PODCAST

SECURITY AWARENESS

Cyber Security & Human Risk

Memahami Peran Manusia dalam

Ketahanan Digital

PODCAST

Agenda

01 **Pendahuluan & Konteks Ancaman**

Statistik, lanskap ancaman, kenapa ini penting

02 **Lanskap Ancaman Modern**

Tipologi serangan, studi kasus Indonesia

03 **Konsep Social Engineering**

Ketika penyerang tidak menyerang sistem — mereka menyerang manusianya.

04 **Program Awareness**

Teknologi bisa dibeli. Tapi budaya keamanan harus dibangun

05 **Q & A**

Tanya Jawab

01

Pendahuluan & Konteks Ancaman

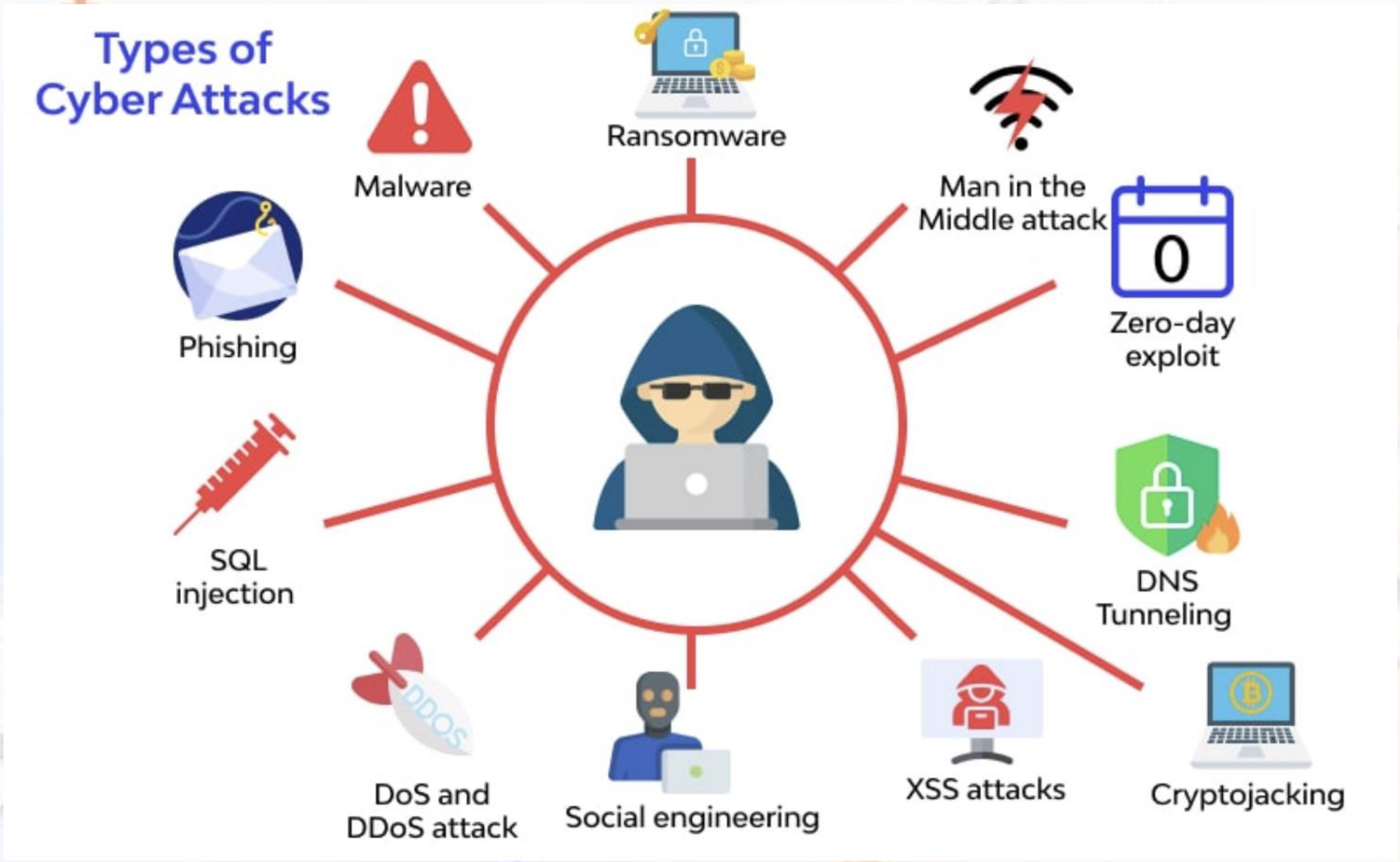
Mengapa keamanan siber adalah prioritas nasional


LIVE
www

MOTIVASI CYBER THREATS

1. SPIONASE
2. PROFIT
3. POLITIK
4. SABOTASE
5. PEMERASAN
6. FUN / SHOWOFF
7. BALAS DENDAM

Types of Cyber Attacks



TRIANGLE CIA

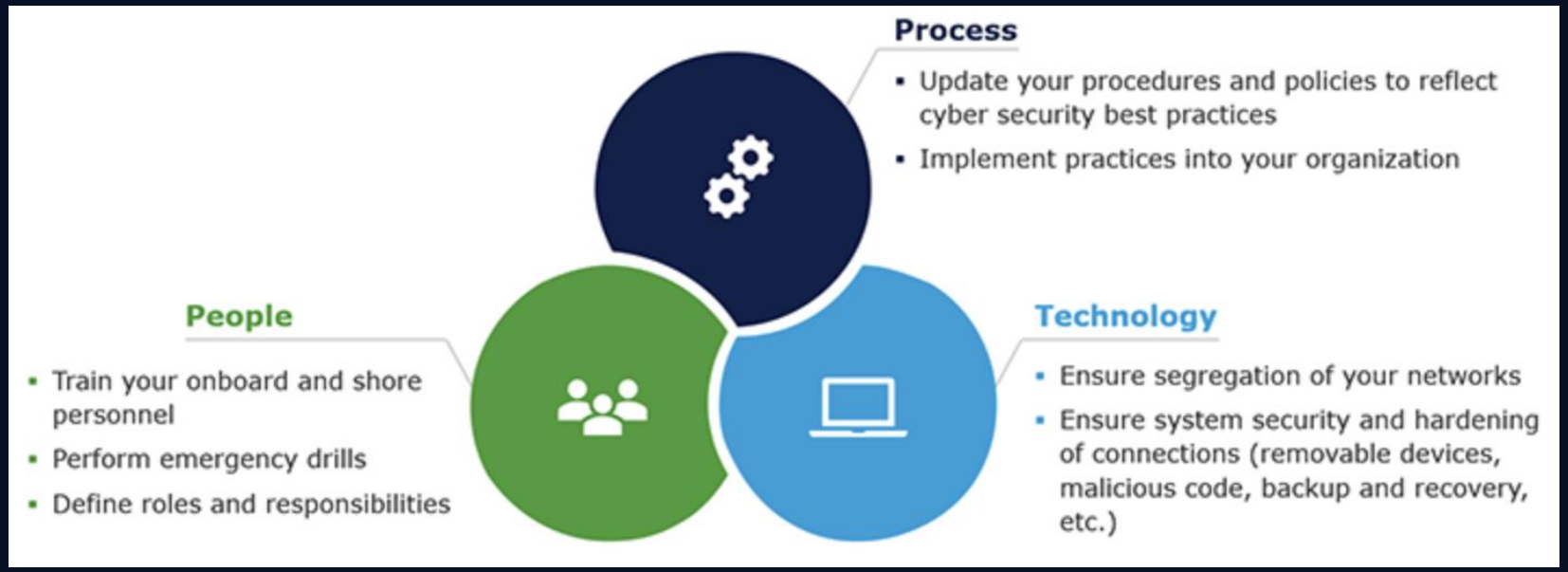
Pilar Dasar Keamanan Siber | CIA

CONFIDENTIAL

INTIGRITY

AVAILABILITY

Aspek Pengamanan

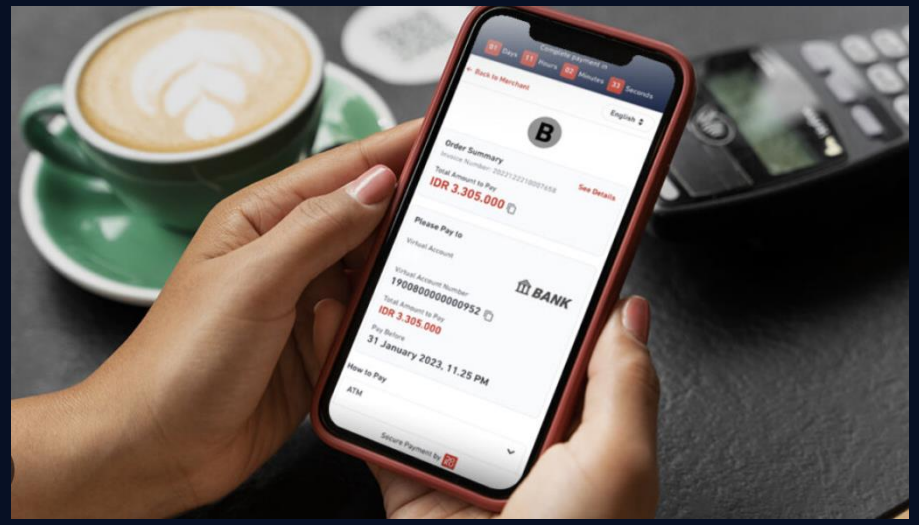


https://www.dnv.com/maritime/insights/topics/maritime-cybersecurity/owners-and-managers/

Evolusi Bisnis

https://www.liputan6.com/citizen6/read/6209587/7-ide-usaha-untuk-jualan-di-pasar-tradisional-yang-tetap-laris-meski-persaingan-ketat#

- Toko Fisik
- Data Manual
- Risiko Pencurian Fisik



https://www.paper.id/blog/pembayaran-digital/bayar-gampang-dengan-payment-link/

- E-Commerce
- Fintech
- SaaS
- Cloud
- Digital Payment

Data = Aset Digital Berharga

Big Data Analytics

Perusahaan mengolah data menjadi produk atau layanan informasi.

Target Marketing

Data membuat iklan tidak "nyasar". Apa yang Anda suka, kapan Anda butuh, dan berapa harga yang sanggup Anda bayar.

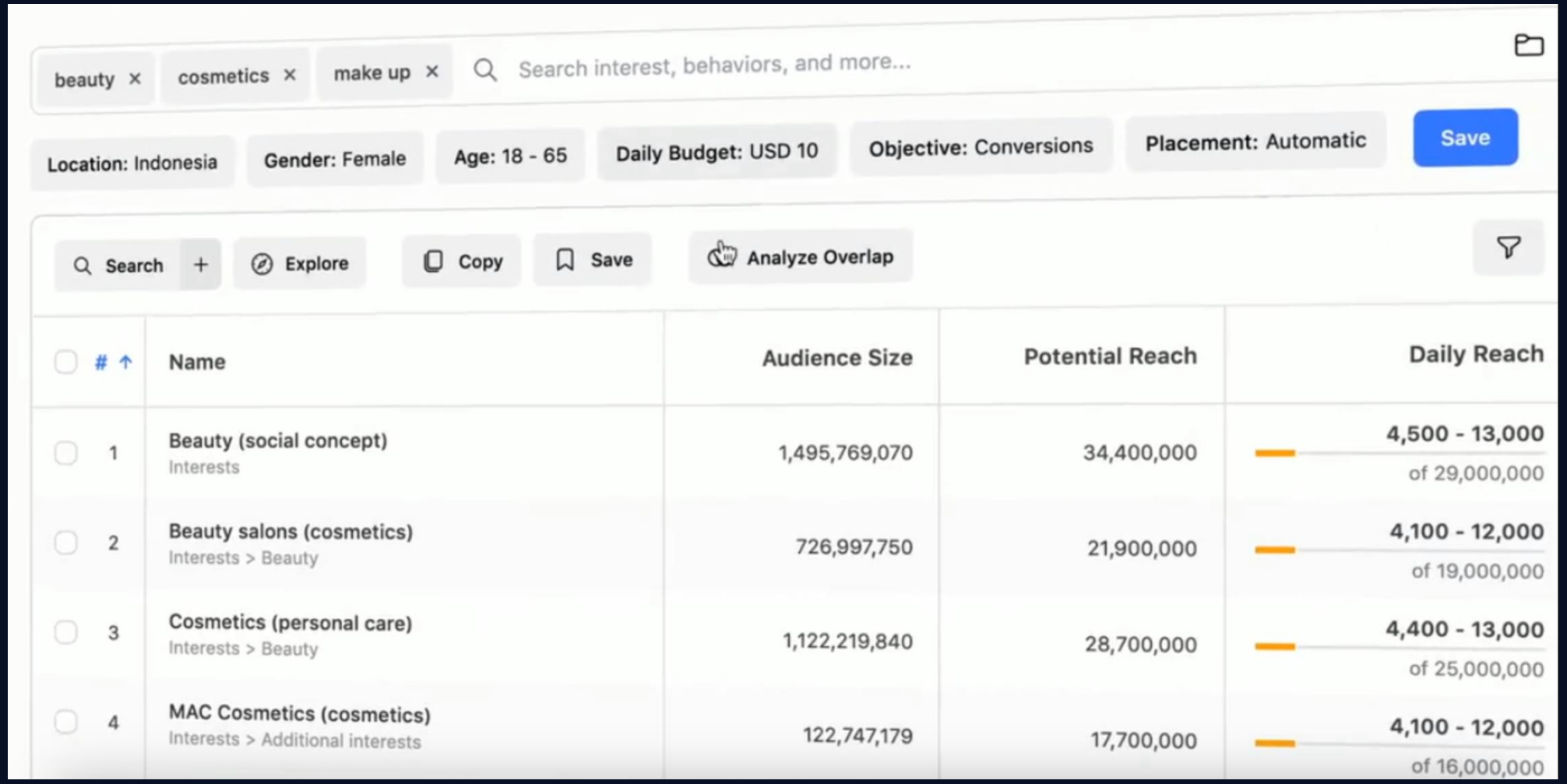
Aset Strategis

Data memberitahu mereka kapan perusahaan harus ekspansi

Nilai Valuasi

Investor menilai *organisasi* bukan dari berapa banyak laptop atau kantor yang mereka punya, tapi seberapa banyak dan seberapa aktif data pengguna yang mereka miliki.

Peran Data Dalam Dunia Bisnis



https://adsumo.co/blog/cara-targeting-broad-audience-di-facebook-ads-ampuh/

Peran Data Dalam Dunia Bisnis (2)

Data = Aset Digital Berharga

Data Collection (Pengumpulan Data)	Platform mengumpulkan: Data yang Anda berikan (nama, email), Data aktivitas (like, klik, search), Data perangkat (IP, lokasi, device)
Data Usage (Penggunaan Data)	Digunakan untuk: Personalisasi konten, Iklan (ads targeting), Rekomendasi, Pengembangan produk
Data Sharing (Berbagi Data)	Data bisa dibagikan ke: Partner bisnis, Advertiser, Vendor pihak ketiga “We may share data with trusted partners”
Data Retention (Penyimpanan Data)	Data disimpan selama diperlukan bahkan bisa tetap ada setelah akun dihapus (periode tertentu)

02

Lanskap Ancaman Modern

Kenali musuh: siapa, bagaimana, dan mengapa mereka menyerang

Studi kasus nyata dari Indonesia: BSI, PDNS, KPU, Kemhan, DPR RI

PEOPLE – PROCESS - TECHNOLOGY

Keamanan IT VS Keamanan Siber

Keamanan IT

Fokus internal sistem

Infrastruktur

Teknis

Keamanan Siber

Fokus ekosistem digital

Data, reputasi, rencana strategis & Bisnis

ANCAMAN NYATA

Indonesia dalam Angka

361 Juta+

Anomali trafik siber tahun 2023 (BSSN)

347

Dugaan insiden siber terdeteksi tahun 2023

186

Sektor pemerintah terdampak — tertinggi semua sektor

#3 Dunia

Indonesia negara paling banyak diserang siber (OJK)

Rp 6.3 T

Estimasi kerugian insiden PDNS 2024

134 Instansi

Terdeteksi bocor di darknet (2023)

282 Layanan

Publik terdampak insiden PDNS 2024

$34 Miliar

Kerugian ekonomi siber tertinggi di Asia

⚠ **Sektor administrasi pemerintahan menjadi sasaran UTAMA — 53% dari total insiden terdeteksi**

Sumber: BSSN, OJK, CISSReC

TIPOLOGI ANCAMAN

3 Kategori Utama yang Menyerang Pemerintah

RANSOMWARE-AS-A-SERVICE

Model bisnis kejahatan siber modern. Penyerang menyewa tool ransomware dan berbagi keuntungan.

- ✦ Enkripsi seluruh data organisasi dalam hitungan jam
- ✦ Tuntutan tebusan (BSI: data diancam bocor | PDNS: $8 juta USD)
- ✦ Varian terbaru: LockBit 3.0, Brain Cipher, BlackCat/ALPHV
- ✦ Target: backup data dihapus dulu sebelum enkripsi dimulai

ADVANCED PERSISTENT THREAT (APT)

Serangan panjang, tersembunyi, terencana. Biasanya disponsori negara atau aktor besar.

- ✦ Diam di jaringan berbulan-bulan tanpa terdeteksi
- ✦ Tujuan: spionase, pencurian data strategis, sabotase
- ✦ Kemhan (Nov 2023): 1.64 TB data dicuri, dijual di darknet
- ✦ Teknik: living-off-the-land, zero-day exploit, supply chain

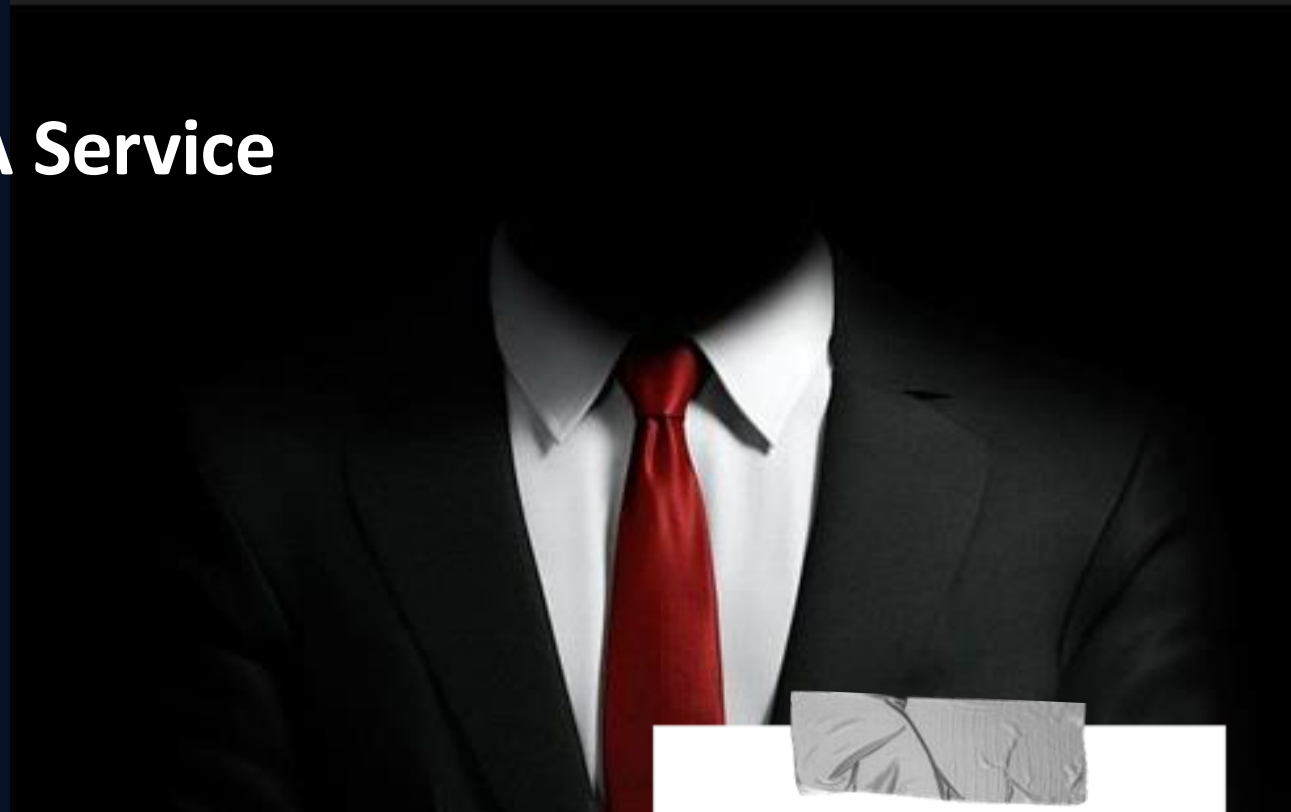
SOCIAL ENGINEERING & PHISHING

Manusia adalah titik terlemah. Penyerang memanipulasi orang, bukan sistem.

- ✦ Spear phishing: email sangat personal, menarget pejabat/IT
- ✦ Pretexting: penyerang berpura-pura jadi vendor/BSSN/Kominfo
- ✦ Credential stuffing: pakai kombinasi username-password bocor
- ✦ Insider threat: karyawan/kontraktor yang terbeli atau ceroboh

New Business Model: Criminal As A Service

"A professional, continuously evolving service-based criminal industry drives the innovation of tools and methods used by criminals and facilitates the digital underground through a multitude of complementary services, extending the attack capacity to those otherwise lacking the skills," states the iOCTA report. "Traditional organised crime groups (OCGs), including those with a mafia-style structure are beginning to use the service-based nature of the cyber crime market to carry or more sophisticated crimes [by] buying access to the skills they require."



Europol IOCTA (Internet Organized Crime Threat Assessment)

- https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web.pdf

Criminal As A Services

Spamming Service Prices

Offering	Price
Cheap email spamming service	US$10 per 1,000,000 emails
Expensive email spamming service using a customer database	US$50–500 per 50,000–1,000,000 emails
SMS spamming service	US$3–150 per 100–10,000 text messages
ICQ spamming service	US$3–20 per 50,000–1,000,000 messages
1-hour ICQ flooding service	US$2
24-hour ICQ flooding service	US$30
Email flooding service	US$3 for 1,000 emails
1-hour call flooding service (i.e., typically takes call center services down)	US$2–5
1-day call flooding service	US$20–50
1-week call flooding service	US$100
SMS flooding service	US$15 for 1,000 text messages
Vkontante.ru account database	US$5–10 for 500 accounts
Mail.ru address database	US$1.30–19.47 per 100–5,000 addresses
Yandex.ru address database	US$7–500 per 1,000–100,000 addresses
Skype SMS spamming tool	US$40
Email spamming and flooding tool	US$30

Distributed Denial-of-Service Service Prices

Offering	Price
1-day DDoS service	US$30–70
1-hour DDoS service	US$10
1-week DDoS service	US$150
1-month DDoS service	US$1,200

Table 5: DDoS service prices

Rootkit Prices

Offering	Price
Linux rootkit that replaces ls, find, grep, and other commands	US$500
Windows rootkit that operates at the driver level and that allows the download of specially assembled drivers	US$292

Exploit Prices

Offering	Price
Exploit bundle rental: 24 hours 1 week 1 month	 US$25 US$125 US$400
Styx Sploit Pack rental (affects Java and Adobe Acrobat and Flash Player)	US$3,000 per month
Eleonore Exploit Pack v. 1.6.2 (for Microsoft Data Access Components [MDAC], IEpeers, SnapShot, HCP, JDT, JWS, PDF collab,collectEmailInfo, PDF SING, and Java Invoke(chain) 1.5/1.6; average reach of 10–25%)	US$2,500–3,000
Phoenix Exploits Kit v. 2.3.12 (for Internet Explorer [IE] 6 MDAC, Java Deserialize, Java GSB, PDF Collab/Printf, Adobe Flash Player 9 and 10, IEpeers, Java SMB, HCP, PDF/SWF, PDF Open, and PDF Lib TIFF)	US$2,200 per domain
Less popular and less effective bundle	US$25+
XSS exploit for Mail.ru: Active XSS exploit Passive XSS exploit Passive XSS exploit for Rambler.ru and Yandex.ru XSS exploit for Gmail.com	 US$50–150 US$10–35 US$10–50 US$200
SQL exploit for a site with 50,000 visitors a day	US$100
Exploit bundle crypting service: 1-time 1-month subscription (5 times)	 US$50 US$150

https://resources.infosecinstitute.com/topic/cybercrime-and-the-underground-market/

STUDI KASUS

Insiden Siber Nyata di Indonesia

Mei 2023

BSI — Ransomware LockBit 3.0

- ATM & m-banking lumpuh 5+ hari
- Nasabah tidak bisa akses layanan
- Data nasabah diancam bocor

Pelajaran: Backup terisolasi & BCP

Juni 2024

PDNS — Brain Cipher Ransomware

- 282 layanan publik lumpuh
- Imigrasi bandara manual 4 hari
- Tebusan $8 juta, tidak dibayar, Dirjen mundur

Pelajaran: Tidak ada backup! Zero Trust

2023

KPU — Kebocoran Data Pemilu

- Data pemilih bocor ke forum hacker
- Bjorka mengklaim akses ke sistem
- Kepercayaan publik tergerus

Pelajaran: Enkripsi data at-rest & in-transit

Nov 2023

Kemhan — Data Theft 1.64 TB

- 1.64 TB data dicuri & dijual
- Dokumen rahasia ditawarkan di darknet
- APT Nation-State diduga terlibat

Pelajaran: Network segmentation & DLP

Sep 2023

DPR RI — YouTube Hack

- Kanal YouTube diretas, 2M+ subscriber hilang
- Konten judi online disiarkan langsung
- Google menonaktifkan sementara akun

Pelajaran: MFA wajib semua akun resmi

Sep 2024

NPWP — 6 Juta Data Bocor

- 6 juta data NPWP dijual di dark web
- Data pejabat tinggi termasuk terdampak
- DJP & Polri investigasi bersama

Pelajaran: Audit akses privileged secara berkala

03

Konsep Social Engineering

Ketika penyerang tidak menyerang sistem — mereka menyerang manusianya.

Apa Itu Social Engineering?

Social Engineering adalah seni memanipulasi psikologi manusia untuk mendapatkan informasi rahasia, akses sistem, atau mengubah perilaku seseorang — tanpa perlu meretas teknologi apapun.

Mengapa Berbahaya?

- Tidak butuh keahlian teknis — siapa pun bisa jadi korban
- Mengeksploitasi naluri manusia: kepercayaan, rasa takut, ingin membantu
- Antivirus & firewall TIDAK melindungi dari manipulasi psikologis
- 95% pelanggaran keamanan siber melibatkan faktor manusia (IBM)
- Biaya serangan rendah, dampak bisa sangat besar

Yang Dieksploitasi Penyerang

Kepercayaan	Kita cenderung percaya orang yang terlihat 'resmi'
Rasa Takut & Urgensi	Panik membuat kita tidak berpikir jernih
Keinginan Membantu	Orang baik mudah dimanfaatkan
Otoritas	Kita sulit menolak permintaan 'atasan'
Konsistensi	Setelah setuju hal kecil, susah menolak hal besar

🦻 *Ingat: Hacker terbaik tidak membobol sistem — mereka membobol manusia yang mengoperasikan sistem tersebut.*

6 Teknik Social Engineering yang Paling Umum — Kenali Sebelum Jadi Korban

Penyerang menggunakan berbagai metode berbeda. Kenali setiap tekniknya:

Phishing

Email/pesan palsu yang tampak asli, memancing korban klik link berbahaya atau isi formulir palsu. Contoh: email 'Bank Anda memblokir akun Anda, klik di sini!'

Vishing

Voice phishing — penipuan melalui telepon. Penyerang berpura-pura jadi IT support, bank, atau pejabat pajak untuk mendapatkan informasi sensitif.

Pretexting

Penyerang menciptakan skenario (pretext) palsu yang meyakinkan. Contoh: 'Saya dari tim HR, perlu verifikasi data KTP Anda untuk sistem baru.'

Baiting

Menjebak korban dengan umpan menarik. Contoh: flashdisk bertuliskan 'GAJI KARYAWAN 2024' ditinggalkan di parkiran — siapa yang tidak penasaran?

Quid Pro Quo

Menawarkan bantuan/hadiah sebagai tukar guling informasi. 'Saya akan bantu reset password Anda jika Anda berikan kode verifikasi SMS-nya.'

Tailgating

Masuk ke area terbatas secara fisik dengan mengikuti orang yang berwenang. Sering terjadi di gedung kantor yang tidak ketat SOP-nya.

Studi Kasus: Serangan Social Engineering di Dunia Nyata

Ini bukan film — ini kejadian sungguhan yang merugikan miliaran dolar:

Twitter

2020

Vishing + Pretexting

130 akun selebriti & tokoh dunia dibobol — Obama, Elon Musk, Bill Gates

📌 Hacker menelepon karyawan Twitter, berpura-pura jadi tim IT internal. Karyawan percaya dan memberikan akses ke sistem admin internal.

🩹 Dampak: 130 akun terverifikasi diambil alih, dipakai untuk penipuan Bitcoin senilai $120.000 dalam hitungan jam.

💡 **Serangan ini 100% social engineering — bukan exploit teknis. Satu karyawan yang tertipu cukup untuk menghancurkan platform global.**

Toyota Boshoku

2019

Phishing (BEC)

Karyawan keuangan mentransfer Rp 700 miliar karena email palsu 'dari atasan'

📌 Penyerang mengirim email yang sangat meyakinkan seolah-olah dari eksekutif Toyota, meminta transfer dana mendesak ke rekening asing untuk 'keperluan bisnis rahasia'.

🩹 Dampak: Rp 700 miliar (sekitar $37 juta USD) raib sebelum penipuan terdeteksi.

💡 **Business Email Compromise (BEC) — variasi social engineering yang menyasar karyawan keuangan dengan urgensi palsu dari 'atasan'.**

Kedua kasus ini BUKAN karena sistem keamanan yang lemah — tapi karena manusia yang tertipu

Siklus Serangan Social Engineering — Bagaimana Penyerang Bekerja

Serangan tidak terjadi sembarangan — penyerang mengikuti siklus yang terencana:

1

Reconnaissance — Pengintaian

Penyerang mengumpulkan informasi target: nama, jabatan, kolega, kebiasaan, dari LinkedIn, Instagram, website perusahaan.

2

Establishing Trust — Membangun Kepercayaan

Penyerang menciptakan identitas palsu yang meyakinkan — berpura-pura jadi vendor, IT support, atau rekan kerja baru.

3

Exploitation — Eksekusi Manipulasi

Menggunakan teknik psikologis (urgensi, otoritas, rasa takut) untuk mendapatkan informasi atau akses yang diinginkan.

4

Exit — Menghilang Tanpa Jejak

Setelah berhasil, penyerang menutup jalur komunikasi dan menghapus jejak. Korban sering tidak sadar telah ditipu hingga kerusakan terjadi.

Red Flags — Tanda Peringatan

- Permintaan mendadak & sangat mendesak
- Meminta password / OTP / PIN
- Pengirim email tidak dikenal dengan domain aneh
- Tawaran yang terlalu bagus untuk jadi kenyataan
- Tekanan untuk bertindak SEKARANG tanpa pikir panjang
- Permintaan melangkahi prosedur normal
- Identitas pengirim sulit diverifikasi

Pertahanan terbaik: BERHENTI, PIKIR, VERIFIKASI. Jangan pernah bertindak karena tekanan atau kepanikan.

04

Program Awareness

Teknologi bisa dibeli. Tapi budaya keamanan harus dibangun

Fakta yang harus Anda tahu:

95%

Pelanggaran keamanan siber melibatkan kesalahan manusia (IBM, 2023)

$10.9 M

Biaya pelanggaran data rata-rata untuk sektor kesehatan — tertinggi 13 tahun berturut

82%

Pelanggaran yang melibatkan social engineering atau phishing dapat dicegah dengan awareness yang baik

Kesimpulan: Satu sesi pelatihan saja bisa mengurangi risiko phishing hingga 70% (Proofpoint, 2023)

5 Pilar Program Security Awareness yang Efektif

Program awareness yang berhasil harus lebih dari sekedar membagikan poster 'Jangan Klik Link Mencurigakan':

01 Edukasi Berkelanjutan

Bukan pelatihan sekali setahun lalu dilupakan. Program yang efektif menggunakan micro-learning: konten pendek (5-10 menit) yang disampaikan rutin setiap bulan dengan topik relevan. Contoh: Newsletter bulanan, video animasi pendek, tips keamanan di screensaver kantor.

02 Simulasi Serangan Nyata

Kirim email phishing simulasi ke karyawan tanpa mereka tahu. Ukur berapa persen yang klik link. Karyawan yang 'gagal' mendapat pelatihan tambahan — bukan hukuman. Tools: KnowBe4, Proofpoint, GoPhish (gratis). Frekuensi ideal: setiap 2-3 bulan.

03 Kebijakan yang Jelas & Masuk Akal

Tulis kebijakan keamanan dengan bahasa yang mudah dipahami semua level karyawan — bukan dokumen teknis yang tidak dibaca siapapun. Kebijakan yang terlalu rumit akan diabaikan. Contoh: Kebijakan 1 halaman tentang 'Apa yang boleh dan tidak boleh di WiFi kantor'.

04 Budaya 'Speak Up'

Ciptakan lingkungan di mana karyawan TIDAK takut melaporkan kesalahan atau insiden keamanan. Budaya menyalahkan membuat orang menyembunyikan masalah hingga terlambat. Contoh: Hotline pelaporan anonim, sesi 'Lessons Learned' tanpa menyebut nama, apresiasi untuk yang melapor.

05 Pengukuran & Evaluasi

Program awareness tanpa pengukuran adalah harapan buta. Ukur: persentase klik phishing, jumlah laporan insiden, skor kuis pelatihan, dan tren dari waktu ke waktu. KPI: Click rate phishing < 5%, 100% karyawan selesaikan pelatihan tahunan, response time laporan < 1 jam.

Roadmap Implementasi Program Awareness — Dari Nol ke Budaya Keamanan

Bagaimana cara memulai? Ikuti roadmap 12 bulan ini untuk membangun program awareness dari nol:

Bulan 1-2

Assessment & Baseline

- Ukur tingkat kesadaran awal karyawan (kuis/survey)
- Lakukan simulasi phishing pertama — catat click rate
- Identifikasi kelompok karyawan berisiko tinggi
- Tetapkan KPI dan target yang ingin dicapai

Bulan 3-5

Edukasi & Pelatihan

- Luncurkan program pelatihan (online/offline)
- Mulai sesi micro-learning bulanan
- Workshop khusus untuk departemen IT & keuangan
- Distribusikan kebijakan keamanan yang baru

Bulan 6-9

Simulasi & Penguatan

- Ulangi simulasi phishing — bandingkan dengan baseline
- Berikan coaching personal untuk yang masih rentan
- Luncurkan kompetisi/gamifikasi keamanan internal
- Evaluasi dan perbarui materi pelatihan

Bulan 10-12

Evaluasi & Budaya

- Ukur KPI akhir — bandingkan dengan target awal
- Rayakan pencapaian tim secara publik
- Integrasikan keamanan ke dalam proses onboarding
- Rencanakan siklus program untuk tahun berikutnya

📈 *Hasil nyata: Perusahaan dengan program awareness terstruktur rata-rata mengurangi insiden keamanan hingga 70% dalam 12 bulan.*

Contoh Materi Awareness yang Relevan untuk Karyawan & UMKM

Materi terbaik adalah yang langsung relevan dengan pekerjaan sehari-hari karyawan:

Password & Autentikasi

- Gunakan password manager (bukan Excel!)
- Aktifkan 2FA di semua akun penting
- Password minimal 12 karakter, campuran
- Jangan pakai ulang password di banyak akun

Email & Phishing

- Cek domain pengirim dengan teliti
- Hover link sebelum klik untuk lihat URL aslinya
- Jangan download lampiran yang tidak diminta
- Verifikasi permintaan transfer via telepon

Work From Home Safety

- Gunakan VPN kantor saat kerja remote
- Jangan bekerja di WiFi publik tanpa VPN
- Kunci layar saat meninggalkan perangkat
- Pisahkan perangkat kerja dan personal

Penggunaan Media Sosial

- Jangan posting info internal di medsos
- Waspadai permintaan koneksi dari orang asing
- LinkedIn bisa digunakan untuk reconnaissance
- Informasi 'kecil' bisa sangat berguna bagi penyerang

Insiden & Pelaporan

- Laporkan email mencurigakan ke IT segera
- Jangan malu akui kesalahan — lebih baik cepat lapor
- Tahu nomor darurat IT / Security team
- Dokumentasi kejadian sebelum menghapus apapun

Kebersihan Digital

- Update software secara rutin
- Hapus data yang tidak diperlukan lagi
- Gunakan perangkat kantor hanya untuk kerja
- Enkripsi file sensitif sebelum dikirim

5 Hal yang Harus Anda Ingat Seumur Hidup

01

Manusia adalah target utama

95% serangan siber mengeksploitasi kelemahan manusia — bukan teknologi. Firewall tercanggih tidak berguna jika karyawan memberikan passwordnya.

02

Social Engineering mengeksploitasi psikologi

Penyerang memanfaatkan kepercayaan, rasa takut, keinginan membantu, dan rasa hormat kepada otoritas. Kesadaran adalah pertahanan pertama.

03

Ancaman bisa datang dari dalam

Insider threat — baik yang sengaja maupun ceroboh — adalah salah satu risiko terbesar. Desain akses yang ketat dan monitoring adalah kuncinya.

04

Awareness adalah investasi, bukan biaya

Program awareness yang efektif bisa mengurangi insiden hingga 70%. Jauh lebih murah dari biaya rata-rata kebocoran data ($4,45 juta).

05

Budaya lebih kuat dari kebijakan

Aturan bisa diabaikan, teknologi bisa dikalahkan — tapi budaya yang tepat membuat setiap karyawan menjadi benteng pertahanan yang aktif.

Framework STOP-THINK-VERIFY — Panduan Praktis Sebelum Klik atau Bertindak

Tiga detik yang bisa menyelamatkan bisnis jutaan rupiah:

✋ STOP

Berhenti Sejenak

- Ada rasa urgensi berlebihan?
- Permintaan tidak biasa dari orang 'dikenal'?
- Ada tekanan untuk bertindak SEKARANG?
- Merasa tidak enak untuk menolak?

💡 ***Jika satu pun jawabannya YA, jangan lanjutkan dulu.***

🧠 THINK

Pikir Secara Kritis

- Apakah permintaan ini masuk akal?
- Apakah saya pernah diminta hal serupa?
- Apa kerugian jika saya menolak/menunda?
- Adakah cara lain membantu tanpa risiko?

💡 ***Orang/sistem yang sah tidak akan marah jika Anda memverifikasi.***

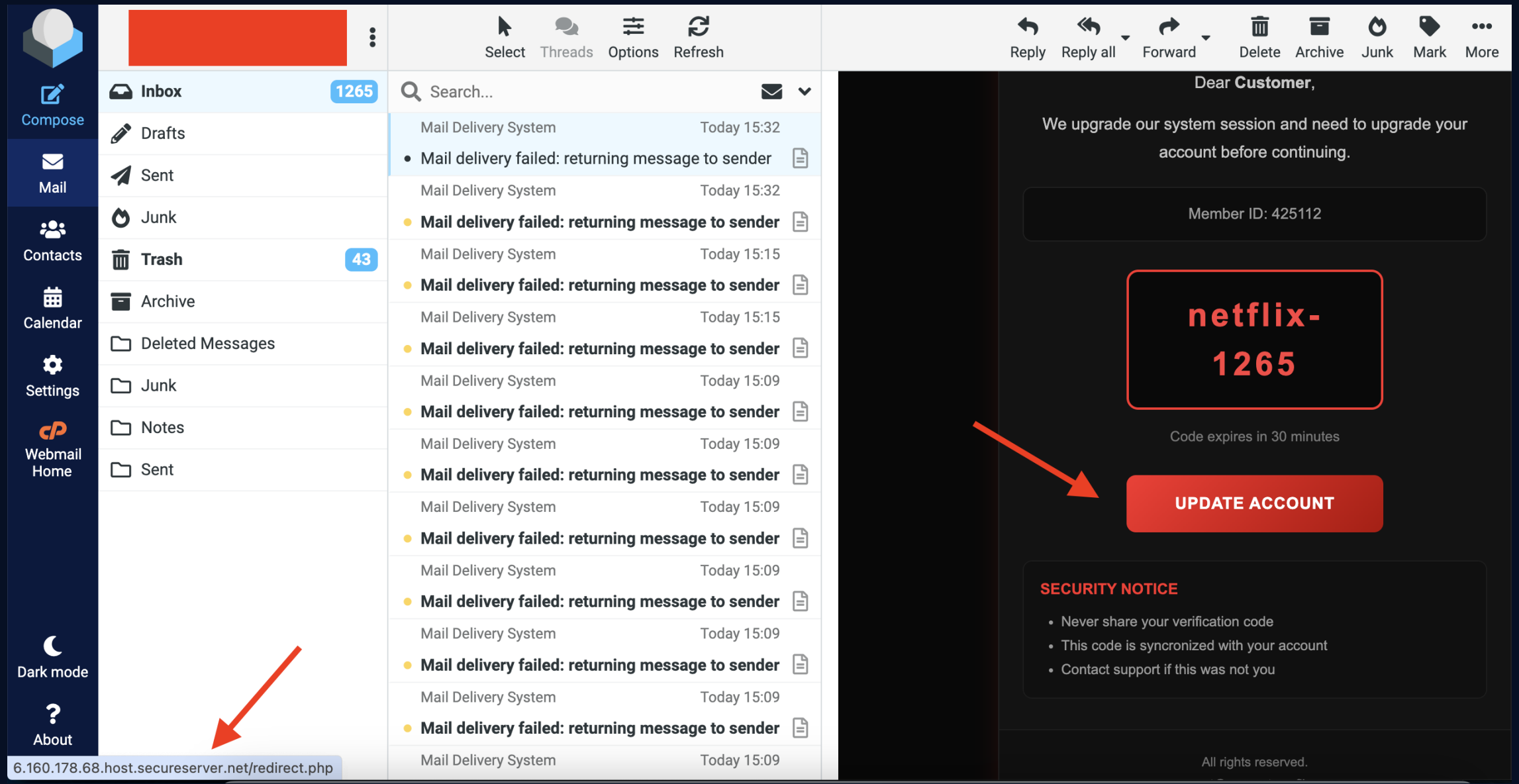
🔍 VERIFY

Verifikasi Independen

- Hubungi pengirim via nomor/email RESMI (bukan dari pesan itu)
- Tanya rekan atau atasan sebelum bertindak
- Cek domain email pengirim dengan teliti
- Gunakan saluran komunikasi berbeda untuk konfirmasi

💡 ***Verifikasi bukan tanda tidak percaya — tapi standar profesional.***

Ingat: Memverifikasi bukan lambat — itu PROFESIONAL. Penyerang mengincar orang yang terburu-buru.


Compose
Mail
Contacts
Calendar
Settings
Webmail Home
Dark mode
About
Select
Threads
Options
Refresh
Inbox 1265
Drafts
Sent
Junk
Trash 43
Archive
Deleted Messages
Junk
Notes
Sent
Search...
Mail Delivery System Today 15:32
Mail delivery failed: returning message to sender
Mail Delivery System Today 15:32
Mail delivery failed: returning message to sender
Mail Delivery System Today 15:15
Mail delivery failed: returning message to sender
Mail Delivery System Today 15:15
Mail delivery failed: returning message to sender
Mail Delivery System Today 15:09
Mail delivery failed: returning message to sender
Mail Delivery System Today 15:09
Mail delivery failed: returning message to sender
Mail Delivery System Today 15:09
Mail delivery failed: returning message to sender
Mail Delivery System Today 15:09
Mail delivery failed: returning message to sender
Mail Delivery System Today 15:09
Mail delivery failed: returning message to sender
Mail Delivery System Today 15:09
Reply
Reply all
Forward
Delete
Archive
Junk
Mark
More
Dear Customer,
We upgrade our system session and need to upgrade your account before continuing.
Member ID: 425112
netflix-1265
Code expires in 30 minutes
UPDATE ACCOUNT
SECURITY NOTICE
Never share your verification code
This code is syncronized with your account
Contact support if this was not you
All rights reserved.
6.160.178.68.host.secureserver.net/redirect.php

KONSEP PENTING:

"Never Trust, Always Verify"

— Prinsip Zero Trust dalam Keamanan Siber

💻 Untuk Teknologi

Sistem tidak otomatis mempercayai perangkat atau pengguna — bahkan yang ada di dalam jaringan internal. Setiap akses harus diverifikasi ulang.

👦 Untuk Manusia

Jangan otomatis percaya identitas seseorang hanya karena mereka tahu nama atasan Anda atau terdengar meyakinkan. Verifikasi selalu via jalur resmi.

🏢 Untuk Bisnis

Terapkan 'least privilege' secara ketat. Batasi akses, audit secara rutin, dan anggap semua permintaan tidak biasa sebagai potensi ancaman.

Zero Trust bukan berarti tidak percaya siapapun secara personal — ini sistem yang dirancang meminimalisir asumsi 'aman' yang berbahaya.

Checklist Harian Keamanan Siber — Untuk Setiap Karyawan Bisnis Digital

Keamanan siber bukan event tahunan — ini kebiasaan harian. Tempelkan di meja kerja Anda:

🌞 Pagi — Sebelum Mulai Kerja

- [ ] Pastikan perangkat sudah di-update (OS & antivirus)
- [ ] Login hanya ke akun kerja resmi — bukan akun personal
- [ ] Aktifkan VPN jika bekerja remote atau di luar kantor
- [ ] Periksa email dengan teliti sebelum klik apapun

💼 Siang — Saat Aktif Bekerja

- [ ] Kunci layar setiap kali meninggalkan meja
- [ ] Jangan buka lampiran email yang tidak diharapkan
- [ ] Verifikasi permintaan transfer/data via telepon langsung
- [ ] Jangan gunakan WiFi publik tanpa VPN untuk data sensitif

🌙 Sore — Sebelum Selesai Kerja

- [ ] Log out dari semua akun dan sistem kerja
- [ ] Simpan dokumen sensitif di tempat yang dienkripsi
- [ ] Laporkan email mencurigakan yang diterima hari ini
- [ ] Kunci atau matikan perangkat — jangan hanya sleep

Aturan Emas: Jika ragu — JANGAN klik. Tanya dulu, klik kemudian. Satu klik yang salah bisa merugikan seluruh perusahaan.

Q & A

"Dalam keamanan siber, teknologi adalah tembok — tapi manusia adalah gerbangnya.

Pastikan gerbang Anda selalu waspada."