HSE PROGRAM		
	WEEKLY SAFETY TALK Periode : Juli 2026	

Safety Talk

Tanggal	: 8 Juli 2026	Lokasi	Ruang Teknis
Koordinator	: Anggun W Rahajeng	Signature	
Pembicara	: Bram Yudha Prakoso	Signature	
Topik	: Keamanan /Keselamatan		

Materi : AWAS DEEPFAKE & AI SCAM

Apa Itu DEEPFAKE ?

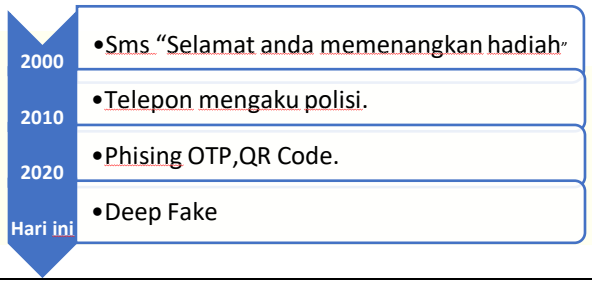
Deepfake adalah teknologi kecerdasan buatan (*AI*) yang memanipulasi atau membuat ulang video, gambar, dan audio manusia. Teknologi ini menggabungkan wajah, ekspresi, atau suara seseorang ke dalam kloningan digital agar terlihat dan terdengar sangat realistis seperti aslinya.



Pelaku mengumpulkan data seperti:

- Foto media sosial
- Video TikTok
- Reels Instagram

Evolusi Penipuan:



Teknologinya berubah. Tetapi targetnya tetap sama yaitu **Manusia.**

HSE PROGRAM		
	WEEKLY SAFETY TALK Periode : Juli 2026	

Bagaimana Deepfake Dibuat ?

1. Mengumpulkan data korban berupa foto, video, atau rekaman suara.
2. Memasukkan data yang telah dikumpulkan ke dalam sistem atau aplikasi berbasis AI.
3. Memberikan perintah (prompt) kepada AI, misalnya:"Buat orang ini mengatakan...""Tempatkan wajah ini ke video...“
4. AI mempelajari pola wajah dan suara dari data yang diberikan.
5. AI menghasilkan konten baru (deepfake) berupa video, gambar, atau audio yang tampak realistis.
6. Pelaku menyebarkan hasil deepfake melalui media sosial, aplikasi pesan, atau platform digital lainnya.

Mengapa Deepfake Sangat Menyakinkan?

AI tidak sekadar menempelkan foto. AI dapat menyesuaikan:

- Sudut wajah
- Ekspresi
- Pencahayaan
- Gerakan kepala
- Sinkronisasi bibir
- Nada bicara

Deepfake Menyerang Psikologi

Pelaku memanfaatkan berbagai bias kognitif manusia, antara lain:

Authority Bias
"Kalau yang bicara tokoh terkenal, pasti benar."

Confirmation Bias
"Ini sesuai keyakinan saya, berarti benar."

Emotional Bias
"Saya panik, berarti ini pasti nyata."

Social Proof Bias
"Semua orang membagikannya, berarti benar."

HSE PROGRAM		
	WEEKLY SAFETY TALK Periode : Juli 2026	

Mengapa Deepfake Berpotensi Lebih Berbahaya di Indonesia?

Ancaman deepfake di Indonesia diperparah oleh beberapa faktor:

1. Tingkat literasi masyarakat yang rendah.
2. Kebiasaan menyebarkan informasi tanpa verifikasi.
3. Kecenderungan mempercayai informasi yang sesuai dengan keyakinan atau emosi.
4. Budaya "katanya", "viral berarti benar", atau "saya lihat sendiri videonya".

Modus AI Scam yang Sedang Marak

Romance Scam

- Pelaku menggunakan foto, video, bahkan video call AI untuk membangun hubungan emosional sebelum meminta uang.

Investment Scam

- Video tokoh terkenal dimanipulasi untuk mengajak korban berinvestasi.

Ancaman yang Lebih Berbahaya: Deepfake Pornografi

Deepfake pornografi adalah penyalahgunaan teknologi AI untuk membuat foto atau video pornografi palsu yang menampilkan seseorang seolah-olah melakukan aktivitas seksual tanpa persetujuannya. Konten ini dibuat dari foto atau video korban dan tampak sangat realistis.

Dampaknya meliputi rusaknya reputasi, trauma psikologis, rasa malu, kecemasan, depresi, terganggunya hubungan pribadi maupun pekerjaan, serta berpotensi dimanfaatkan untuk pemerasan, pelecehan, dan perundungan. Konten yang sudah tersebar juga sulit dihapus sehingga dampaknya bisa berlangsung lama.

Motif Pelaku Deep Fake Pornografi Pelaku dapat memiliki berbagai tujuan, seperti:

- Balas dendam (revenge) terhadap mantan pasangan atau orang yang tidak disukai.
- Pelecehan seksual berbasis digital untuk mempermalukan korban.
- Pemerasan (sextortion) dengan mengancam akan menyebarkan konten palsu jika korban tidak membayar uang atau memenuhi tuntutan tertentu.
- Perundungan (cyberbullying) untuk merusak kondisi psikologis korban.
- Mencari keuntungan finansial melalui situs web atau layanan berbayar.

- Menyebarkan disinformasi untuk merusak reputasi tokoh publik

Mengapa AI Bisa Digunakan untuk Membuat Deepfake

1. **AI Bersifat Netral**
   AI hanyalah alat yang tidak memiliki niat, emosi, atau tujuan. AI hanya menjalankan perintah dari manusia, sehingga baik atau buruknya penggunaan AI bergantung pada penggunanya.
2. **Tidak Semua AI Memiliki Pengaman (Guardrails)**
   Guardrails adalah mekanisme keamanan yang membatasi AI agar tidak menghasilkan konten berbahaya, melanggar hukum, atau tidak etis. Layanan seperti **ChatGPT** memiliki guardrails, tetapi tidak semua AI menerapkannya dengan tingkat pembatasan yang sama.
3. **AI Open-Source**
   AI open-source dapat diunduh, dijalankan, dan dikendalikan sendiri oleh pengguna di komputer atau server mereka. Berbeda dengan layanan AI yang dikelola perusahaan, AI open-source memberikan kendali lebih besar kepada pengguna, sehingga pengguna juga bertanggung jawab atas cara penggunaannya Contoh.

Bagaimana Cara Kita Melindungi Diri?

1. Sampai di sini mungkin muncul pertanyaan. Kalau AI sudah secanggih ini, lalu bagaimana kita melindungi diri?
2. Apakah kita harus berhenti menggunakan media sosial?
3. Apakah kita harus takut dengan AI?

Scientific Temper(Sikap Ilmiah)

Scientific Temper adalah Kebiasaan berpikir berdasarkan bukti, logika, dan verifikasi sebelum mempercayai atau menyebarkan suatu informasi.
Sikap ini meliputi:

Bertanya
"Dari mana informasinya?"

Meminta bukti
"Apa sumbernya?"

Memeriksa ulang
"Apakah ada konfirmasi lain?"

Bersedia mengubah pendapat
"Kalau terbukti salah, saya siap mengoreksi."



HSE PROGRAM		
	WEEKLY SAFETY TALK Periode : Juli 2026	

Kenali Ciri-ciri Deepfake

beberapa tanda berikut masih dapat menjadi petunjuk:

1. **Pada Video**

- Gerakan bibir kurang sinkron dengan suara.
- Ekspresi wajah tampak kaku atau tidak alami.
- Kedipan mata terlalu sedikit atau tidak wajar.
- Pencahayaan dan bayangan pada wajah tidak sesuai dengan lingkungan.
- Tepi wajah, rambut, atau telinga tampak kabur atau berubah-ubah.
- Resolusi wajah berbeda dengan bagian tubuh lainnya.

2. **Pada Audio**

- Intonasi terdengar datar atau terlalu sempurna.
- Ada jeda yang tidak alami.
- Pengucapan kata tertentu terdengar aneh.
- Suara terdengar seperti robot pada beberapa bagian.



3. **Pada Video Call**

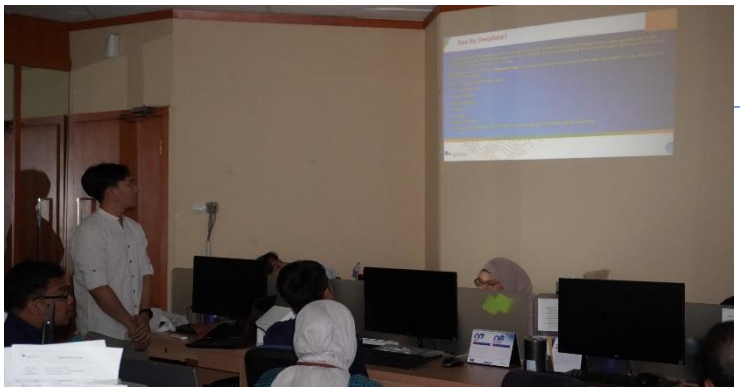
- Gerakan bibir terlambat mengikuti suara.
- Gerakan kepala terlihat kaku.
- Wajah tampak "bergetar" saat jaringan stabil.
- Pelaku cenderung menghindari gerakan yang terlalu banyak atau mematikan kamera dengan alasan koneksi buruk.

Kesimpulan

Deepfake tidak selalu bisa dikenali dari tampilannya. Karena itu, pertahanan terbaik bukan mata yang lebih tajam, melainkan kebiasaan untuk berpikir kritis, memverifikasi informasi, dan tidak terburu-buru mengambil keputusan

HSE PROGRAM		
	WEEKLY SAFETY TALK Periode : Juli 2026	

Dokumentasi :





** Pastikan semua pekerja untuk hadir dalam rapat, apabila tidak hadir mohon diberikan salinan notulen rapat.*

geOnet!	PT GEONET INFOMEDIA DAFTAR HADIR	No : 023.GI-HSE.ST Tanggal : 08 Juli 2026

SAFETY TALK

Hari/ Tgl : Rabu, 08 Juli 2026
Tempat : Ruang Teknis
Topic/Materi : **Awas Deepfake & AI Scam**
Pembicara : Bram

No	Nama	Jabatan/ Email	TTD	
1	NURDIN	HSE nurdin@geonet.co.id	1)	
2	M. Chairul. Fajri	Dev mfajri@geonet.co.id		2)
3	Mulyadi	Staff Finance	3)	
4	Randy Septian	Admin rseptian@geonet.co.id		4)
5	Jasmika Firdaus	Leader support jfirdaus@geonet.co.id	5)	
6	ISMAIL	Admin ismail@geonet.co.id		6)
7	RISKY FAHREZA	DEV rfahreza@geonet.co.id	7)	
8	Taris Fathur Rachman	Dev Lead trachman@geonet.co.id		8)
9	Jeri Giovahni	supporting	9)	
10	Nur Fadiah Apriani	Finance n.fadiah@geonet.co.id		10)
11	Agustina Dewi	Finance Manager adewi@geonet.co.id	11)	
12	Dede Kusfiana	Finance staff dkusfiana@geonet.co.id		12)
13	Dikky Pradana	Dev manager dpradana@geonet	13)	
14	[illegible]	M. [illegible] [illegible]@gmail.co.id		14)
15	Fahmuddin Sidqi	sidqifahmuddin@gmail.com	15)	
16	Prasiska Wulandari	PS [illegible]@geonet.co.id		16)
17	Silka Suci Yunivilda	HSE Intern silkasvilda@gmail.com	17)	

geOnet!	PT GEONET INFOMEDIA DAFTAR HADIR	No : 023.GI-HSE.ST Tanggal : 08 Juli 2026

No	Nama	Jabatan/ email	TTD	
18	Rian Budi Setiawan	Mgr. rbsetiawan@geonet.co.id	18)	
19	Ahmad Fobari	HRD abobari@geonet.co.id		19)
20	Altanesa Nabilla Zahrani	GIS Engineer anabilla@geonet.co.id	20)	
21	firdaus	Teknik Support firdaus@geonet.co.id		21)
22	UMAR ABDURROHMAN	RND Uabdurrohman@geonet.co.id	22)	
23	Lukman Hakim	Sales lhakim@geonet.co.id		23)
24	Dwinanda Mutiara	Sales dmutiara@geonet.co.id	24)	
25	Salsabila Fatehat	Sales sfatehat@geonet.co.id		25)
26	Bram Yudha P.	bypramoso@geonet.co.id	26)	
27				27)
28			28)	
29				29)
30			30)	
31				31)
32			32)	
33				33)
34			34)	

Penanggung Jawab

(HSE Manager)