# Lawan Pelecehan Seksual di Media Online

Pilar: Digital Safety

Andrey Ferriyan

https://andrey.web.id

# Andrey Ferriyan

Core Competency: Network Security

IT Director: ATSOFT Teknologi (https://atsoft.co.id)

# Asal Mula Internet dan Perangkat Pendukungnya

- Dibangun sebagai sarana untuk transfer file dari satu komputer ke komputer lain
- Dibangun dan dikembangkannya web sebagai sarana pertukaran informasi antar saintis
- Dibangun dengan asumsi dan niat bahwa semua manusia itu baik

# Tantangan Bagi Pelajar

- Arus informasi yang begitu masif
- Literasi digital sebatas social media
- Mudah mengakses dan menyebarkan berita dan informasi hoax
- Kasus bullying dan penipuan
- Pelecehan seksual online

# Siapa saja yang rawan jadi korban?

- Seseorang yang terlibat dalam hubungan intim
- Profesional yang terlibat dalam ekspresi publik (jurnalis, penulis, peneliti, aktor, dan lain-lain)
- Penyintas dan korban penyerangan fisik

# Tipe Kekerasan Seksual Berdasarkan Pelanggaran

- Pelanggaran privasi
- Pengawasan dan pemantauan
- Perusakan kredibilitas
- Pelecehan (yang dapat disertai pelecehan *offline*)
- Ancaman dan kekerasan langsung
- Serangan pada target komunitas tertentu

# Pelanggaran privasi

- Bentuk pelanggaran:
  - Infringement privacy (pelanggaran privasi)
  - Malicious distribution (ancaman distribusi foto / video pribadi)
  - Cyber harassment (pelecehan online)
- Mengakses, menggunakan, memanipulasi, dan menyebarkan data pribadi baik dalam bentuk video atau foto tanpa persetujuan
- *Doxing* atau menggali dan menyebarkan informasi pribadi seseorang dengan tujuan pelecehan atau intimidasi di dunia nyata.

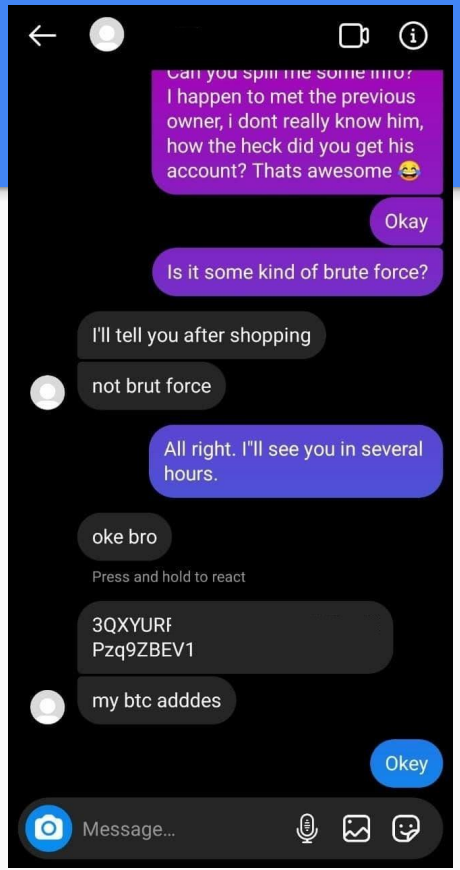
# Pengawasan dan Pemantauan

- Bentuk pelanggaran:
  - Hacking (peretasan)
  - Illegal content (konten ilegal)
- *Stalking* (menguntit)
- Memasang spyware atau aplikasi tertentu tanpa persetujuan
- Pelacakan target dengan GPS

# Perusakan Kredibilitas

- Bentuk pelanggaran:
  - Hacking (peretasan)
  - Illegal content (konten ilegal)
  - Online defamation (pencemaran nama baik)
- Mencuri identitas dan impersonasi (berpura-pura menjadi orang tersebut)
- Menyebarluaskan informasi pribadi untuk merusak reputasi seseorang
- Manipulasi dan membuat konten palsu

# Kasus Instagram

# Pelecehan (yang dapat disertai dengan pelecehan offline)

- Bentuk pelanggaran:
  - Online harassment (pelecehan online)
- Pelecehan berulang melalui pesan, perhatian, dan/atau kontak yang tidak diinginkan
- Komentar kasar
- Konten online yang menggambarkan perempuan sebagai objek seksual
- Penggunaan gambar tidak senonoh untuk merendahkan wanita

# Ancaman dan Kekerasan Langsung

- Bentuk pelanggaran:
  - Cyber grooming (pendekatan untuk memperdaya)
  - Online defamation (pencemaran nama baik)
  - Online recruitment (perekrutan online)
- Perdagangan perempuan melalui teknologi, termasuk pemilihan dan persiapan korban
- Pemerasan seksual
- Pencurian identitas dan properti
- Impersonasi dan peniruan yang berujung fisik

# Serangan dengan Target Komunitas Tertentu

- Bentuk pelanggaran:
  - Hacking (peretasan)
- Meretas situs web, media sosial, atau email
- Pengawasan
- Melakukan intimidasi dan pelecehan individu

# Bentuk Perlawanan

1. Dokumentasikan hal-hal yang terjadi pada diri
2. Selalu melakukan pemantauan situasi yang dihadapi
3. Mengamankan diri
4. Cari bantuan dan laporkan: https://linktr.ee/KomnasPerempuan
5. Blokir pelaku

# Bentuk Pencegahan

1. Pisahkan akun pribadi dengan akun publik
2. Cek dan atur ulang pengaturan privasi
3. Gunakan password yang kuat dan verifikasi login
4. Tidak melakukan pemasangan aplikasi pihak ketiga
5. Tidak berbagi pin / password apapun dengan orang lain

# Pencegahan: gunakan password manager

1. Online password manager (https://lastpass.com, https://1password.com)
2. Offline password manager (KeePass, KeePassXC, Bitwarden)

# Pencegahan: gunakan protokol enkripsi

1. Browsing selalu gunakan HTTPS ketika login ke dalam sebuah sistem aplikasi web
2. Gunakan password yang tidak mudah ditebak. Gunakan kombinasi:
   a. Angka, huruf besar kecil, dan karakter lain: iniC$$ontohpassword827
   b. Jumlah karakter password minimal adalah 10
3. Jangan menggunakan password seperti:
   a. Nama kita atau ada nama panggilan kita
   b. Tempat dan tanggal lahir
   c. Nama orang tua
   d. Alamat rumah

# Pencegahan: MFA

1. Selalu gunakan Multi Factor Authentication atau Two-Factor Authentication
    a. Instagram : https://help.instagram.com/566810106808145
    b. Facebook: https://web.facebook.com/help/148233965247823/?_rdc=1&_rdr
    c. TikTok: https://www.tiktok.com/safety/youth-portal/keep-your-account-secure?lang=en
2. Aplikasikan pada email dan sosial media anda

# Referensi

1. “Memahami dan Menyikapi Kekerasan Berbasis Gender Online”, SAFEnet (https://id.safenet.or.id/)

SELESAI