

CYBER

Cyber Security Checklist untuk UKM

10 langkah wajib mengamankan bisnis dari serangan ransomware, phishing, dan data breach.

Kenapa UKM jadi target utama?

UKM sering dianggap "terlalu kecil untuk dihack" — asumsi berbahaya yang salah. Data menunjukkan justru UKM yang paling sering menjadi korban serangan siber karena defense mereka jauh lebih lemah dibanding korporasi besar.

Serangan ke UKM sering bermotif finansial: ransomware, business email compromise, atau pencurian data pelanggan untuk dijual. Rata-rata kerugian per insiden: Rp 200 juta - Rp 2 miliar.

Kabar baiknya: 80% serangan bisa dicegah dengan basic cyber hygiene. Checklist ini adalah standard minimum yang wajib dimiliki setiap UKM.

10 langkah wajib cyber security

1. Multi-Factor Authentication (MFA) di semua akun

MFA menambah lapisan verifikasi selain password (biasanya OTP via SMS/authenticator app). Bahkan jika password bocor, akun tetap aman. Aktifkan MFA untuk: email bisnis, cloud storage, banking, admin panel website, media sosial.

2. Password policy yang kuat

Gunakan password minimum 12 karakter, kombinasi huruf besar-kecil, angka, dan simbol. Setiap akun harus punya password unik. Gunakan password manager (1Password, Bitwarden) untuk mengelola. Ganti password setiap 90 hari untuk akun kritis.

3. Backup rutin dan uji restore

Backup semua data critical setiap hari, simpan di lokasi terpisah (cloud + external drive). Ikuti aturan 3-2-1: 3 salinan data, 2 media berbeda, 1 offsite. Yang lebih penting: uji restore backup setiap 3 bulan untuk memastikan backup benar-benar working.

4. Software updates dan patch management

Ransomware sering exploit vulnerability di software yang tidak di-update. Aktifkan auto-update untuk OS, browser, dan aplikasi bisnis. Untuk server, jadwalkan patching mingguan.

5. Endpoint security

Pasang antivirus enterprise-grade (Bitdefender, Kaspersky, ESET) di semua device kerja. Aktifkan firewall Windows/Mac. Untuk device mobile karyawan yang akses data bisnis, gunakan MDM (Mobile Device Management).

6. Security awareness training

Human adalah link paling lemah. Training karyawan minimum sekali per tahun tentang: cara mengenali phishing, tidak klik link mencurigakan, jangan share password, verify permintaan tidak biasa via channel lain. Test dengan simulated phishing.

7. Access control dan least privilege

Berikan akses hanya seperlunya (need-to-know basis). Sales tidak perlu akses ke sistem HR. Segera revoke akses saat karyawan resign atau pindah role. Audit access rights setiap 6 bulan.

8. Email security

Email adalah vector serangan #1. Aktifkan spam filter dan phishing detection di email provider. Untuk domain sendiri, setup SPF, DKIM, dan DMARC records untuk mencegah email spoofing. Ajarkan karyawan verify sender email dan URL sebelum klik.

9. Incident response plan

Siapkan playbook untuk kasus insiden: siapa yang harus dihubungi, urutan langkah, komunikasi ke pelanggan, notifikasi ke regulator (UU PDP). Update playbook dan test setahun sekali.

10. Cyber insurance

Sebagai lapisan proteksi finansial, cyber insurance menanggung biaya recovery, notifikasi data breach, tuntutan hukum, dan denda regulasi. Wajib untuk bisnis yang menyimpan data pelanggan atau bergantung pada sistem digital.

Self-assessment: seberapa siap cyber security bisnis Anda?

Ceklist di bawah. Skor 8+ dari 10 = cukup baik. Skor 5-7 = perlu perbaikan urgent. Skor <5 = risiko tinggi, prioritaskan segera.

- ☐ MFA aktif untuk semua akun bisnis
- ☐ Password manager digunakan oleh semua karyawan
- ☐ Backup harian aktif dan sudah di-test restore dalam 3 bulan terakhir
- ☐ Semua software OS dan aplikasi di-update mingguan
- ☐ Antivirus enterprise-grade terpasang di semua device
- ☐ Semua karyawan sudah training security awareness dalam 12 bulan terakhir
- ☐ Access control policy sudah diterapkan (least privilege)
- ☐ Email domain sudah setup SPF, DKIM, DMARC
- ☐ Incident response plan sudah dibuat dan diketahui tim IT
- ☐ Cyber insurance sudah aktif dengan coverage minimum Rp 1 miliar

ACTION

Untuk setiap item yang belum tercentang, tetapkan deadline penyelesaian dan siapa yang bertanggung jawab. Review progress setiap bulan sampai semua tercentang.

LANGKAH SELANJUTNYA

Butuh diskusi lebih detail?

Panduan ini memberikan gambaran umum. Untuk kebutuhan spesifik bisnis Anda, tim Fortis Garda siap membantu — konsultasi awal 30 menit gratis dan tanpa komitmen.

HUBUNGI KAMI

WhatsApp: +62 813 9999 1244

Email: info@fortisgarda.com

Website: www.fortisgarda.com

Dokumen ini disusun untuk tujuan edukasi. Kondisi spesifik polis, cakupan, dan premi dapat berbeda tergantung profil risiko dan perusahaan asuransi. Selalu konsultasikan dengan agen atau broker asuransi berlisensi sebelum mengambil keputusan.