Nama = Cindy Naysilla Ismail

Kelas = Manajemen Informatika 5A

Mata Kuliah = Etika dan Hukum Teknologi Informasi

Mencari 5 Kejahatan di Dunia Cyber

1. **Illegal Online Gambling**

Contoh kasus **:** situs taruhan olahraga yang menerima taruhan warga Indonesia dan membayar/menarik uang lewat rekening atau e-wallet.

Modusnya **:** penyedia platform mempromosikan link lewat grup atau ads, menggunakan agen (bandar) lokal untuk deposit/withdraw, menyediakan sistem member/agen, dan menyamarkan transaksi sebagai "game" atau "investasi".

Sasarannya **:** orang dewasa rentan (pemburu keuntungan cepat), kelompok ekonomi menengah/kerja lepas, kadang korban direkrut lewat iklan sosial media atau referral.

Penanggulangan / pencegahan:

- Hentikan akses: blokir domain/nomor yang mempromosikan judi (oleh provider/Kominfo).
- Penguatan deteksi transaksi mencurigakan pada perbankan / fintech (lapor ke bank bila ada transaksi mencurigakan).
- Edukasi publik: bahaya adiksi & risiko penipuan.
- Penindakan: pelaporan ke polisi siber/Bareskrim dan koordinasi dengan penyedia layanan pembayaran untuk pembekuan dana.

Sejak Oktober 2024 sampai Mei 2025, Kementerian Komunikasi & Digital (Komdigi) telah memblokir lebih dari 1,3 juta konten judi online (termasuk situs dan alamat IP) yang tersebar di berbagai platform digital.

UU / pasal yang biasa dipakai untuk menjerat : kegiatan penyebaran dan/atau membuat akses terhadap informasi elektronik yang berisi muatan perjudian dapat dijerat UU ITE (Pasal 27 ayat (2) jo. ketentuan pidana terkait), serta ketentuan KUHP tentang perjudian dan/atau Pasal-pasal pelengkap untuk bandar/penyelenggara. Sumber membahas penerapan Pasal 27 ayat (2) UU ITE terhadap judi online.

2. **Cyberstalking**

Cyberstalking adalah bentuk penguntitan atau pelecehan yang dilakukan melalui media digital, biasanya dengan tujuan mengintimidasi, mengancam, atau mengontrol korban. Perilaku ini bersifat berulang (repetitif) dan bisa sangat meresahkan korban karena terasa seperti tidak bisa "lari" dari si pelaku, sebab dilakukan lewat dunia maya.

Contoh kasus : mantan pasangan mengirimi pesan ancaman, memantau lokasi lewat akun palsu, menyebar foto pribadi berulang kali, atau membuat akun palsu untuk mengintimidasi korban.

Modusnya : pembuatan akun palsu, penguntitan (persistent messaging), doxxing (menyebar data pribadi), pemantauan lokasi melalui metadata foto/fitur share location, atau pesan berulang yang menimbulkan teror/ketakutan.

Sasarannya : korban individu (mantan pasangan, tokoh publik, jurnalis, perempuan/anak muda), orang yang profil onlinenya terbuka.

Penanggulangan / pencegahan:

- Simpan bukti (screenshot, link, log pesan); blokir & laporkan akun.
- Aktifkan pengamanan akun (2FA), buat pribadi setting lebih ketat, hapus/limit publikasi data lokasi.
- Lapor ke Polri (unit siber) untuk tindak lanjut; gunakan tuntutan pidana bila ada ancaman/pelecehan.
- Dukungan psikologis & advokasi bagi korban.

UU / pasal yang biasa dipakai untuk menjerat: cyberstalking biasanya dituntut lewat kombinasi pasal UU ITE (ancaman/pencemaran nama baik/penyebaran informasi) seperti Pasal-Pasal di UU ITE yang mengatur ancaman/penyebaran informasi elektronik, serta ketentuan KUHP tentang pengancaman/pencemaran nama baik — makanya penanganannya sering memakai beberapa pasal sekaligus. Kajian/putusan terbaru menunjukkan penggunaan pasal UU ITE (mis. Pasal 27B/29/45B dalam amandemen) untuk menjerat pelaku

3. **Deepfake Crime**

Kronologi Kasus : Pada awal tahun 2025, masyarakat Indonesia dihebohkan dengan beredarnya video yang menampilkan Presiden **Prabowo Subianto** dan sejumlah pejabat negara lain, seperti Menteri Keuangan Sri Mulyani. Dalam video tersebut, mereka tampak berbicara mengenai adanya program bantuan sosial (bansos) atau giveaway yang bisa diakses oleh masyarakat. Agar terlihat meyakinkan, pelaku menggunakan teknologi deepfake untuk

memanipulasi wajah dan suara pejabat sehingga seolah-olah benar-benar memberikan pernyataan resmi. Video itu kemudian disebarkan secara masif melalui **media sosial** (Facebook, Instagram, TikTok) serta aplikasi perpesanan seperti WhatsApp dan Telegram. Dalam narasi, korban diarahkan untuk menghubungi nomor tertentu atau mengisi formulir online untuk mendapatkan "hadiah bansos".

Modus :

1. **Pembuatan Video Palsu**
    - Pelaku menggunakan teknologi *deep learning* untuk memanipulasi wajah Presiden Prabowo dan pejabat lain.
    - Hasil deepfake terlihat cukup meyakinkan karena meniru gerakan bibir dan suara.

2. **Penyebaran**
    - Video diunggah ke media sosial dan disebar lewat akun palsu atau grup WhatsApp.
    - Judul/video dikemas provokatif seperti: *"Bansos Gratis dari Presiden – Daftar Sekarang!"*.

3. **Umpan Penipuan**
    - Korban diarahkan untuk **mendaftar** di link atau kontak tertentu.
    - Untuk memproses "pencairan bansos", korban diminta membayar **biaya administrasi** Rp100 ribu – Rp1 juta.

4. **Eksploitasi Korban**
    - Setelah transfer, dana masuk ke rekening/ewallet milik pelaku.
    - Tidak ada bansos yang diterima, dan kontak pelaku sulit dilacak.

Sasaran :

- **Masyarakat umum**: terutama mereka yang aktif di media sosial.
- **Kelompok ekonomi rentan**: karena mudah tergiur janji bansos/uang cepat.
- **Orang tua / pengguna awam digital**: kurang bisa membedakan mana video asli dan manipulasi digital.

Diperkirakan lebih dari **100 orang menjadi korban** dengan kerugian sekitar **Rp65 juta** hanya dari satu pelaku (JS, ditangkap di Lampung).

Penanggulangan :

1. **Pihak Kepolisian (Polri Siber)**

- Melacak akun pelaku melalui jejak digital (rekening bank, e-wallet, nomor ponsel).
- Menangkap pelaku di Lampung dan mengungkap sindikat penyebaran konten deepfake.

2. **Kominfo**

    - Melakukan **takedown** terhadap video deepfake yang beredar.
    - Mengimbau masyarakat agar tidak mudah percaya dengan janji bansos online.

3. **Edukasi Publik**

    - Literasi digital digencarkan: ajakan untuk memverifikasi informasi melalui situs resmi pemerintah.
    - Masyarakat diingatkan untuk tidak membayar biaya apapun dalam program bansos resmi.

4. **Langkah Pencegahan**

    - Masyarakat disarankan mengecek informasi resmi di situs pemerintah.
    - Melaporkan akun/nomor yang menawarkan bansos mencurigakan.

Dasar Hukum :

Pelaku dalam kasus ini dijerat dengan:

1. **UU ITE (UU No. 11 Tahun 2008 jo UU No. 1 Tahun 2024)**

    - **Pasal 35**: setiap orang dengan sengaja membuat, mengubah, menghapus, merusak, menghilangkan Informasi Elektronik dengan tujuan agar dianggap seolah-olah data otentik → *deepfake termasuk dalam kategori ini*.
    - **Pasal 51 ayat (1)**: ancaman pidana penjara paling lama 12 tahun dan/atau denda paling banyak Rp12 miliar.

2. **KUHP Pasal 378 (Penipuan)**

    - Mengatur tentang penipuan dengan tipu muslihat yang menyebabkan orang menyerahkan barang/uang.
    - Ancaman pidana penjara paling lama 4 tahun.

Jika terbukti dilakukan secara terorganisir, pelaku juga bisa dijerat pasal lain terkait **pencucian uang** bila dana hasil penipuan dialirkan ke berbagai rekening.

4. IoT Hacking

Contoh kasus : peretas masuk ke kamera CCTV rumah atau thermostat pintar, menonaktifkan kamera, atau memanipulasi perangkat untuk memata-mata/menyebabkan kerusakan. Juga termasuk botnet yang memanfaatkan perangkat IoT untuk serangan DDoS.

Modusnya **:** eksploitasi firmware yang tak terupdate, password default, port terbuka, backdoor, atau serangan supply-chain; scanning massal mencari perangkat rentan; lalu memasang malware/botnet.

Sasarannya **:** perangkat konsumen (kamera CCTV, router, smart TV), fasilitas bisnis (sensor industri), rumah tangga, dan infrastruktur yang terhubung.

Penanggulangan / pencegahan **:**

5. Keamanan perangkat: ubah password default, patch/update firmware rutin, segmentasi jaringan (pisah IoT dari jaringan kerja/PC), non-aktifkan fitur remote yang tak perlu.
6. Provider/manufaktur: secure-by-design, update OTA, penanganan CVE.
7. Penegakan: bila ada akses tanpa izin ke sistem elektronik, dapat dilaporkan ke polisi; lakukan forensic untuk menilai dampak (kebocoran data).

UU / pasal yang biasa dipakai untuk menjerat: akses ilegal ke komputer/sistem elektronik dan perusakan/penyadapan diatur di UU ITE (mis. Pasal 30 tentang mengakses sistem elektronik tanpa hak) — sehingga peretasan IoT umumnya dijerat dengan pasal-pasal UU ITE; bila terjadi kebocoran data pribadi, juga relevan UU Perlindungan Data Pribadi (UU PDP).

5. **Social Engineering**

Contoh kasus **:** pelaku menelepon korban berpura-pura dari bank, meminta OTP/credential; atau mengirim email phish yang menipu korban memasukkan data login ke situs palsu; hasilnya: akses rekening atau pencurian identitas.

Modusnya **:** manipulasi psikologis (urgency, authority, fear), pembuatan situs/identitas palsu, pengiriman link berbahaya (phishing), telepon voice scam (vishing), SMS (smishing), dan rekayasa teknis untuk bypass verifikasi.

Sasarannya **:** nasabah bank, karyawan perusahaan (untuk akses korporat), pengguna layanan online yang kurang awas.

Penanggulangan / pencegahan:

- Edukasi berkelanjutan (jangka panjang) tentang tanda phising & rekayasa sosial.
- Prosedur organisasi: jangan berikan credential/OTP lewat telepon/email; prosedur verifikasi multi-saluran; least privilege untuk akses internal.
- Teknis: email filtering, DMARC/SPF/DKIM, MFA (two-factor authentication) — tapi MFA bukan pengaman absolut terhadap beberapa teknik social engineering.
- Lapor bila ada kerugian — penipuan online bisa dipidanakan (KUHP Pasal 378) dan/atau UU ITE (pasal-pasal tentang penipuan/akses ilegal/kejahatan elektronik).

UU / pasal yang biasa dipakai untuk menjerat: penipuan online/social engineering sering dijerat Pasal 378 KUHP (penipuan) sebagai dasar umum; lex specialis di UU ITE (mis. pasal tentang penipuan dan akses ilegal/penyalahgunaan sistem elektronik) juga sering diterapkan. Selain itu UU PDP relevan bila terjadi penyalahgunaan data pribadi.