KIWA TENGEN

MODUL KEAMANAN SIBER

Topik 3: Perlindungan Data & Etika Digital

Subtopik 3.1: Cara Membuat Password Kuat & Manajemen Akun

Disusun oleh:
Ketut Ananda Dharmawati
NIM: 2215091035

Program Studi S1 Sistem Informasi
Jurusan Teknik Informatika
Fakultas Teknik dan Kejuruan
Universitas Pendidikan Ganesha

BERSAMA CORPU KIWA TENGEN,
KLUNGKUNG TANGGUH HADAPI SERANGAN SIBER

DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN KLUNGKUNG
2025

KATA PENGANTAR

Puji syukur kita panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas rahmat-Nya modul pembelajaran *"Keamanan Siber untuk ASN dan Masyarakat"* dapat disusun hingga membahas subtopik penting mengenai *Cara Membuat Password Kuat & Manajemen Akun*. Di era digital saat ini, akun digital menjadi gerbang utama untuk mengakses berbagai layanan, baik dalam pemerintahan maupun kehidupan sehari-hari. Password yang lemah atau dikelola secara sembarangan dapat menjadi titik masuk bagi pelaku kejahatan siber untuk mencuri data pribadi, mengakses sistem instansi, bahkan menyebarkan informasi palsu.

Melalui subtopik ini, diharapkan ASN dan masyarakat Kabupaten Klungkung dapat memahami pentingnya menjaga keamanan akun masing-masing. Bukan sekadar mengganti kata sandi secara berkala, tetapi membangun kebiasaan digital yang disiplin, cerdas, dan bertanggung jawab. Dengan manajemen akun yang baik, kita turut menjaga kepercayaan publik terhadap layanan digital pemerintah dan melindungi diri dari ancaman kejahatan siber yang semakin kompleks di tahun 2025. Terima kasih kepada semua pihak yang telah berkontribusi dalam penyusunan subtopik ini. Semoga subtopik ini memberikan manfaat nyata dalam mendukung terwujudnya tata kelola pemerintahan dan kehidupan masyarakat yang lebih aman di era digital.

Kami menyadari bahwa modul ini masih memiliki keterbatasan dan belum sempurna. Oleh karena itu, kami sangat mengharapkan kritik dan saran yang membangun dari para pembaca demi penyempurnaan modul ajar ini di masa mendatang.

Klungkung, 2025

Penyusun

DAFTAR ISI

Tujuan Pembelajaran

Setelah mempelajari bagian ini, peserta (ASN maupun masyarakat) mampu:

1. Memahami pentingnya keamanan akun digital bagi ASN dan masyarakat di era layanan berbasis elektronik.
2. Mengidentifikasi ciri-ciri password yang kuat serta kesalahan umum dalam penggunaannya.
3. Menerapkan praktik manajemen akun yang aman, termasuk penggunaan *Two-Factor Authentication (2FA)* dan *password manager*.
4. Mengetahui tren keamanan akun tahun 2025 seperti autentikasi biometrik dan *passwordless login*.
5. Membangun budaya keamanan digital dengan disiplin menjaga akun pribadi dan dinas.

Sasaran Peserta

1. Aparatur Sipil Negara (ASN):
    A. ASN di lingkungan Pemerintah Kabupaten Klungkung yang menggunakan sistem dan aplikasi digital dalam pelaksanaan tugasnya.
    B. ASN yang bertanggung jawab atas pengelolaan data publik dan sistem administrasi pemerintahan berbasis elektronik (SPBE).
    C. ASN yang perlu meningkatkan literasi keamanan siber agar tidak menjadi titik lemah dalam rantai keamanan instansi.
2. Masyarakat Umum Kabupaten Klungkung:
    A. Masyarakat yang aktif menggunakan layanan digital seperti perbankan daring, e-commerce, dan aplikasi pelayanan publik.
    B. Pengguna media sosial dan perangkat pintar yang perlu memahami pentingnya menjaga akun pribadi agar tidak disalahgunakan.

C. Pelajar, UMKM, dan komunitas digital lokal yang berperan dalam menjaga kepercayaan dan keamanan ekosistem digital daerah.

A. Pentingnya Keamanan Akun di Era Digital

Di tahun 2025, hampir setiap layanan publik dan kegiatan masyarakat terhubung ke sistem digital: e-KTP, pajak online, perizinan daring, hingga transaksi keuangan pribadi. Setiap layanan itu membutuhkan **akun digital** dan setiap akun membutuhkan **keamanan**. Maka, menjaga akun bukan lagi hal sepele, melainkan **fondasi utama perlindungan data pribadi dan institusi**.

1. Mengapa Keamanan Akun Krusial

Bagi **Aparatur Sipil Negara (ASN)**, akun kerja sering terhubung langsung dengan basis data pemerintahan. Satu kebocoran akun dapat membuka jalan bagi peretas untuk mengakses ribuan data warga, mengubah arsip, atau bahkan melumpuhkan layanan publik. Sementara bagi **masyarakat**, akun perbankan, marketplace, atau media sosial menyimpan data identitas dan transaksi yang bisa disalahgunakan untuk penipuan digital.

🔐 **Satu kata sandi yang bocor dapat berakibat fatal, bukan hanya kehilangan uang, tapi juga kepercayaan publik.**

2. Dampak Kebocoran Akun

Kebocoran akun bukan sekadar masalah pribadi. Ia bisa menjalar menjadi ancaman luas:

a. **Kerugian finansial:** akun e-banking atau dompet digital diretas.
b. **Kehilangan data pribadi:** seperti NIK, alamat, nomor rekening.
c. **Gangguan layanan publik:** jika akun ASN disusupi, sistem perizinan atau administrasi bisa terganggu.
d. **Kerusakan reputasi digital:** data bocor dapat digunakan untuk menyebar hoaks atau memanipulasi identitas seseorang.

Menurut *Data Breach Investigations Report (Verizon, 2024)*, lebih dari **81% insiden peretasan global** disebabkan oleh **kata sandi yang lemah atau dicuri**. Angka ini meningkat seiring meningkatnya ketergantungan pada layanan daring, termasuk sistem

pemerintahan daerah di Indonesia.

3. Peran Password dalam Sistem Keamanan Digital

Password adalah **lapisan pertahanan pertama**. Ia berfungsi seperti kunci rumah: jika mudah ditebak, siapa pun bisa masuk. Namun, masih banyak pengguna yang menggunakan pola mudah seperti *"123456"*, *"qwerty"*, atau nama anaknya. Bahkan sebagian ASN di daerah mengaku memakai satu password untuk beberapa akun sekaligus. Padahal, jika satu sistem bocor, seluruh akun yang menggunakan password sama ikut terancam. Untuk itu, kini mulai diterapkan kebijakan ***multi-faktor autentikasi* (MFA),** misalnya kombinasi antara *password*, kode OTP, dan sidik jari, guna memperkuat lapisan keamanan akun baik di instansi pemerintah maupun layanan publik.

B. Prinsip Membuat Password yang Kuat dan Aman

Membuat password bukan sekadar memilih kombinasi huruf dan angka. Ia adalah seni kecil dalam menjaga diri di dunia digital. Password yang kuat harus **unik, sulit ditebak, dan mudah diingat oleh pemiliknya sendiri**. Banyak kasus peretasan terjadi bukan karena teknologi yang canggih, melainkan karena **pengguna ceroboh dalam membuat atau menyimpan password.**

1. Hindari Password Sederhana dan Informasi Pribadi

Hingga saat ini, password yang paling sering diretas di dunia masih sama: *"123456"*, *"password"*, *"admin"*, dan *"qwerty"*. Bahkan di Indonesia, survei BSSN (2024) menemukan bahwa **lebih dari 40% pengguna ASN** masih menggunakan nama pribadi, tanggal lahir, atau nama anak sebagai kata sandi utama mereka.

- Hindari kombinasi yang mudah ditebak seperti:
  a. Tanggal lahir, nama lengkap, atau nama instansi.
  b. Pola sederhana pada keyboard (misal: qwerty, asdfgh).
  c. Satu kata tanpa variasi karakter.

🧠 Gunakan prinsip "tidak ada yang tahu kecuali Anda sendiri."

2. Gunakan Kombinasi Karakter yang Kompleks

Password yang aman minimal terdiri dari:

a. **12 karakter** atau lebih.
b. Kombinasi **huruf besar, huruf kecil, angka, dan simbol.**

Contoh perbandingan kekuatan password:

Jenis Password	Contoh	Waktu untuk Ditebak
Lemah	klungkung123	< 3 detik
Sedang	Klungkung@24	± 2 jam
Kuat	K!w@T3ng3n_2025	> 10.000 tahun (perkiraan AI cracking, 2025)

3. Gunakan Password Berbeda untuk Setiap Akun

Kesalahan umum banyak pengguna, termasuk ASN, adalah menggunakan **satu password untuk semua akun** email, perizinan, keuangan, bahkan media sosial. Padahal, jika salah satu akun bocor, maka **seluruh akun lain otomatis ikut berisiko.**

🔐 Solusinya: gunakan **password manager** yang terpercaya untuk menyimpan dan membuat password unik otomatis. Contoh aplikasi resmi: Bitwarden, 1Password, atau Google Password Manager.

4. Perbarui Password Secara Berkala

BSSN dan CSIRT (2024) merekomendasikan agar password penting, seperti akun email dinas dan portal ASN diganti **setiap 3–6 bulan sekali**. Selain itu, jika ada indikasi kebocoran data dari layanan publik (misalnya laporan BSSN atau berita nasional), segera ubah semua password yang terkait. Langkah ini sederhana, tapi sangat efektif untuk mencegah akses tidak sah.

5. Gunakan Otentikasi Ganda (Multi-Factor Authentication / MFA)

Teknologi kini tidak cukup mengandalkan password saja. **MFA (*Multi-Factor Authentication*)** menambah lapisan keamanan tambahan, seperti:

a. Kode OTP yang dikirim lewat SMS/email.
b. Sidik jari atau pengenalan wajah.
c. Token digital atau aplikasi keamanan (contoh: Microsoft Authenticator, Google

Authenticator).

Dengan MFA, walaupun password bocor, **akun tetap tidak bisa diakses tanpa kode tambahan.** ASN disarankan untuk mengaktifkan MFA di semua sistem pemerintahan berbasis cloud, sedangkan masyarakat dapat mengaktifkannya di akun e-commerce, perbankan, dan media sosial.

C. Manajemen Akun Digital: Langkah Sederhana, Dampak Besar

1. Mengapa Manajemen Akun Penting?

Manajemen akun bukan hanya soal mengingat kata sandi, tetapi **cara mengatur, memisahkan, dan melindungi identitas digital** agar tidak disalahgunakan. Bagi ASN, setiap akun yang terhubung ke sistem pemerintahan, seperti SIMPEG, e-Office, SIAK, dan aplikasi pelayanan publik, **mewakili kredibilitas instansi**. Sedangkan bagi masyarakat, akun pribadi sering terhubung dengan data finansial, kesehatan, dan pendidikan. Jika akun-akun ini tidak dikelola dengan baik, dampaknya bisa fatal:

a. Akun dinas dipakai untuk menyebar pesan palsu atau hoaks.
b. Akun pribadi dibajak untuk penipuan "modus pinjaman".
c. Data pribadi seperti NIK, nomor rekening, atau foto KTP bocor dan disalahgunakan.

Intinya: satu akun bisa jadi pintu masuk serangan, jika tidak dikelola dengan bijak.

2. Pisahkan Akun Pribadi dan Akun Pekerjaan

- **Untuk ASN:**

Gunakan **akun email resmi instansi** untuk urusan kedinasan. Hindari memakai Gmail pribadi atau WhatsApp pribadi untuk berbagi dokumen kerja. Selain menjaga profesionalitas, pemisahan ini juga melindungi data instansi agar tidak tercampur dengan komunikasi pribadi.

- **Untuk masyarakat:**

Pisahkan akun belanja, perbankan, dan hiburan digital. Jangan gunakan satu akun email untuk semua platform. Jika satu akun diretas, yang lain tetap aman.

📍 *Kebiasaan sederhana ini dapat menurunkan risiko peretasan lintas akun hingga 80%*

3. Gunakan Autentikasi Dua Faktor (2FA)

Autentikasi dua faktor atau **2FA** adalah sistem keamanan tambahan yang memerlukan dua langkah verifikasi:

a. Password utama
b. Kode unik yang dikirim ke HP atau email
c. Jika peretas mengetahui password Anda, akun tetap tidak bisa diakses tanpa kode 2FA. Platform pemerintah seperti **e-Office, MySAPK, dan mail.go.id** sudah mendukung sistem ini.
d. Untuk masyarakat, 2FA bisa diaktifkan di aplikasi seperti WhatsApp, Gmail, dan Instagram melalui menu "Keamanan".

🧩 *Aktifkan 2FA sekarang, hanya butuh satu menit, tapi bisa menyelamatkan seluruh data Anda.*

4. Hindari Login Sembarangan dan Akses Publik

🚫 Jangan login akun penting di komputer umum (warnet, hotel, atau perangkat bersama). Gunakan mode *private/incognito* bila terpaksa. Hapus riwayat login dan pastikan sudah "log out" sebelum meninggalkan perangkat. ASN disarankan untuk **tidak menggunakan jaringan publik (Wi-Fi gratis)** saat mengakses data instansi. Gunakan VPN resmi jika bekerja dari luar kantor.

5. Rutin Periksa Aktivitas Akun

Hampir semua layanan digital kini memiliki fitur **"Login Activity"**. Cek secara berkala apakah ada login dari lokasi asing. Jika ada, segera ubah password dan aktifkan 2FA. BSSN juga menyarankan **pergantian password minimal setiap 6 bulan**, terutama untuk akun dinas.

D. Perlindungan Tambahan dalam Manajemen Akun Digital

1. Pentingnya Perlindungan Lapisan Kedua

Keamanan digital tidak cukup hanya dengan password kuat.

Bayangkan password seperti **kunci pintu rumah**, sementara perlindungan tambahan adalah **pintu pagar dan kamera pengawasnya**. Lapisan keamanan tambahan memberi waktu dan peringatan sebelum akun Anda disalahgunakan. BSSN (2024) mencatat bahwa akun yang menggunakan perlindungan ganda memiliki kemungkinan diretas **70% lebih rendah** dibanding akun yang hanya mengandalkan kata sandi.

2. Backup Data Secara Berkala

🔁 **Backup atau cadangan data** berarti menyalin informasi penting (dokumen, foto, data kerja, dsb.) ke tempat penyimpanan lain, seperti flashdisk, hard disk eksternal, atau penyimpanan awan (cloud). Hal ini penting agar data tetap bisa dipulihkan jika perangkat hilang, rusak, atau terkena ransomware.

🗂️ **Rekomendasi praktik backup:**

a. ASN → lakukan backup dokumen kerja ke **server instansi atau cloud resmi pemerintah (drive.go.id)**.
b. Masyarakat → gunakan layanan aman seperti Google Drive, OneDrive, atau Mega.nz, dengan verifikasi dua langkah aktif.
c. Simpan salinan offline untuk dokumen sangat penting.

💡 **Ingat:** backup bukan hanya cadangan, tapi juga *bukti tanggung jawab digital*.

3. Batasi Izin Aplikasi dan Perangkat

Banyak aplikasi meminta akses ke kontak, lokasi, mikrofon, bahkan kamera padahal tidak relevan. Kebiasaan menekan “Allow” tanpa membaca izin adalah pintu masuk pencurian data.

🔍 **Langkah sederhana untuk membatasi izin:**

a. Buka “Pengaturan → Privasi & Keamanan” di HP Anda.
b. Nonaktifkan akses aplikasi yang tidak diperlukan.
c. Cabut izin untuk aplikasi yang tidak digunakan lebih dari 30 hari.
d. ASN wajib melakukan pemeriksaan izin aplikasi minimal **setiap tiga bulan** untuk mencegah kebocoran data internal melalui aplikasi pihak ketiga.

4. Kelola Perangkat yang Terhubung

Kadang kita login akun di banyak perangkat laptop kantor, HP pribadi, bahkan komputer umum. Jika tidak dikelola, perangkat lama tetap menyimpan akses aktif, yang bisa dimanfaatkan oleh pihak tidak bertanggung jawab.

🧭 **Langkah aman:**

a. Periksa daftar perangkat aktif di akun (misal: *"Perangkat yang sedang masuk"* di Google, Microsoft, atau e-office).
b. Klik "Keluar dari semua perangkat" setelah pergantian HP/laptop.
c. Hindari penggunaan HP kantor untuk urusan pribadi, begitu pula sebaliknya.

5. Lindungi Akun dari "Lupa Password"

Masalah umum bukan hanya diretas, tapi **tidak bisa login karena lupa password**. Solusi modern kini lebih aman, tanpa perlu menulis password di kertas.

🔑 **Cara cerdas mengatasi lupa password:**

a. Gunakan **password manager resmi** (Bitwarden, NordPass, Google Passwords).
b. Simpan *recovery code* dengan aman di tempat berbeda (bukan di ponsel).
c. Perbarui email pemulihan agar selalu aktif dan bisa diakses.

E. Studi Kasus dan Praktik Baik dalam Keamanan Akun Digital

1. Kasus Nyata: Kebocoran Akun Akibat Password Lemah (Indonesia, 2024)

Pada tahun 2024, Badan Siber dan Sandi Negara (BSSN) mencatat lebih dari **30 juta data akun pengguna** di Indonesia bocor dan diperjualbelikan di forum daring. Sebagian besar kasus terjadi karena **pengguna menggunakan kata sandi yang sama di banyak platform**, atau karena **password yang terlalu sederhana** seperti *123456*, *admin*, dan *qwerty*. Salah satu contoh yang menjadi sorotan adalah **insiden kebocoran akun e-commerce lokal**, di mana banyak akun ASN dan masyarakat ikut terdampak. Dari hasil investigasi, ditemukan bahwa:

a. Password tidak pernah diganti sejak 2021,
b. Tidak ada aktivasi autentikasi dua faktor,

c. Banyak pengguna memakai alamat email dinas untuk login pribadi.

Kasus ini menunjukkan bahwa **keamanan akun bukan tanggung jawab teknologi semata, tapi juga perilaku pengguna.**

3. Praktik Baik Masyarakat Klungkung: Literasi Digital dari Desa

Masyarakat Desa Akah, Klungkung, menginisiasi gerakan "**Aman Digital dari Desa**" pada 2024. Melalui pelatihan sederhana yang diselenggarakan di balai desa, warga belajar:

a. Cara membuat password kuat,
b. Cara mengaktifkan *two-factor authentication* (2FA) di WhatsApp,
c. Cara mengenali pesan palsu dan modus penipuan online.

Kini, lebih dari **80% warga peserta pelatihan telah mengganti password mereka secara berkala**, dan **angka penipuan online di wilayah tersebut menurun signifikan**. Inisiatif seperti ini menunjukkan bahwa edukasi sederhana bisa memberi dampak besar jika dilakukan bersama-sama.

4. Praktik Baik ASN: Pengelolaan Akun Dinas Secara Terpadu

Dinas Kependudukan dan Catatan Sipil Klungkung menjadi contoh penerapan manajemen akun yang baik. Setiap pegawai:

a. Menggunakan email resmi dengan domain *@klungkungkab.go.id*,
b. Menerapkan *password rotation policy* setiap 90 hari,
c. Menggunakan *password manager internal* yang terenkripsi,
d. Melakukan pelatihan keamanan digital rutin tiap semester.

Pertanyaan Reflektif

1. Banyak orang menganggap mengganti password itu merepotkan. Menurut Anda, bagaimana cara membangun kebiasaan rutin mengganti password tanpa merasa terbebani, baik di lingkungan kantor maupun di rumah?
2. Seorang rekan ASN Anda masih menggunakan password yang sama di semua aplikasi kerja karena takut lupa. Jika Anda di posisi tersebut, bagaimana Anda akan menjelaskan risikonya tanpa membuat rekan tersebut merasa disalahkan?
3. Anda sedang bekerja di luar kantor dan butuh mengakses data penting melalui Wi-Fi publik di kafe. Apa langkah aman yang sebaiknya dilakukan agar data dan akun Anda tetap terlindungi?
4. Sebagian masyarakat masih percaya bahwa menyimpan password di catatan ponsel itu aman. Bagaimana cara Anda menjelaskan risiko kebiasaan ini kepada masyarakat agar mereka lebih sadar pentingnya manajemen akun?
5. Dalam konteks ASN, apa hubungan antara keamanan akun pribadi dan kepercayaan publik terhadap instansi pemerintah? Apakah pelanggaran kecil seperti membagikan akun dinas ke rekan kerja bisa berdampak besar terhadap reputasi instansi?
6. Anda menerima email mencurigakan yang seolah-olah berasal dari atasan dan meminta login ulang ke sistem e-office. Apa langkah konkret yang harus dilakukan sebelum mengambil tindakan apa pun?
7. Sebagai bagian dari masyarakat digital di Kabupaten Klungkung, apa satu perubahan perilaku yang bisa Anda mulai hari ini untuk memperkuat keamanan akun pribadi maupun keluarga Anda?
8. Dalam konteks tugas pelayanan publik, bagaimana Anda memastikan keamanan akun dinas tidak terganggu meskipun bekerja dari rumah (WFH) atau perangkat pribadi?

DAFTAR PUSTAKA

Badan Siber dan Sandi Negara (BSSN). (2023). *Panduan Keamanan Akun Digital untuk ASN dan Masyarakat.* Direktorat Keamanan Siber dan Sandi Pemerintahan. https://bssn.go.id/panduan-keamanan-akun-digital/

Badan Siber dan Sandi Negara (BSSN). (2024). *Laporan Tahunan Keamanan Siber Indonesia 2024.* Jakarta: BSSN. https://bssn.go.id/laporan-tahunan-bssn-2024

European Union Agency for Cybersecurity (ENISA). (2023). *Password Management Guidelines.* Athens: ENISA. https://doi.org/10.2824/38274

Google Safety Center. (2024). *Tips Keamanan Akun dan Penggunaan Password Manager.* https://safety.google/security/passwords/

Kementerian Komunikasi dan Informatika Republik Indonesia (Kominfo). (2023). *Pedoman Perlindungan Data Pribadi dan Keamanan Akun Digital.* Direktorat Jenderal Aplikasi Informatika. https://aptika.kominfo.go.id

Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi (KemenPANRB). (2023). *Kebijakan Keamanan Sistem Pemerintahan Berbasis Elektronik (SPBE).* https://spbe.go.id

Microsoft Security. (2024). *Passwordless Authentication: The Future of Account Security.* https://www.microsoft.com/security/blog/2024/03/10/passwordless-authentication-future/

National Institute of Standards and Technology (NIST). (2023). *Digital Identity Guidelines: Authentication and Lifecycle Management (SP 800-63B).* U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-63b

Verizon. (2024). *Data Breach Investigations Report (DBIR) 2024.* Verizon Enterprise Solutions. https://www.verizon.com/business/resources/reports/dbir/

World Economic Forum (WEF). (2024). *Global Cybersecurity Outlook 2024.* Geneva: WEF. https://www.weforum.org/reports/global-cybersecurity-outlook-2024