UPH Universitas Pelita Harapan | fit

PPK ORMAWA
HIMPUNAN MAHASISWA INFORMATIKA

MODUL SESI 5
OPTIMALISASI DIGITAL UMKM KELAPA DUA

DASAR CYBER SECURITY UNTUK UMKM

Katalog Digital dan *Strategic Coaching*
untuk Menggerakkan Ekonomi Lokal

hmp.informatics@cs-uph.net

Himpunan Mahasiswa
Informatika UPH Lippo Village

HMIF UPH

I. Kenapa Penting Memahami Keamanan Siber?

Dalam era digital saat ini, keamanan siber bukan lagi urusan perusahaan besar saja. Pelaku usaha mikro, kecil, dan menengah (UMKM) juga menjadi target utama serangan digital karena sering kali memiliki perlindungan yang minim. Penting sekali untuk meningkatkan kesadaran dan kemampuan dasar pelaku UMKM dalam melindungi data, perangkat, dan transaksi digital mereka.

UMKM harus memahami berbagai ancaman siber yang umum terjadi di lingkungan usaha kecil, mampu mengenali risiko, dan dapat menerapkan langkah-langkah sederhana untuk menjaga keamanan usaha di dunia digital.

II. Dasar Keamanan Siber

Keamanan siber adalah upaya melindungi sistem, jaringan, dan data dari akses tidak sah, kerusakan, atau pencurian. Bagi UMKM, keamanan digital berarti menjaga kepercayaan pelanggan.

Sering kali, pelaku UMKM beranggapan bahwa bisnis mereka terlalu kecil untuk diserang. Padahal, justru karena skala kecil inilah, mereka lebih rentan. Serangan dapat berupa pembobolan akun marketplace, kebocoran data pelanggan, hingga pencurian dana dari transaksi online.

Dampaknya bukan hanya kerugian finansial, tetapi juga rusaknya reputasi usaha dan hilangnya kepercayaan konsumen. Oleh sebab itu, keamanan siber harus dipandang sebagai investasi penting dalam menjaga keberlangsungan bisnis.

III. Jenis-Jenis Ancaman Siber yang Umum pada UMKM

UMKM perlu mengenali bentuk ancaman digital yang paling sering terjadi agar dapat menyiapkan langkah pencegahan yang tepat. Beberapa di antaranya meliputi:

a. Phishing

Phishing adalah upaya penipuan dengan mengelabui korban melalui email, pesan, atau tautan palsu agar memberikan informasi sensitif seperti kata sandi, data kartu kredit, atau akses akun bisnis.

Biasanya, penyerang menyamar sebagai pihak resmi seperti bank, marketplace, atau lembaga pemerintah. Ada beberapa bentuk phishing:

- Spoofing nama tampilan, yaitu pengirim menggunakan nama yang mirip dengan pihak terpercaya.
- Spoofing domain serupa, contohnya mengganti huruf dalam alamat email agar terlihat sah.
- Spoofing domain organisasi, di mana penyerang meniru domain perusahaan sebenarnya.

Untuk mengantisipasi, UMKM dapat menerapkan sistem DMARC (Domain-based Message Authentication, Reporting, and Conformance). DMARC membantu memverifikasi email agar penerima tahu apakah pesan benar berasal dari domain resmi atau bukan. Meskipun tidak menghentikan semua bentuk phishing, DMARC efektif mencegah penyerang yang mencoba menggunakan nama domain organisasi secara ilegal.

b. Malware dan Ransomware

Malware adalah perangkat lunak berbahaya yang dapat mencuri data, merusak sistem, atau mengunci file penting (ransomware). Serangan ini bisa datang dari lampiran email, situs web palsu, atau instalasi aplikasi tidak resmi. Akibatnya, data pelanggan, laporan keuangan, hingga sistem operasional bisa lumpuh total.

c. Pencurian Data Pelanggan

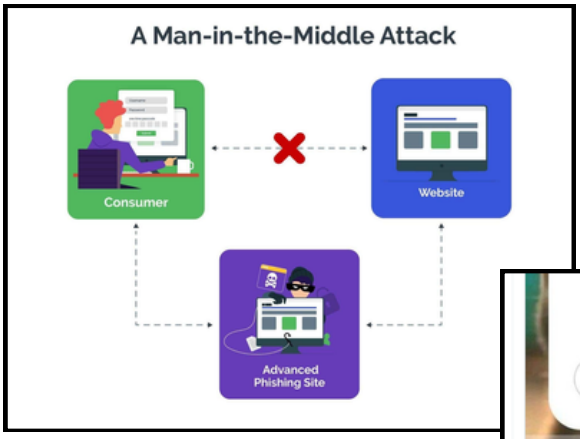
Data pelanggan seperti nomor telepon, alamat, dan riwayat pembelian sering menjadi sasaran karena memiliki nilai jual tinggi di pasar gelap digital.
Kebocoran data ini tidak hanya melanggar privasi tetapi juga bisa menurunkan kepercayaan pelanggan secara drastis.

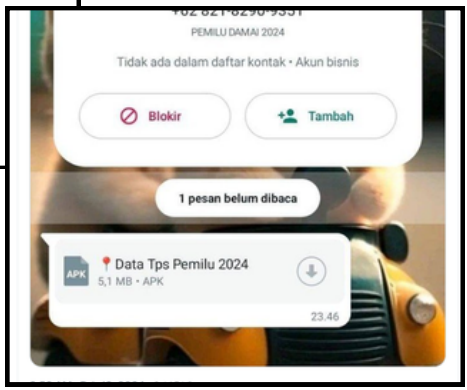
d. Serangan Melalui Media Sosial

Akun media sosial bisnis sering diretas untuk menyebarkan tautan berbahaya atau penipuan promo palsu. Karena media sosial menjadi etalase utama UMKM, kehilangan kendali atas akun dapat merusak citra usaha secara cepat.

e. Penggunaan Wi-Fi Publik yang Tidak Aman

Mengakses akun bisnis melalui Wi-Fi publik berisiko karena data bisa disadap oleh pihak lain di jaringan yang sama. Hindari login ke akun penting saat menggunakan koneksi publik tanpa perlindungan VPN.





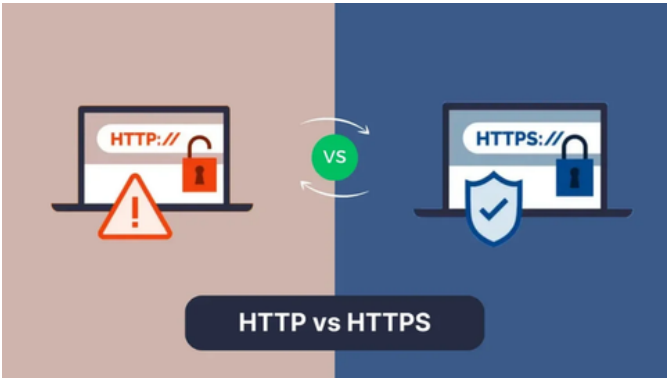
IV. Prinsip Dasar Keamanan Siber: CIA Triad

Keamanan siber memiliki tiga pilar utama yang dikenal dengan istilah CIA Triad, yaitu Confidentiality, Integrity, dan Availability. Ketiga prinsip ini menjadi dasar dari setiap kebijakan keamanan digital.

a. Confidentiality (Kerahasiaan)

Kerahasiaan berarti menjaga agar informasi hanya dapat diakses oleh pihak yang berwenang. Contohnya: penggunaan kata sandi yang kuat, autentikasi dua faktor (2FA), serta enkripsi data.

Enkripsi adalah proses mengubah data menjadi kode yang tidak bisa dibaca oleh pihak lain tanpa kunci tertentu. Misalnya, data transaksi di toko online sebaiknya dikirim melalui protokol HTTPS, bukan HTTP biasa, agar aman dari penyadapan.



b. Integrity (Keutuhan)

Integritas memastikan bahwa data tidak diubah atau dimanipulasi tanpa izin. Penerapan integritas dapat dilakukan dengan memperbarui sistem dan aplikasi secara berkala, memantau log aktivitas pengguna, dan menghindari penggunaan software bajakan. Tujuannya adalah menjaga agar data tetap asli, akurat, dan dapat dipercaya.

c. Availability (Ketersediaan)

Ketersediaan berarti sistem dan data selalu dapat diakses saat dibutuhkan.

Langkah praktis untuk menjaganya antara lain:

- Memiliki server yang andal
- Melakukan backup data secara berkala
- Menggunakan perlindungan daya cadangan (UPS) untuk mencegah kehilangan data akibat mati listrik.

Dengan menjaga keseimbangan antara tiga pilar CIA ini, UMKM dapat membangun fondasi keamanan digital yang kokoh.

V. Perlindungan Data dan Transaksi Digital

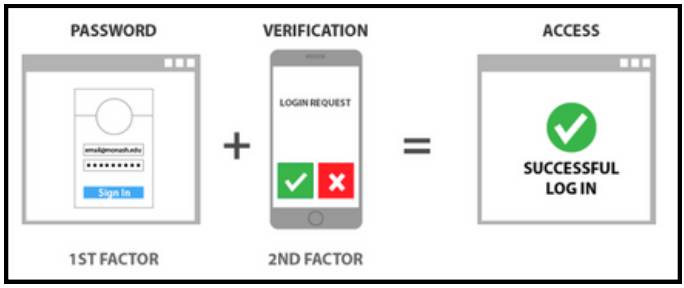
Data pelanggan dan transaksi digital merupakan aset utama bagi UMKM. Oleh karena itu, perlindungan terhadap dua hal ini wajib menjadi prioritas. Beberapa praktik penting yang bisa diterapkan antara lain:

a. Gunakan Enkripsi dan HTTPS

Pastikan situs web bisnis atau halaman transaksi menggunakan protokol HTTPS, yang berarti data dikirim melalui jalur terenkripsi. Hindari mengirim informasi sensitif melalui situs tanpa simbol gembok di bilah alamat browser.

b. Simpan Data Pelanggan dengan Aman

Data pelanggan sebaiknya tidak disimpan di perangkat pribadi tanpa perlindungan. Gunakan penyimpanan berbasis cloud terpercaya dengan autentikasi ganda, atau media eksternal terenkripsi. Jangan pernah membagikan data pelanggan kepada pihak ketiga tanpa izin.

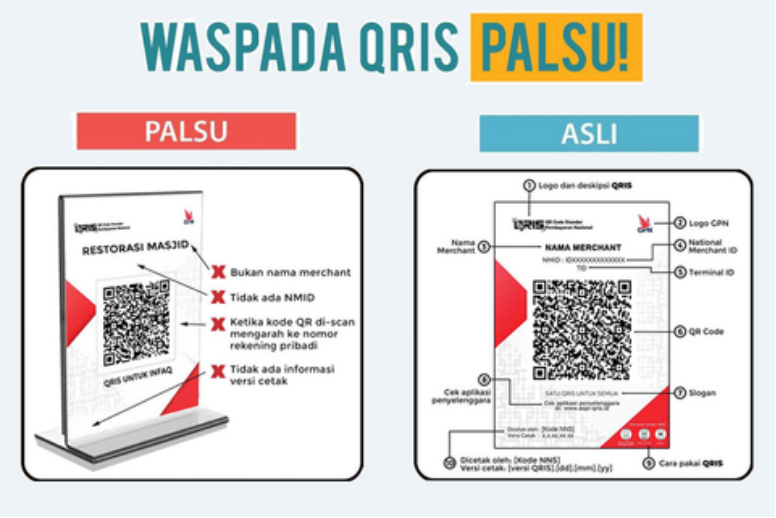


c. Lindungi Akun dan Perangkat Bisnis

Gunakan perangkat kerja yang terpisah dari perangkat pribadi. Pastikan akun bisnis seperti email, marketplace, atau WhatsApp Business dilengkapi 2FA dan menggunakan password unik yang berbeda dari akun pribadi.

d. Edukasi Tim dan Karyawan

Kesadaran keamanan tidak cukup hanya di tingkat pemilik usaha. Semua anggota tim perlu memahami risiko digital, cara mengenali email mencurigakan, dan pentingnya menjaga kerahasiaan akun perusahaan. Edukasi yang konsisten dapat mencegah banyak kesalahan manusia yang sering menjadi penyebab utama kebocoran data.



VI. Langkah-Langkah Praktis Keamanan Siber untuk UMKM

Berikut daftar tindakan sederhana yang bisa diterapkan sehari-hari oleh pelaku UMKM:

✅ **Backup Data Secara Rutin**
Simpan salinan data di cloud atau media eksternal. Backup melindungi dari kehilangan akibat serangan ransomware atau kerusakan perangkat.

✅ **Perbarui Sistem dan Aplikasi**
Pembaruan software membawa perbaikan keamanan penting. Selalu gunakan versi terbaru dari sistem operasi, aplikasi kasir, atau browser.

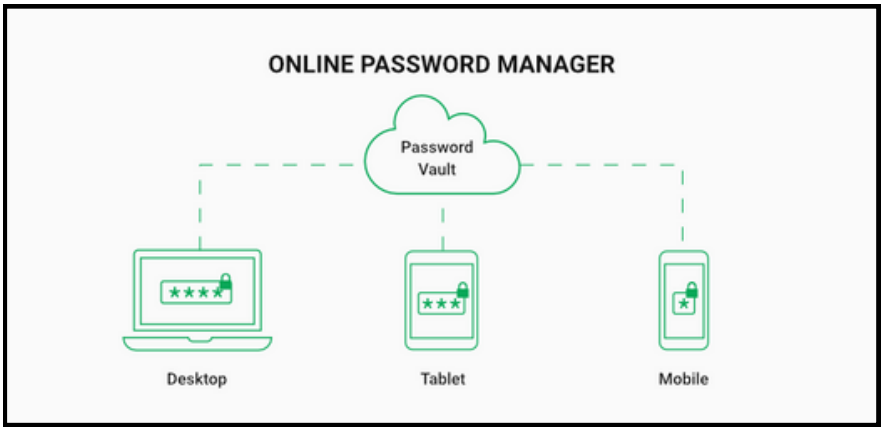
✅ **Gunakan Antivirus Resmi**
Hindari antivirus bajakan. Gunakan produk yang memiliki dukungan pembaruan rutin agar dapat mengenali ancaman terbaru.

✅ **Edukasi Karyawan**
Lakukan pelatihan singkat tentang keamanan digital, seperti mengenali tautan palsu dan cara membuat password yang kuat.

✅ **Gunakan Password Manager**
Aplikasi pengelola kata sandi membantu menyimpan dan menghasilkan password kuat tanpa perlu mengingat semuanya.

✅ **Gunakan Akun Bisnis Resmi di Media Sosial**
Hindari mencampur akun pribadi dan bisnis. Akun resmi memudahkan pengelolaan keamanan serta pemulihan bila diretas.

Dengan mengikuti langkah-langkah tersebut, UMKM dapat meminimalkan risiko serangan tanpa perlu investasi besar.



VII. Contoh Kasus Nyata

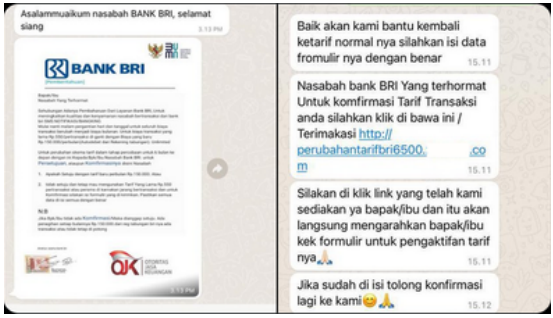
1. Phishing (Penipuan Lewat Email atau Pesan Palsu)

Contoh kasus:

- Anda menerima email dari “Bank BCA” yang meminta untuk verifikasi akun lewat tautan. Saat diklik, halaman login terlihat mirip situs asli, tapi sebenarnya palsu. Begitu Anda mengetik username dan password, data langsung dicuri.
- Pesan WhatsApp berisi link “Hadiah 1 juta dari Shopee” atau “Update layanan e-banking”. Padahal link itu mengarahkan ke situs palsu yang mencuri data login atau menginstal malware.

Ciri-ciri:

- Alamat pengirim mirip tapi tidak persis (contoh: bca-verifikasi@gmail.com).
- Pesan mendesak (contoh: “Akun Anda akan diblokir dalam 24 jam”).
- Tautan aneh atau tidak sesuai domain resmi.



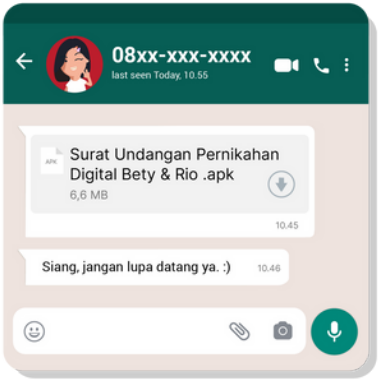
2. File Berbahaya (.APK / .EXE Palsu)

Contoh kasus:

- Undangan pernikahan digital dalam bentuk file .apk (biasanya dikirim lewat WhatsApp). Saat diinstal di Android, file tersebut meminta izin akses SMS dan kontak, lalu mencuri data OTP dari SMS banking.
- Aplikasi “cek bantuan sosial” atau “cek resi ekspedisi” dalam bentuk .apk juga sering ternyata berisi trojan pencuri data.

Tips:

- Jangan pernah menginstal file .apk dari luar Google Play Store.
- Pastikan sumber aplikasi resmi (misalnya dari website instansi pemerintah).



3. Rekayasa Sosial (Social Engineering)

Contoh kasus:

- Penipu berpura-pura sebagai teknisi bank atau CS marketplace, meminta kode OTP “untuk verifikasi”. Padahal kode itu digunakan untuk mengambil alih akun Anda. Pihak perusahaan resmi tidak akan pernah meminta OTP!
- Modus “kenalan lama” yang mengaku butuh bantuan finansial juga sering dimanfaatkan untuk menipu lewat transfer online.

Intinya:

Penipu memanfaatkan kelemahan manusia, bukan sistem. Oleh karena itu, waspada lebih penting daripada sekadar alat keamanan.

4. Penggunaan Software Bajakan

Contoh kasus:

- UMKM menggunakan software kasir bajakan karena lebih murah. Tanpa disadari, software tersebut menyimpan backdoor yang memungkinkan pencurian data transaksi.

Risiko:

- Tidak ada pembaruan keamanan.
- Mudah dimasuki malware atau spyware.

Solusi:

- Gunakan software legal atau versi gratis resmi yang terpercaya (misalnya LibreOffice, GIMP, atau aplikasi POS open-source).

5. Penipuan Online Marketplace

Contoh kasus:

- Pelaku menyamar sebagai pembeli yang meminta penjual mengirimkan barang “melalui kurir khusus” dengan tautan pelacakan. Saat penjual membuka tautan, ia diarahkan ke situs login palsu yang mencuri akun Tokopedia/Shopee-nya.
- Penjual dikirim bukti transfer palsu dan diminta mengirim barang sebelum dana benar-benar masuk.

Tips:

- Selalu lakukan transaksi hanya di dalam platform resmi marketplace.
- Jangan percaya tautan yang dikirim lewat chat pribadi.

hmp.informatics@cs-uph.net

Himpunan Mahasiswa
Informatika UPH Lippo Village

HMIF UPH