. Oleh karena itu, lansia harus selalu waspada akan telepon, sms, atau aktivitas lain yang mencurigakan terkait penipuan digital setelah kebocoran data pribadi. Misalnya saja lansia perlu mudah panik jika ada telepon yang meminta transfer uang karena ada anggota keluarga kecelakaan

BAGAIMANA CARA MEMANTAU TINDAKAN ATASI KEBOCORAN DATA PRIBADI?

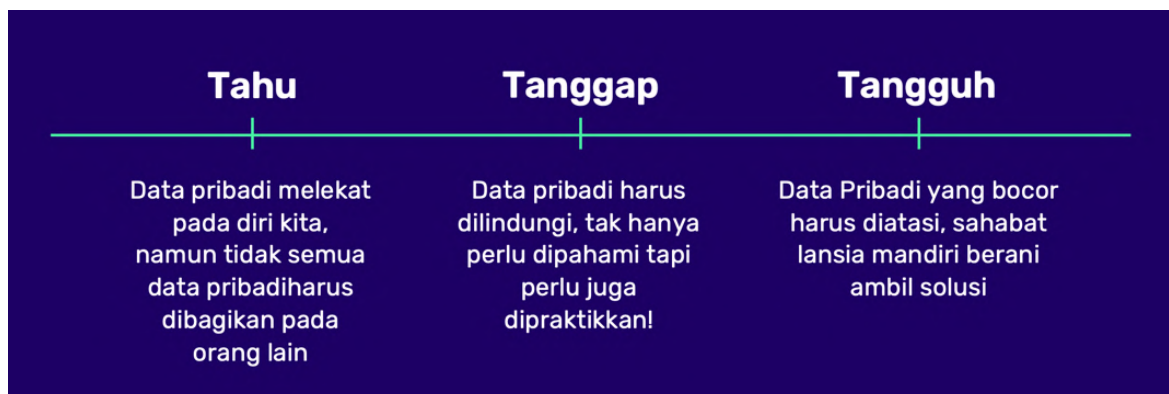
Kawan Tular Nalar, selain mengambil langkah-langkah strategis yang bisa dilakukan secara mandiri untuk meminimalisir resiko kebocoran data pribadi dari, alangkah baiknya jika lansia juga turut memantau tindakan dari pemangku relevan yang berkepentingan dalam mengatasi kebocoran data pribadi. Caranya adalah dengan selalu melakukan update informasi terbaru terhadap penanganan kebocoran data pribadi yang sedang berlangsung. Segera tanggap jika ada langkah yang harus dilakukan namun tetap waspada.

Kawan Tular Nalar, data pribadi adalah harta yang penting serta harus dilindungi oleh seluruh pengguna media digital termasuk lansia. Dengan kemampuan perlindungan yang maksimal maka lansia bisa terhindar dari berbagai kejahatan siber maupun penipuan digital yang selalu mengintai kita di ruang digital.

05

LANSIA MANDIRI, LANSIA LINDUNGI DATA PRIBADI

Untuk itu, penting untuk meningkatkan kompetensi literasi digital lansia dalam melakukan perlindungan diri dalam tiga level yang dirumuskan oleh program Tular Nalar untuk Lansia: Tahu, Tanggap dan Tangguh.



Gambar 5.1.
Level Tahap. Tanggap dan Tangguh

Level Tahu, lansia diharapkan mampu memahami data pribadi dan ragamnya baik yang termasuk dalam data pribadi yang bersifat umum maupun yang bersifat khusus. Selain itu, lansia juga akan mempunyai kemampuan memahami berbagai alasan yang mendasari pentingnya perlindungan data pribadi. Dengan kemampuan memahami (tahu) ini, lansia akan mempunyai bekal untuk memahami data pribadi mana yang bisa maupun yang tidak bisa dibagikan pada orang lain.

Level Tanggap, lansia diharapkan mampu melindungi data pribadi dirinya sendiri maupun orang-orang terdekatnya, baik anggota keluarga, sahabat, kolega maupun warga lainnya. Tentu saja lansia bisa berkolaborasi dengan anggota keluarga, sahabat, kolega maupun warga lainnya untuk melakukan berbagai upaya yang maksimal untuk perlindungan data diri.

Level Tangguh, lansia diharapkan mampu mengatasi kebocoran data pribadi jika menghadapinya dengan melakukan upaya-upaya yang bersifat mandiri maupun dengan berkolaborasi dengan pemangku kepentingan lainnya.

Sebagai panutan keluarga dan warga sekitar, lansia bisa berdiri paling depan untuk melakukan berbagai upaya perlindungan data pribadi. Lansia Mandiri, Lansia Lindungi Data Pribadi.

PENULIS

Novi Kurnia

Staf pengajar di Departemen Ilmu Komunikasi di Fisipol UGM dengan minat studi literasi digital, sinema Indonesia, serta gender dan media. Doktor lulusan Flinders University (South Australia) pada tahun 2014 ini aktif di berbagai komunitas maupun gerakan literasi digital. Selain menjadi salah satu pendiri sekaligus koordinator nasional Jaringan Pegiat Literasi Digital (Japelidi), ia adalah salah satu dewan pengarah Gerakan Nasional Literasi Digital Siberkreasi. Ia juga merupakan salah satu pakar kurikulum Tular Nalar. Ia dan tim memenangkan beberapa grant riset terkait literasi digital, misalnya: (1) Misinformasi Krisis Iklim (2023-2024), (2) Penipuan Digital (2021-2022), (3) Pengaturan Konten Berbahaya (2021-2022), (4) Literasi Digital dan WhatsApp Group bagi Perempuan Indonesia. Selain menuliskan beragam publikasi berupa buku, artikel jurnal, book chapter, monograf, modul, maupun video terkait literasi digital, ia aktif menjadi narasumber di berbagai forum ilmiah baik di level nasional dan internasional. Ia bisa dihubungi melalui: novikurnia@ugm.ac.id

PENYUNTING

Giri Lumakto

Giri Lumakto adalah seorang peneliti, penulis dan pegiat literasi digital. Sejak 2014 banyak tulisan dan publikasi ilmiah diterbitkan tentang etika, privasi, dan keamanan dunia digital. Pendidikan S1 ditempuh di Universitas Muhammadiyah Surakarta sedang S2 diselesaikan di University of Wollongong Australia. Sudah selama 4 tahun, ia ditunjuk menjadi koordinator Kurikulum di program Tular Nalar dari Mafindo yang disponsori Google.org. Pengalaman karir lain yang pernah dijalani antara lain bersama KPK, Atlas Corp. US, kognisi.id, Komnas Perempuan, dan juga meruapkan pendiri IPL (Indonesia Privacy League). Fokus bidang keilmuan dan pelatihan yang Giri tekuni adalah literasi digital, privasi, komunikasi digital, dan classroom management. Ia bisa dihubungi melalui email di lumakto.giri@gmail.com.

Dwitasari Teteki B.

Lebih akrabnya dikenal dengan nama Ayik Teteki, adalah relawan pegiat literasi digital dari Mafindo (Masyarakat Antifitnah Indonesia) Magelang Raya sejak Juli 2018. Sebagai pegiat literasi digital, Ayik Teteki aktif memberikan edukasi dan pelatihan kepada masyarakat tentang pentingnya literasi digital dan pelatihan antihoaks. Sejak tahun 2020 Ayik telah bergabung dalam tim kurikulum Tular Nalar Mafindo yang didukung oleh Google.org untuk mengembangkan kurikulum pelatihan literasi digital bagi anak muda first time voters dan lansia. Meskipun sebagai pekerja lepas untuk melakukan riset, penulisan, dan pelatihan, Ayik senang belajar dan telah menyelesaikan pendidikannya di Magister Kajian Budaya Universitas Sanata Dharma Yogyakarta. Ayik gemar membaca, dan crocheting (merajut). Kontak dengan Ayik dapat menghubungi ayik.teteki@gmail.com atau DM IG [ayikteteki](https://www.instagram.com/ayikteteki).

Niken Pupy Satyawati

Niken lahir di Sragen 18 Maret 1974. Menyelesaikan pendidikan S1 dan S2 Ilmu Komunikasi di Universitas Sebelas Maret Solo, kini Niken tercatat sebagai dosen Universitas Muhammadiyah Karanganyar (Umuka). Niken aktif mendorong gerakan literasi dan bergiat melaksanakan program-program literasi digital bersama komunitas Masyarakat Anti-fitnah Indonesia (Mafindo). Pada tahun 2017 Niken mengikuti training of trainer cek fakta yang diadakan di Kantor Google Jakarta. Tahun 2018 Niken berpartisipasi dalam Internet Governance Forum di Kantor Pusat UNESCO, Paris, Prancis. Bersama sejumlah relawan Mafindo, Niken bergabung di Divisi Kurikulum Tular Nalar yang disponsori Google.org. Niken turut berkontribusi dalam penulisan beberapa modul literasi digital. Saat luang Niken menghabiskan waktu untuk melakukan solo travelling ataupun bersama keluarga. Niken juga menikmati waktu di rumah saja untuk berselancar di internet, mendengarkan musik, berkebun dan membaca buku. Niken dapat dihubungi melalui email dengan alamat nikensatyawati86@gmail.com.

SUPERVISI

Santi Indra Astuti

Dosen di Fakultas Ilmu Komunikasi, Universitas Islam Bandung (UNISBA) sejak 1998. Minatnya merentang mulai dari kajian media hingga media/digital literacy. Selain mengajar, ybs terlibat dalam sejumlah aktivitas lapangan, di antaranya kampanye anti rokok, gerakan anti hoaks, infodemic management, dan literasi media/literasi digital di tengah publik. Bergabung memperkuat Mafindo sejak tahun 2016. Sejak 2020 – November 2024 menjadi Program Manager Tular Nalar, sebuah inisiatif pembelajaran literasi digital bagi berbagai kalangan, termasuk lansia dan segmen rentan lainnya. Pada tahun 2017, mendirikan Jaringan Pegiat Literasi Digital (Japelidi) beranggotakan dosen, peneliti, dan pegiat literasi digital seluruh Indonesia. Email: santi.indraastuti@gmail.com. FB/IG Santi Indra Astuti.