

Modul 2 – Mengamankan Akun dan Password

Lindungi aset digital bisnis Anda dari akses tidak sah. Modul ini membekali Anda dengan strategi praktis untuk membuat password kuat, mengelola kredensial, dan mengaktifkan lapisan keamanan tambahan pada akun-akun bisnis penting.

Edy Susanto - Founder C-SIX Security



Gambaran Modul

Apa yang Akan Kita Pelajari?

Modul ini dirancang untuk membantu pemilik usaha dan pengelola akun bisnis memahami ancaman nyata terhadap keamanan akun digital, sekaligus memberikan solusi praktis yang dapat langsung diterapkan.

01

Password yang Kuat

Teknik membuat dan mengelola kata sandi yang sulit diretas

02

Password Manager

Alat bantu untuk menyimpan dan mengelola password secara aman

03

Multi-Factor Authentication

Lapisan keamanan tambahan di luar password biasa

04

Keamanan Akun Bisnis

Email, WhatsApp Business, dan media sosial bisnis



Mengapa Keamanan Akun Sangat Penting?

Ancaman Nyata

- Pembajakan akun media sosial bisnis
- Pencurian data pelanggan
- Penipuan mengatasnamakan bisnis Anda
- Kehilangan akses ke akun email utama

Dampak bagi Bisnis

Akun bisnis yang dibajak dapat merusak reputasi, menghilangkan kepercayaan pelanggan, dan menyebabkan kerugian finansial yang signifikan. Banyak usaha kecil tidak dapat pulih setelah insiden keamanan besar.

⚠️ 81% pelanggaran data melibatkan password yang lemah atau dicuri.

Materi 1

Cara Membuat Password yang Kuat

Password yang kuat adalah garis pertahanan pertama Anda. Hindari password yang mudah ditebak seperti nama, tanggal lahir, atau kata sederhana. Gunakan kombinasi yang kompleks dan unik untuk setiap akun.



Minimal 12 Karakter

Semakin panjang password, semakin sulit diretas. Targetkan 12–16 karakter.



Kombinasi Karakter

Gabungkan huruf besar, huruf kecil, angka, dan simbol seperti @, #, atau !.



Unik untuk Setiap Akun

Jangan gunakan password yang sama di dua akun berbeda. Satu bocor, semua terancam.



Hindari Informasi Pribadi

Nama, tanggal lahir, nama bisnis, atau kata umum sangat mudah ditebak oleh peretas.



Tip: Gunakan frasa acak seperti **Kopi!Meja7Langit#Biru** – panjang, mudah diingat, sulit ditebak.

Password Manager: Solusi Cerdas Mengelola Password

Mengingat puluhan password yang berbeda dan kompleks adalah hal yang mustahil. **Password Manager** adalah aplikasi yang menyimpan semua password Anda dalam satu brankas terenkripsi. Anda hanya perlu mengingat satu *master password*.

Rekomendasi Aplikasi

Bitwarden

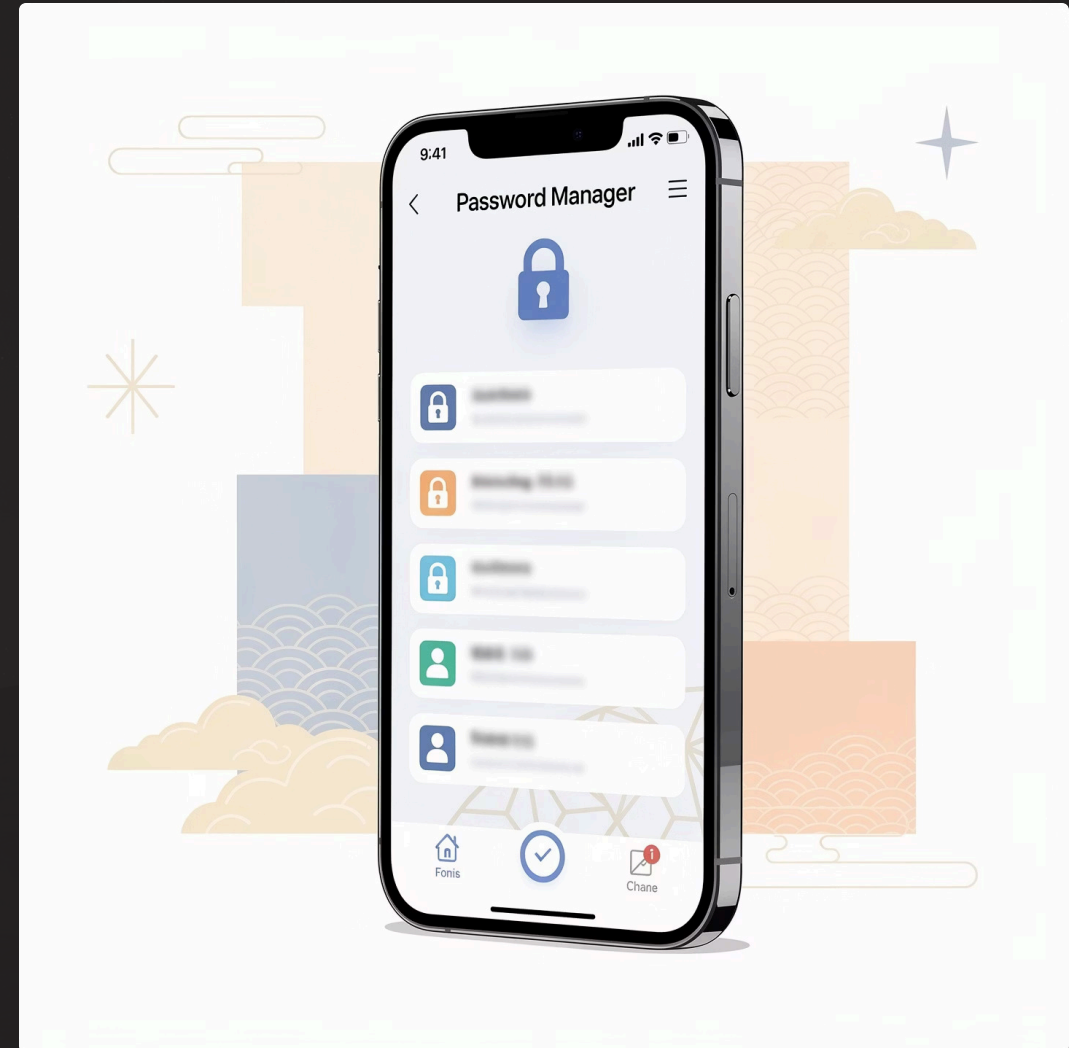
Gratis, open-source, tersedia di semua platform

1Password

Berbayar, antarmuka ramah pengguna, fitur tim

Google Password Manager

Terintegrasi dengan akun Google, mudah digunakan

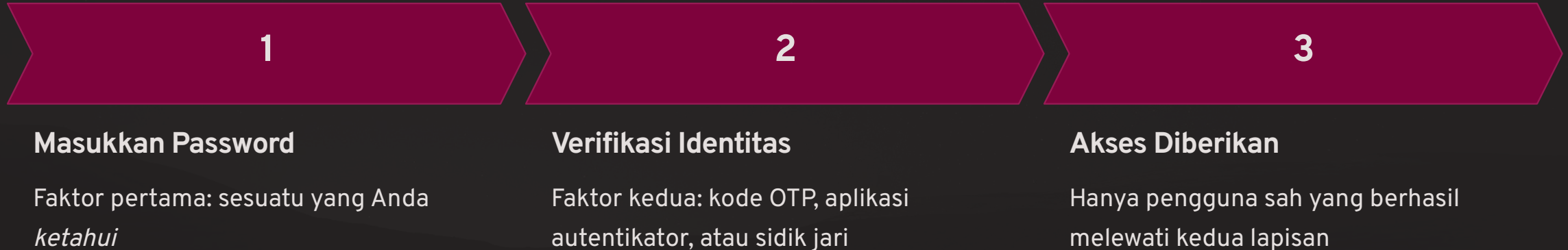


- ✔ Manfaat utama: Password Manager dapat membuat password acak yang sangat kuat secara otomatis dan mengisinya saat Anda login.

Materi 3

Multi-Factor Authentication (MFA)

MFA menambahkan lapisan keamanan kedua di luar password. Meskipun password Anda bocor, peretas tetap tidak bisa masuk tanpa faktor verifikasi kedua yang hanya ada pada Anda.



i **Aplikasi MFA yang direkomendasikan:** Google Authenticator, Microsoft Authenticator, atau Authy. Lebih aman dibanding kode SMS karena tidak bisa dicegat.

Materi 4 & 5

Mengamankan Akun Email & WhatsApp Business

Keamanan Email Bisnis

Email adalah kunci utama hampir semua akun digital. Jika email bisnis Anda dibajak, semua akun lain yang terhubung ikut terancam.

- Aktifkan MFA pada akun Gmail / Outlook bisnis
- Periksa aplikasi pihak ketiga yang memiliki akses
- Pantau aktivitas login dari lokasi atau perangkat asing
- Jangan gunakan email bisnis untuk hal pribadi

Keamanan WhatsApp Business

WhatsApp Business sering menjadi target pembajakan karena digunakan langsung untuk komunikasi dengan pelanggan.

- Aktifkan **Verifikasi Dua Langkah** di Pengaturan > Akun
- Jangan pernah berbagi kode OTP kepada siapapun
- Batasi siapa yang dapat melihat profil dan status bisnis
- Waspada terhadap upaya *SIM swap* dari operator seluler

Materi 6

Mengamankan Media Sosial Bisnis

Akun Instagram, Facebook, TikTok, dan platform media sosial bisnis lainnya adalah aset berharga yang membutuhkan perlindungan ekstra, terutama karena digunakan untuk berinteraksi langsung dengan pelanggan dan menjalankan iklan.



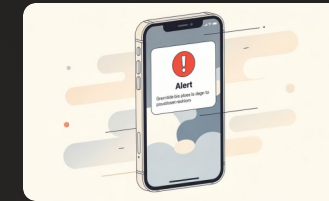
Instagram & Facebook

- Aktifkan autentikasi dua faktor
- Audit aplikasi yang terhubung secara berkala
- Gunakan *Trusted Contacts* sebagai cadangan



Kelola Akses Admin

- Batasi jumlah admin akun bisnis
- Hapus akses mantan karyawan segera
- Gunakan *Business Manager* untuk kontrol terpusat



Pantau Aktivitas Mencurigakan

- Aktifkan notifikasi login dari perangkat baru
- Periksa riwayat aktivitas secara rutin
- Segera respon email peringatan keamanan

Sesi Praktik

Aktivitas: Aktifkan MFA & Audit Password

Sekarang saatnya mempraktikkan apa yang telah dipelajari. Selesaikan dua aktivitas berikut bersama fasilitator. Pastikan Anda memiliki smartphone dan akses ke akun bisnis utama Anda.

✔ Praktik 1: Aktivasi MFA

1. Unduh aplikasi **Google Authenticator** atau **Authy** di smartphone Anda
2. Buka pengaturan keamanan akun Google atau email bisnis Anda
3. Cari opsi *Verifikasi 2 Langkah* dan ikuti panduan aktivasi
4. Scan kode QR dengan aplikasi autentikator
5. Simpan kode cadangan (*backup codes*) di tempat aman

🔍 Praktik 2: Audit Password Sederhana

1. Buat daftar semua akun bisnis yang Anda gunakan
2. Identifikasi akun mana yang masih menggunakan password lemah atau duplikat
3. Prioritaskan akun email, WhatsApp, dan media sosial untuk diperbarui terlebih dahulu
4. Ganti password dengan kombinasi kuat (gunakan metode frasa acak)
5. Catat pembaruan di password manager pilihan Anda

⚠ Jangan tunda! Lakukan audit ini setidaknya sekali setiap 3 bulan.



Ringkasan & Outcome Modul 2

Setelah menyelesaikan modul ini, Anda kini memiliki kemampuan nyata untuk melindungi akun bisnis dari ancaman pembajakan. Terapkan kebiasaan keamanan digital ini secara konsisten untuk menjaga kepercayaan pelanggan dan kelangsungan bisnis Anda.

Password Kuat

Buat password unik, panjang, dan kompleks untuk setiap akun bisnis

Password Manager


Gunakan Bitwarden atau alat serupa untuk mengelola semua kredensial dengan aman

MFA Aktif

Aktifkan autentikasi dua faktor di semua akun bisnis penting

Audit Rutin

Lakukan audit password dan review akses akun secara berkala setiap kuartal

 **Outcome:** Peserta mampu secara signifikan mengurangi risiko pembajakan akun bisnis melalui penerapan praktik keamanan yang telah dipelajari.