UNIVERSITAS AMIKOM YOGYAKARTA
Creative Economy Park

MATA KULIAH CYBER SECURITY

Program Studi Magister Informatika

Universitas AMIKOM Yogyakarta
Tahun 2025

Creative Economy Park

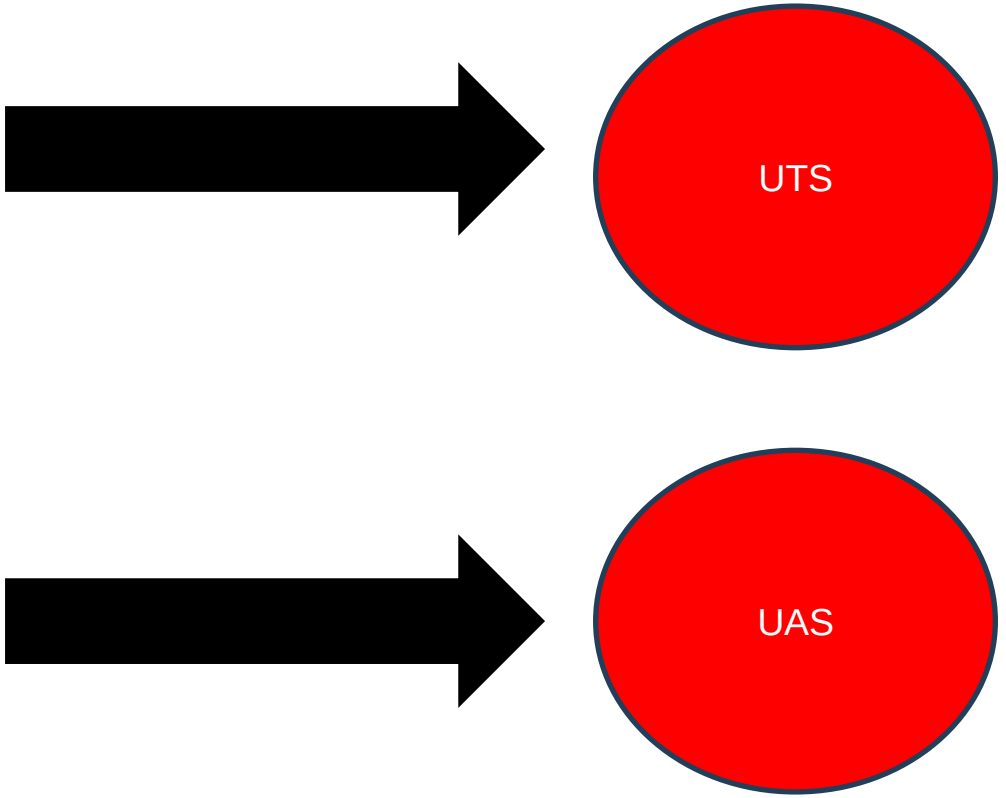
Dr. Ir. Yoga Sahria, S.Kom., M.Kom.

Fakultas Ilmu Komputer

Universitas AMIKOM Yogyakarta
Jln RingRoad Utara, Depok, Condongcatur
Yogyakarta

Outline Mata Kuliah Selama 1 Semester

1. Ruang lingkup keamanan cyber menurut framework Cyber Security Body of Knowledge (CyBoK)
2. Serangan infrastruktur jaringan
3. Malware
4. Serangan aplikasi desktop dan web
5. Social engineering
6. Solusi pengamanan data dan sistem modern
7. Regulasi dan kebijakan cyber law di Indonesia
8. Implementasi kebijakan keamanan TI
9. Penetration testing
10. Digital Forensic



UNIVERSITAS AMIKOM YOGYAKARTA
Creative Economy Park

Social Engineering

PERTEMUAN 4

Universitas AMIKOM Yogyakarta
Tahun 2025

Creative Economy Park

Dr. Ir. Yoga Sahria, S.Kom., M.Kom.

Fakultas Ilmu Komputer

Universitas AMIKOM Yogyakarta
Jln RingRoad Utara, Depok, Condongcatur
Yogyakarta

Social Engineering Attacks Cyber Security

Minggu 4

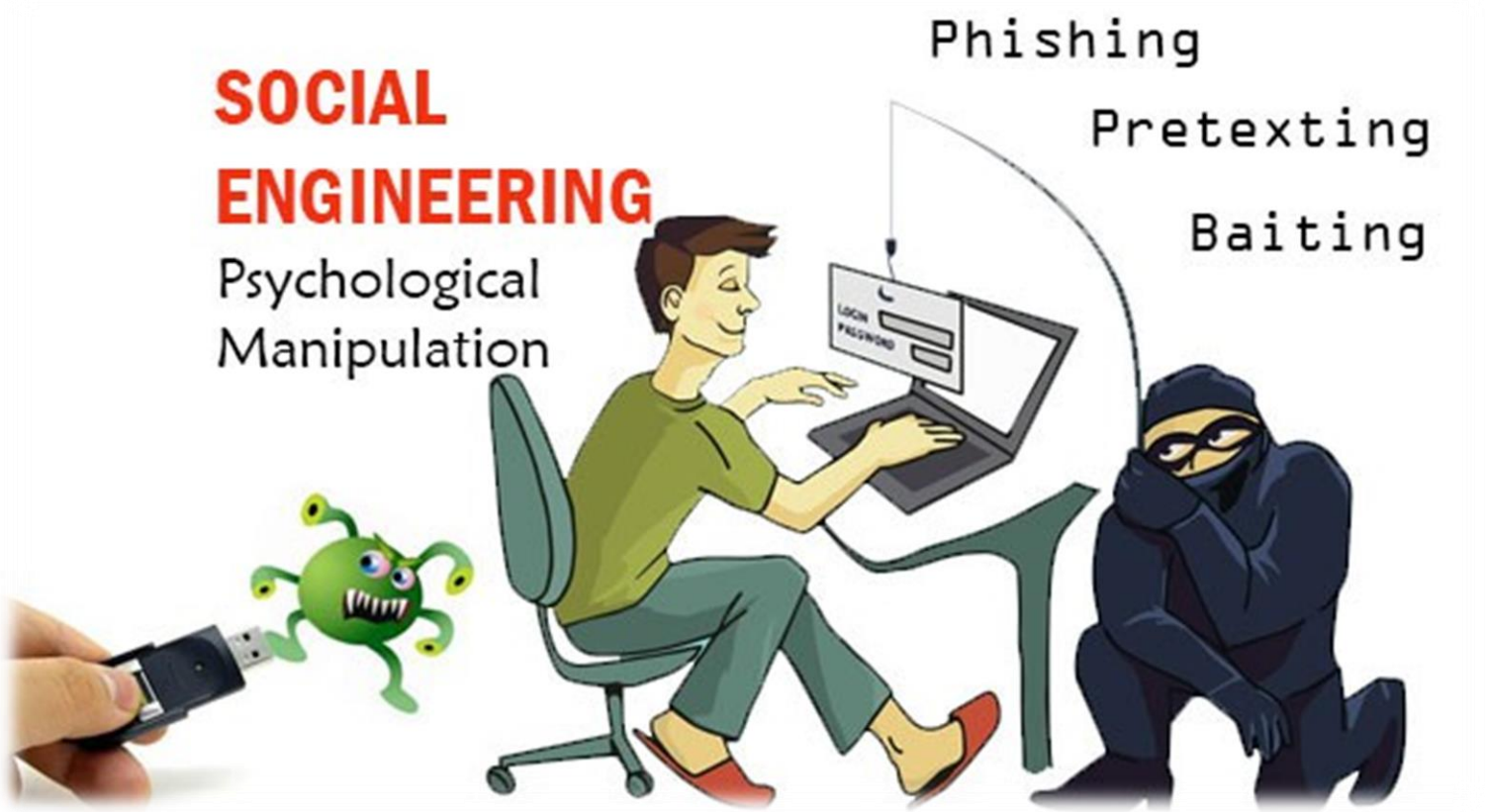
Dr. Ir. Yoga Sahria, S.Kom., M.Kom.

Outline Pembelajaran

1. Tujuan dan teknik social engineering
2. Framework social engineering
3. Skenario dan antisipasi Social Engineering

Tujuan *Social Engineering*

- ***Social Engineering*** adalah metode manipulasi psikologis yang digunakan oleh penyerang untuk mendapatkan informasi rahasia atau akses ke sistem tanpa melalui jalur teknis.



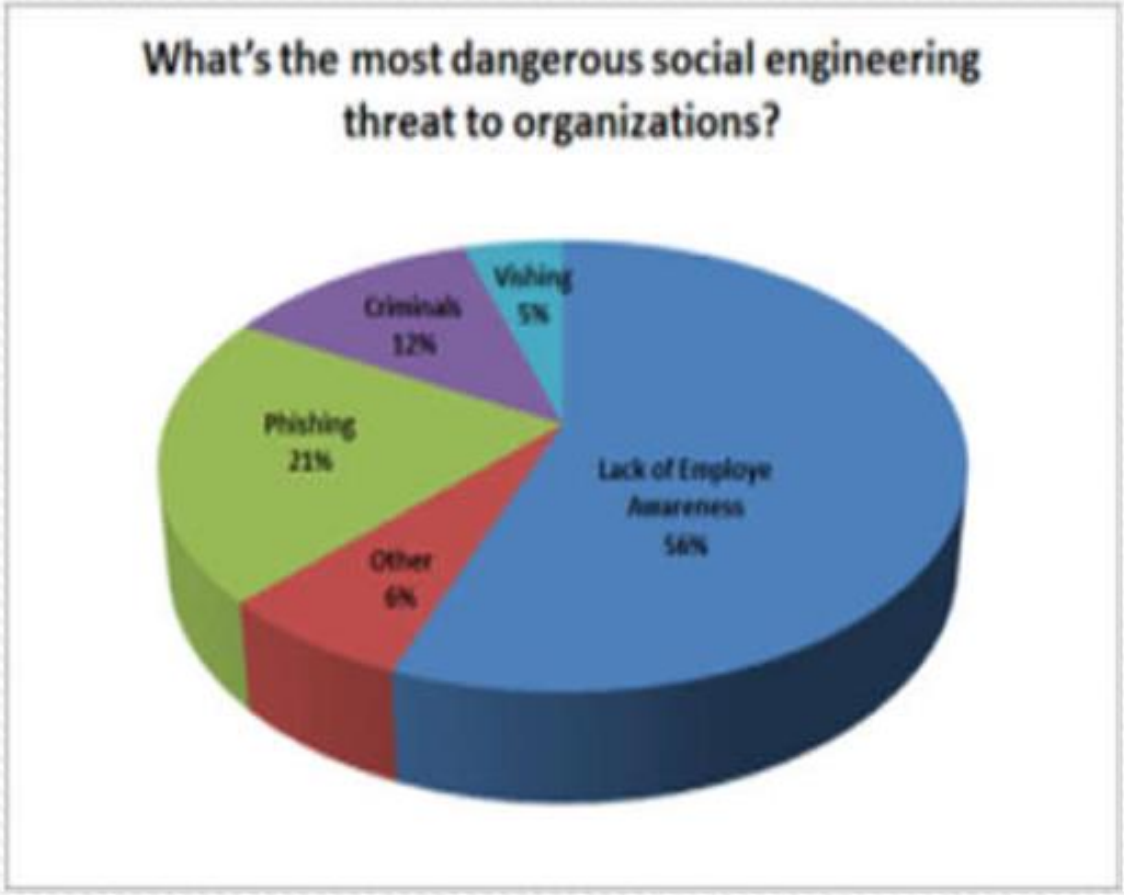
Faktor Psikologis Manusia

- According to www.terranovasecurity.com, Social Engineering relies on these five basic emotional traits for its success, including:

Social Engineering "MOTIVIATIONS"	How it Affects People that Fall for these Social Engineering Techniques
FEAR	Example: You receive a voice mail that you're under investigation for tax fraud and you must call and pay an immediate fee to the "IRS"
GREED	Example: Someone convinces you that a mere $10.00 investment will pocket you $10,000 or more
CURIOUSITY	Example: Cybercriminals convince you that some event you see on the news affects you and they have evidence that they send you for review and it is in fact Malware
HELPFULNESS	Example: Playing on the basic desire of humans to trust and help one another – collecting charity and donations for a false cause
URGENCY	Example: You receive a fake or spoofed email from a vendor you use indicating that they need to confirm your credit card information ASAP

Pengertian Social Engineering

Social engineering adalah kegiatan untuk mendapatkan informasi rahasia/penting dengan cara menipu pemilik informasi tersebut (targeted) umumnya dilakukan melalui telepon dan Internet dengan pendekatan yang manusiawi melalui mekanisme interaksi sosial.



Social engineering

- **Social engineering** adalah teknik manipulasi psikologis yang digunakan oleh penyerang untuk mengeksploitasi kelemahan manusia, seperti **ketakutan, keserakahan, rasa ingin tahu, kepercayaan, urgensi, dan rasa kasihan**, dengan tujuan memperoleh informasi sensitif atau akses tanpa menggunakan serangan teknis langsung.
- Penyerang memanfaatkan faktor-faktor ini untuk mendorong korban bertindak cepat atau memberikan informasi tanpa berpikir kritis. Faktor psikologis ini membuat manusia rentan terhadap berbagai bentuk serangan, **seperti phishing, pretexting, dan baiting**, yang jika berhasil, dapat membahayakan keamanan data atau sistem.

Tips menghindar ancaman social engineering

1. Tanyakan **nama dan identitas** (verifikasi)
2. Tanyakan mengapa memerlukan **informasi**
3. Tanyakan siapa yang **mengautorisasi** permintaan informasi

Target social engineering

Serangan Social Engineering

Siapa yang Anda percayai? >>> Nobody

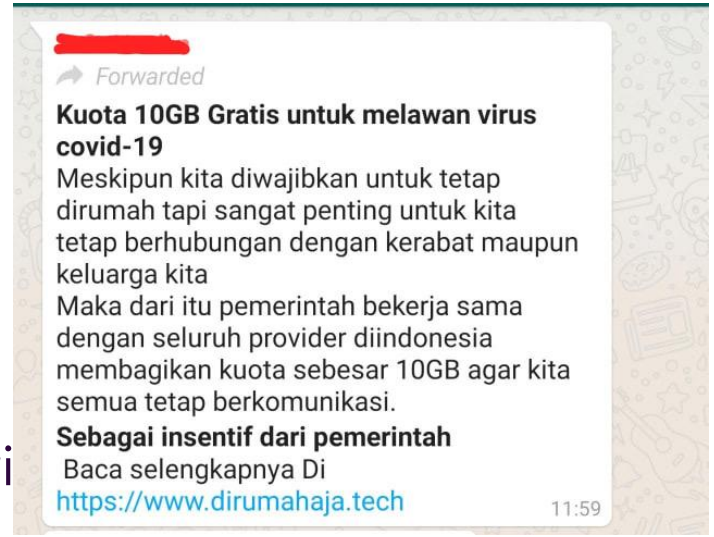
- ***Everyone will be a victim, so that everyone could be a suspect***
- Semua orang akan menjadi korban, sehingga semua orang bisa menjadi tersangka

Tujuan

- **Mengambil data pribadi atau organisasi,** seperti kredensial login, informasi keuangan, atau informasi sensitif lainnya.
- **Mengakses sistem atau jaringan tanpa izin**, seperti melalui manipulasi karyawan untuk memberikan akses.
- **Menyebarkan malware atau serangan siber lainnya,** dengan membujuk korban untuk mengunduh file atau link berbahaya.
- **Menghancurkan reputasi atau kepercayaan,** terutama jika data sensitif perusahaan bocor.

Teknik Social Engineering

- **Phishing** Salah satu serangan rekayasa sosial yang paling sering terjadi. Mengirim email atau pesan teks yang berpura-pura menjadi bisnis asli dalam upaya untuk menipu penerima agar mengungkapkan informasi pribadi.
- **Spear Phishing** Mirip dengan phishing tetapi secara eksplisit menargetkan individu atau kelompok. Email yang dikirim ke korban berisi tautan dan lampiran untuk menyebarkan malware, mencuri data, dan meningkatkan hak istimewa dalam sistem.
- **Whaling (Penipuan CEO)** Whaling terjadi ketika penyerang mencoba menipu CEO, CFO, atau eksekutif berpangkat tinggi lainnya agar memberikan informasi penting seperti nomor kartu kredit atau kredensial login menggunakan email atau halaman web dengan teks palsu.
- **Baiting** Ini adalah jenis serangan rekayasa sosial khusus yang melibatkan penempatan malware (virus, worm, atau Trojan horse) pada drive yang dapat dilepas seperti stik USB.



Teknik Social Engineering

- **Vishing (Voice Phishing)** Vishing adalah serangan yang menggunakan teknologi suara dan pesan untuk mengelabui Anda agar memberikan informasi pribadi.
- **Serangan Smishing** Ini adalah jenis penipuan phishing yang menargetkan perangkat seluler. Misalnya, sebuah pesan mungkin mengatakan bahwa akun Anda telah disusupi, dan Anda harus membalas dengan informasi nama pengguna dan kata sandi.
- **Tailgating** Jenis serangan ini terjadi ketika orang yang tidak berwenang mengikuti seseorang dengan akses resmi ke area aman dan memperoleh tingkat akses yang sama tanpa kredensial atau izin.
- **Serangan Quid Pro Quo** Serangan quid pro quo melibatkan seseorang yang meminta kredensial Anda dengan imbalan sesuatu (biasanya uang).

Teknik Social Engineering

- **Watering Hole:** Serangan rekayasa sosial di mana seorang peretas membobol situs web populer yang sering dikunjungi target dan menggunakannya untuk mendapatkan informasi tentang mereka.
- **Dumpster Diving:** melibatkan penyerang yang mencari dokumen yang berisi informasi pribadi atau sensitif di tempat sampah.
- **Farming vs Hunting:** Hunting adalah praktik pengumpulan data dari orang-orang dengan sedikit atau tanpa interaksi pribadi. Di sisi lain, Farming sangat bergantung pada pembentukan hubungan baik untuk mendapatkan kepercayaan dari target sebelum tindakan nyata terjadi.
- **Pretexting**: penciptaan cerita palsu/fiksi untuk mendapatkan informasi dari korban, seperti menyamar sebagai orang terdekat seperti teman semasa kecil atau saudara jauh yang sudah lama tidak berkomunikasi.

Examples of Social Engineering

Some common cyberattacks also double as social engineering attacks.

Scareware

Email hacking

Access tailgating

Phishing

DNS spoofing

Physical breaches

Watering hole attacks

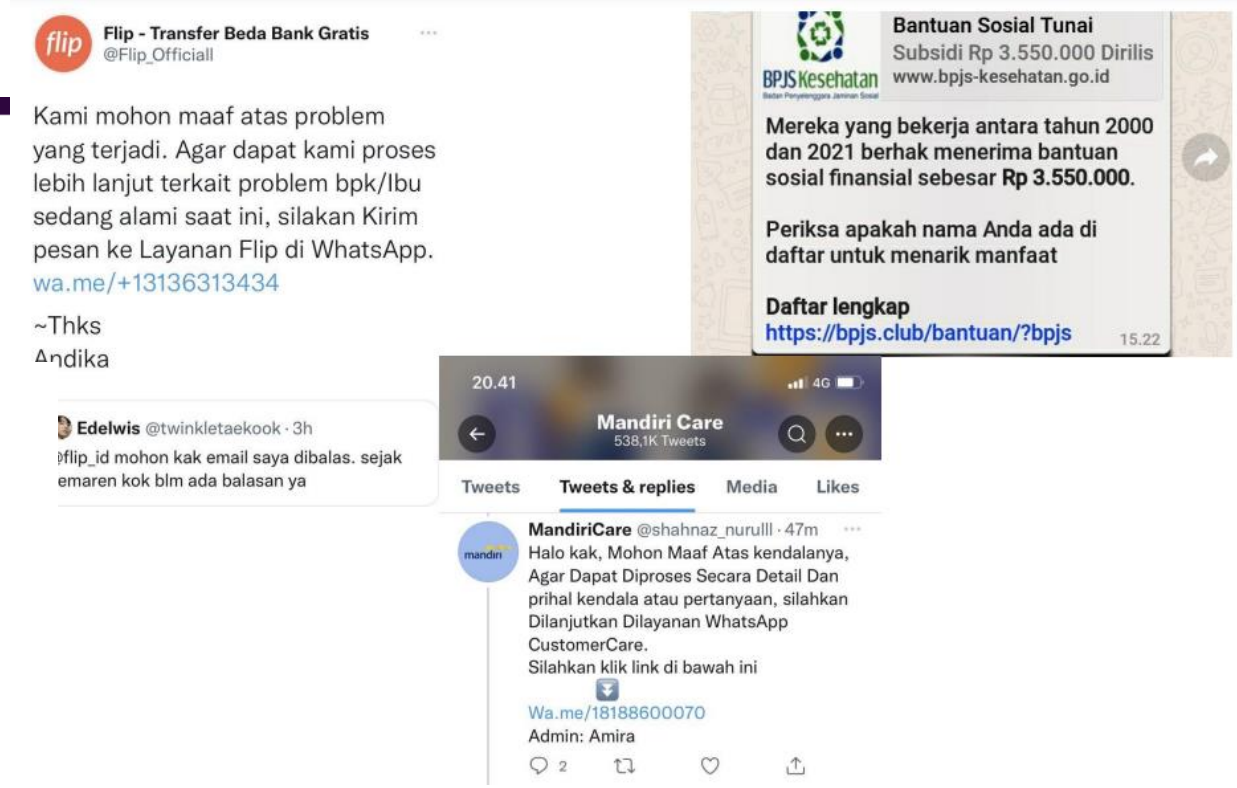
Baiting

Pretexting

Quid pro quo

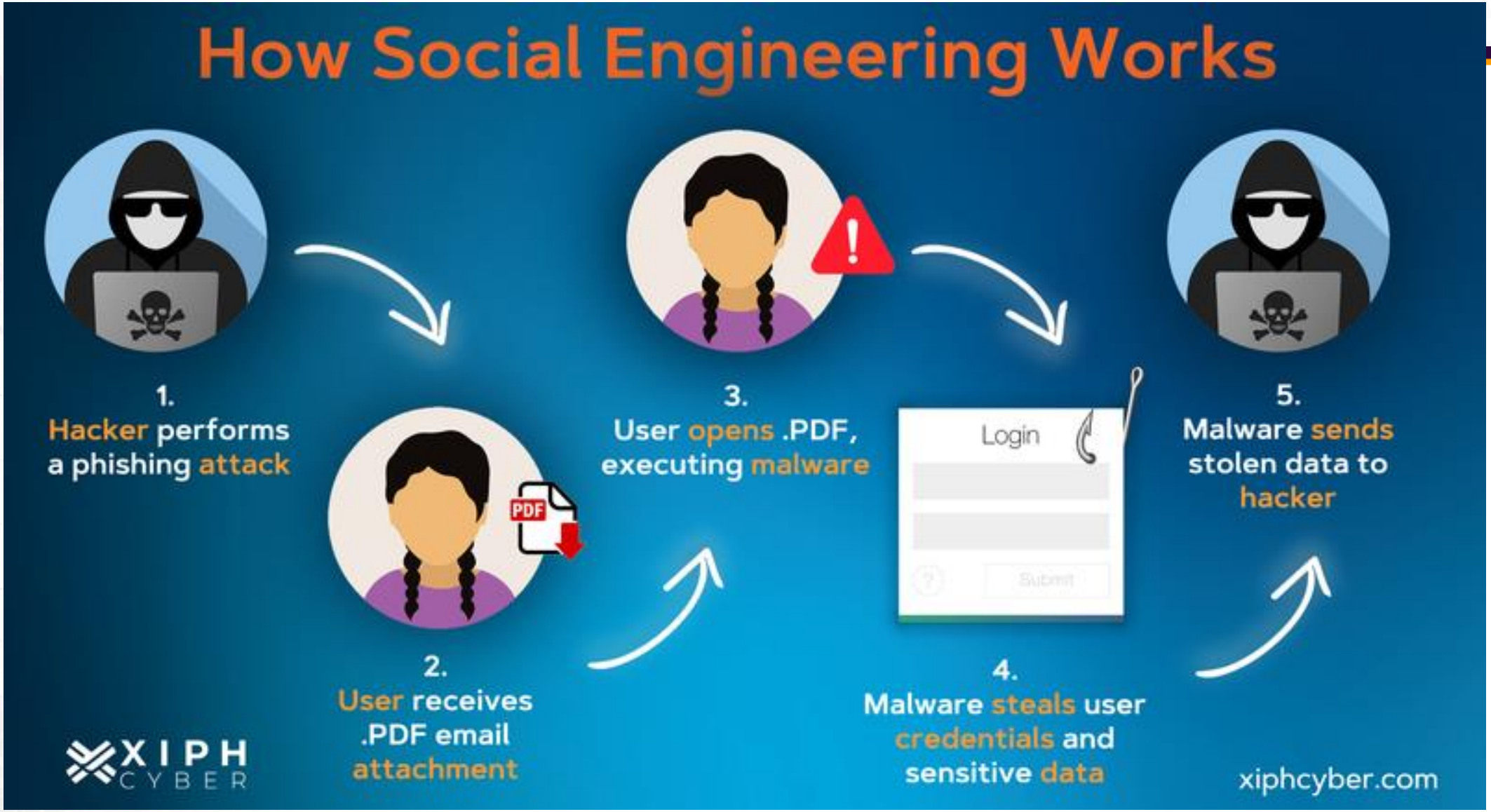
Phising Website

- Register domain yang serupa:
  - www.kilkbca.co.id
  - www.ibank-bni.co.id
- Akun helpdesk di FB, Twitter:
  - @helpdesk_ovo, @ovo.id, @ovoindonesia, @ovo_id
  - @gojek.id, @go.jek, @gojekindonesia, @gojek_id
  - @bni.id, @help.bni, @bni_support, @halo_bni



Bagaimana cara kerja rekayasa sosial?

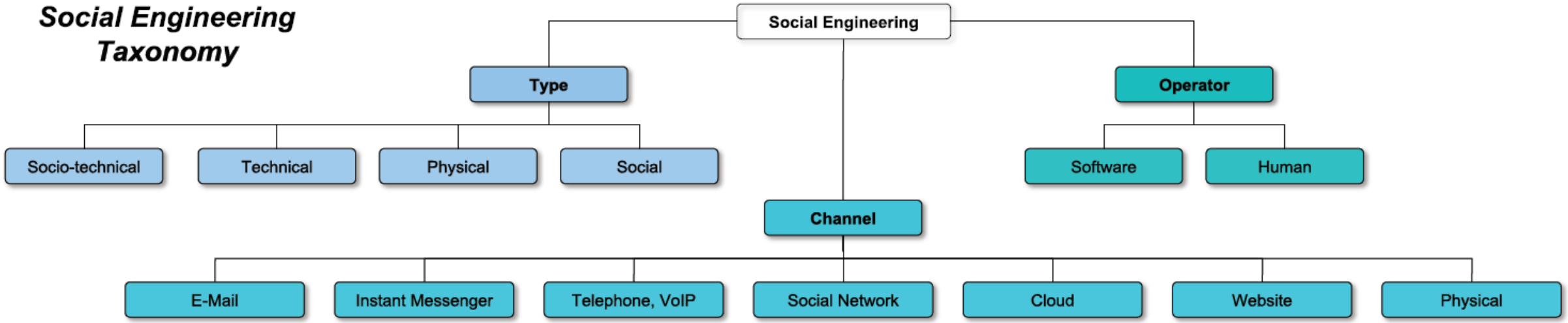
- Rekayasa sosial memanfaatkan kesalahan manusia dan biasanya menimbulkan kepercayaan, otoritas, atau ketakutan palsu untuk mengelabui korban agar membocorkan informasi yang berharga. Penyerang bahkan dapat mempelajari target mereka dan mengumpulkan informasi dari sumber yang tersedia untuk umum seperti profil media sosial dan situs web perusahaan sebelum meluncurkan kampanye serangan.
- Beberapa bahkan dapat membuat skenario atau pesan yang meyakinkan untuk memanipulasi korban mereka.
- Serangan rekayasa sosial memerlukan persiapan, dan penjahat dunia maya sering kali perlu melakukan penelitian sebelum meluncurkan skema penipuan mereka. Tahap pengintaian ini melibatkan pengumpulan informasi tentang **target potensial, peran, kebiasaan, dan kerentanan mereka, yang memungkinkan penyerang untuk menyusun skenario** yang meyakinkan dan memanipulasi kelemahan manusia secara lebih efektif.


How Social Engineering Works
1.
Hacker performs a phishing attack
2.
User receives .PDF email attachment
PDF
3.
User opens .PDF, executing malware
4.
Malware steals user credentials and sensitive data
Login
Submit
5.
Malware sends stolen data to hacker
XIPH CYBER
xiphcyber.com

Bagaimana cara kerja rekayasa sosial?

- **Identifikasi target:** Penyerang memilih target dengan cermat berdasarkan peran mereka dalam organisasi atau nilai potensial informasi yang mereka miliki (misalnya akses ke server internal atau basis data).
- **Kumpulkan informasi:** Penjahat dunia maya mengumpulkan informasi yang relevan tentang target mereka (misalnya alamat email, lokasi kantor) dari sumber yang tersedia untuk umum seperti profil media sosial (misalnya LinkedIn, Facebook), situs web perusahaan, dan direktori daring.
- **Susun skenario yang meyakinkan:** Penyerang menyusun dalih atau skenario yang dapat dipercaya yang disesuaikan dengan anggota tim atau pemimpin. Ini dapat melibatkan penyamaran sebagai kolega, atasan, klien, atau investor tepercaya.
- **Luncurkan serangan:** Penyerang akan memulai kontak dengan target menggunakan berbagai saluran komunikasi — yang paling umum adalah email. Ini juga dapat mencakup panggilan telepon atau pesan media sosial yang tidak diminta.
- **Manipulasi target:** Selama interaksi, penyerang dapat menggunakan taktik psikologis untuk memanipulasi emosi, kepercayaan, atau keingintahuan target. Manipulasi ini menyebabkan target mengungkapkan informasi sensitif atau melakukan tindakan tertentu seperti mengunduh lampiran PDF dengan malware.
- **Eksploitasi:** Setelah target mematuhi permintaan penyerang, penyerang memperoleh akses tidak sah ke sistem, data, atau aset keuangan.

Social Engineering Taxonomy



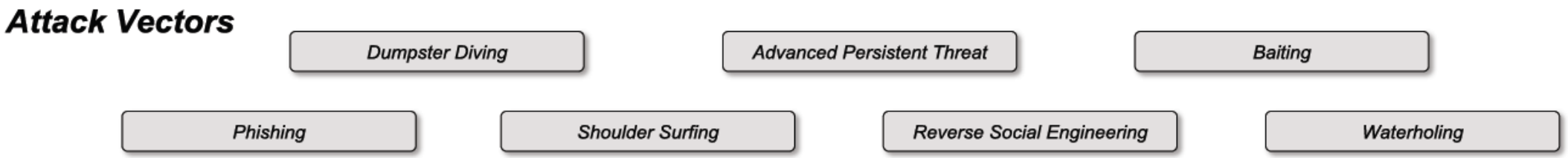


Figure 1: Overview of our classification of attack characteristics and attack scenarios.

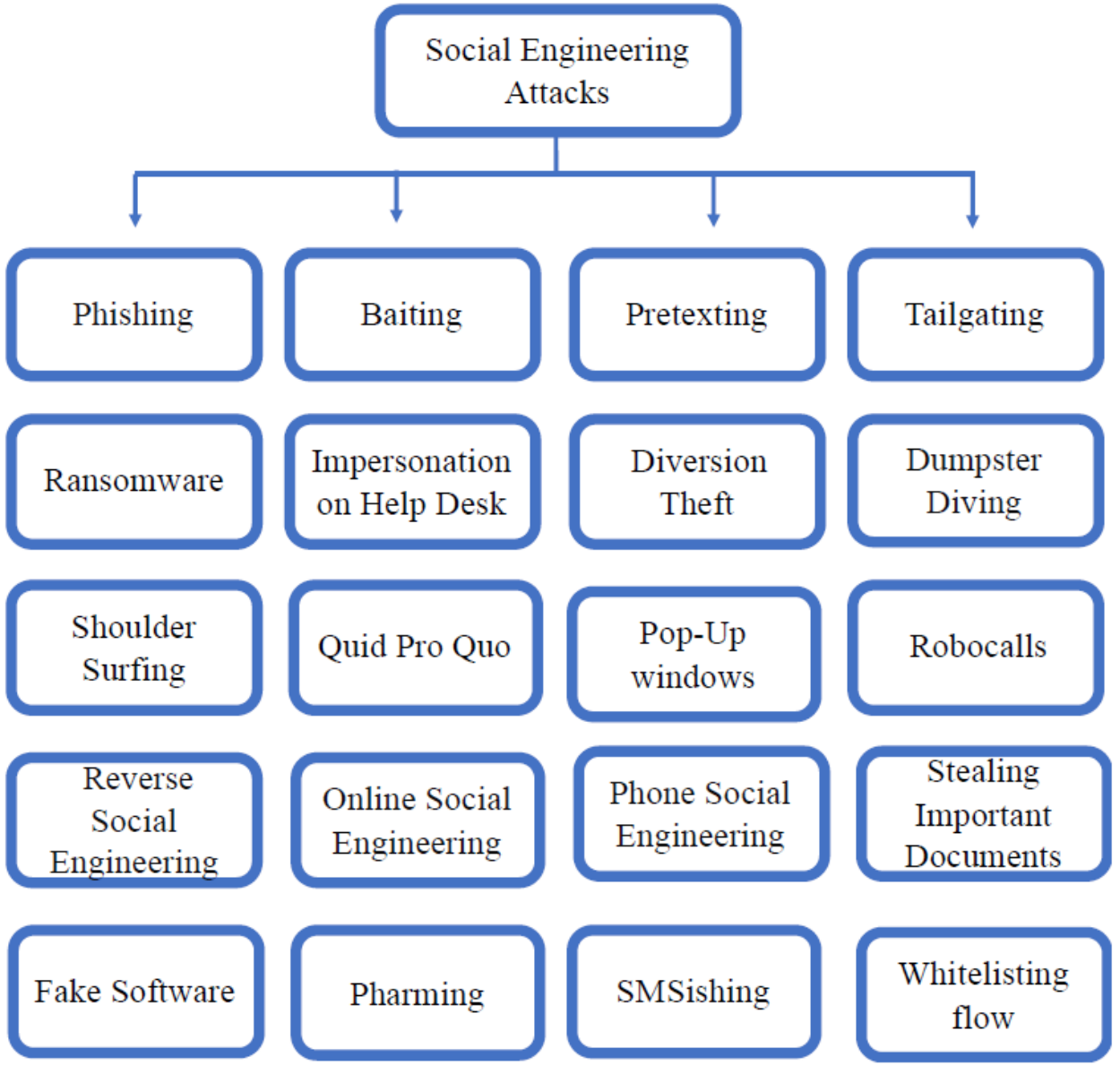


Figure 4. Social engineering attacks.

The Social Engineering Life Cycle

Preparing the ground for the attack:
- Identifying the victim(s.)
- Gathering background information.
- Selecting attack method(s).

Deceiving the victim(s) to gain a foothold:
- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

Obtaining the information over a period of time:
- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

Closing the interaction, ideally without arousing suspicion:
- Removing all traces of malware.
- Covering tracks.
- Bringing the charade to a natural end.

The Social Engineering Life Cycle

- **Information Gathering (Pengumpulan Informasi)** Penyerang mengumpulkan data tentang target yang bisa dieksploitasi.
- **Developing Relationships (Membangun Hubungan)** Penyerang mulai membangun kepercayaan dengan korban, seringkali dengan menyamar sebagai pihak yang tepercaya.
- **Exploitation (Eksploitasi)** Setelah mendapatkan kepercayaan, penyerang mengeksploitasi korban untuk mendapatkan akses atau informasi.
- **Execution (Eksekusi)** Penyerang mencapai tujuannya, baik dengan mencuri informasi, menyebarkan malware, atau mendapatkan akses ilegal ke sistem.

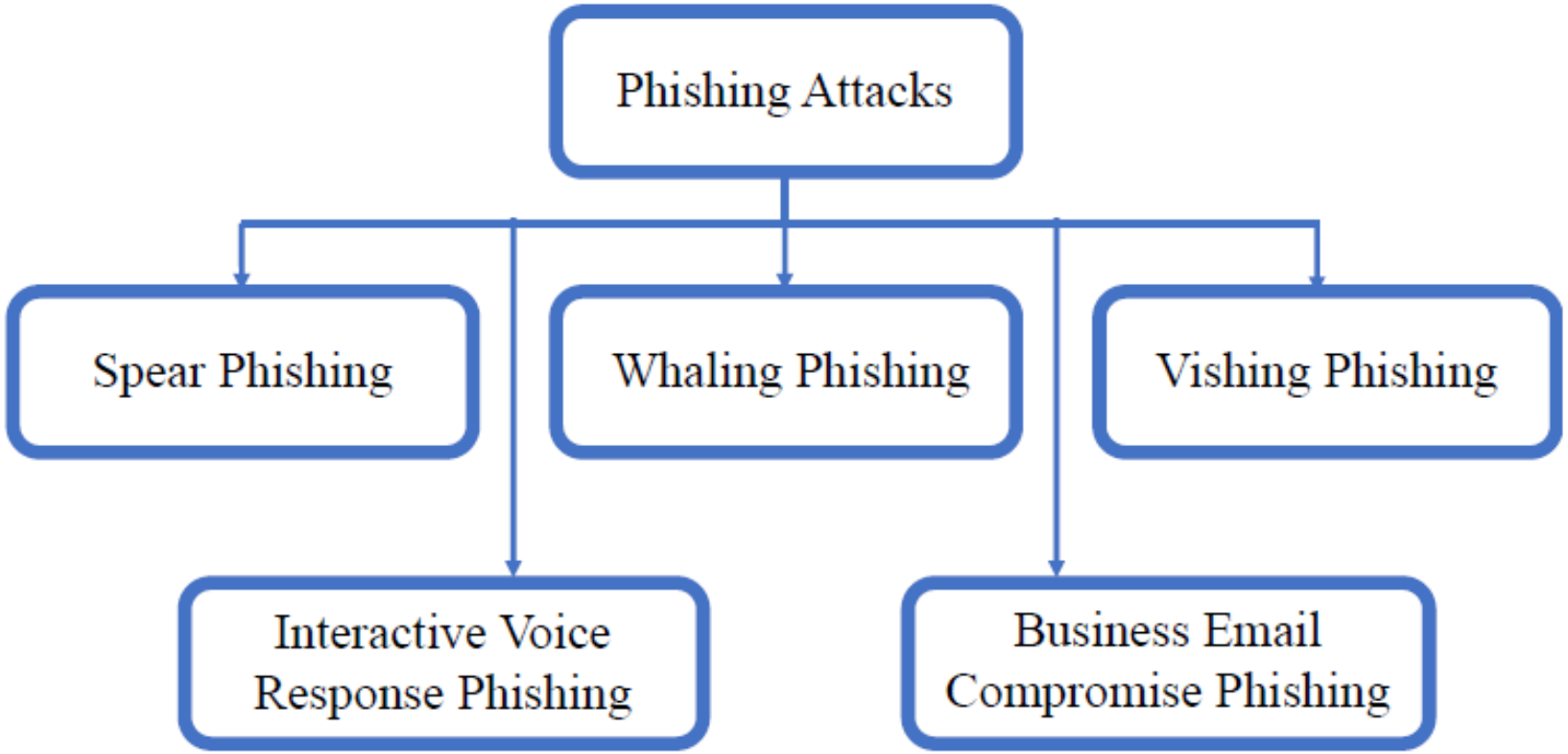


Figure 5. Phishing attacks.

Ontologi

- Model ontologis mencakup komponen-komponen serangan rekayasa sosial seperti komunikasi langsung dan tidak langsung, insinyur sosial, target, media, prinsip kepatuhan, dan teknik.

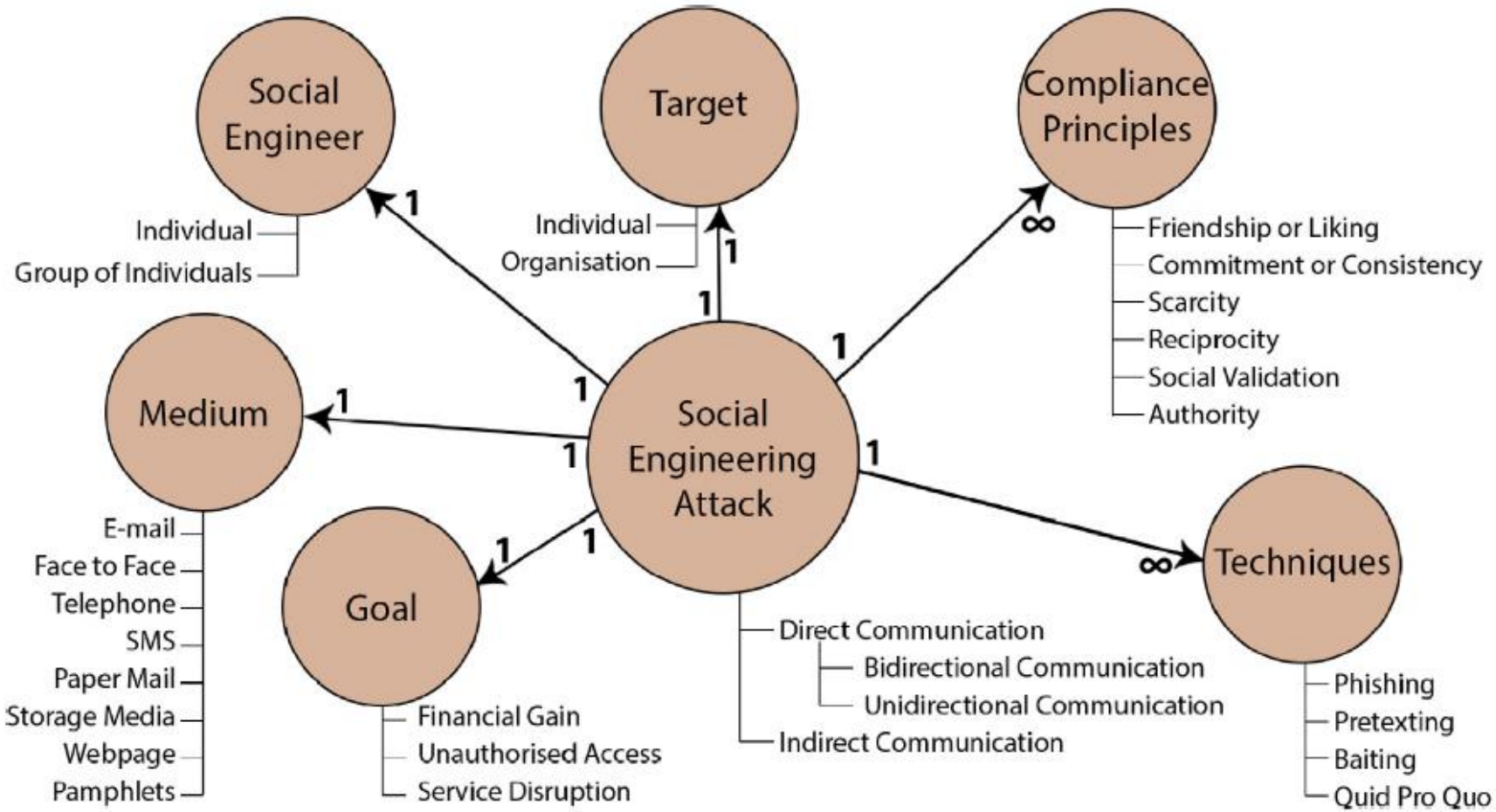


Fig. 1 – An ontological model of a social engineering attack.

Framework Social Engineering

1. **Formulasi Serangan** Menentukan tujuan dan target serangan.
2. **Pengumpulan Informasi** Mengidentifikasi dan mengumpulkan informasi dari berbagai sumber tentang target dan tujuan.
3. **Persiapan** Menggabungkan informasi yang dikumpulkan dan mengembangkan vektor serangan.
4. **Mengembangkan Hubungan** Membangun komunikasi dan kepercayaan dengan target.
5. **Eksploitasi Hubungan** Memanfaatkan hubungan yang telah dibangun untuk mencapai tujuan serangan.
6. **Debrief** Mengevaluasi keberhasilan serangan dan memastikan target tidak menyadari bahwa mereka telah diserang.

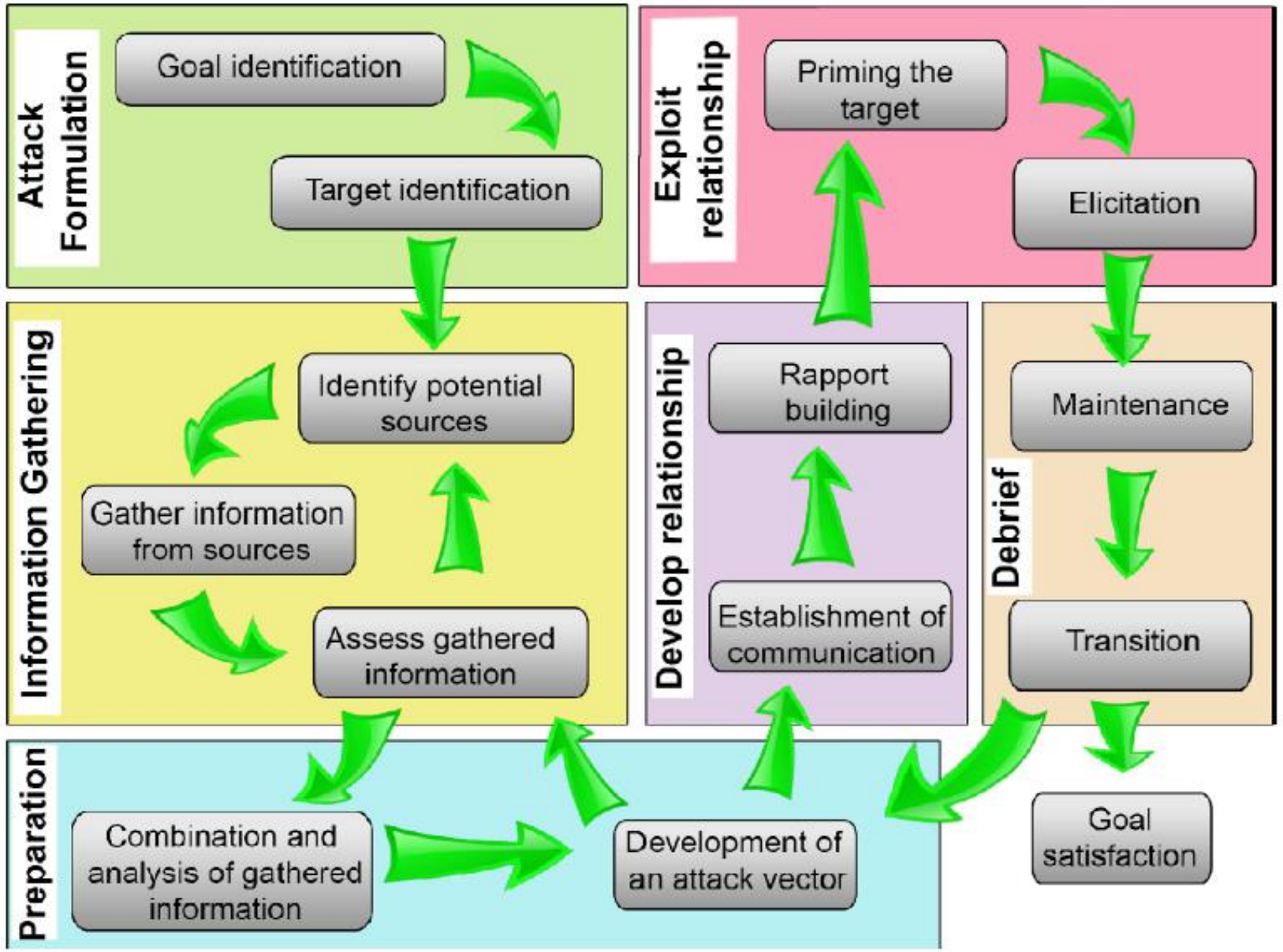


Fig. 2 – Social engineering attack framework.

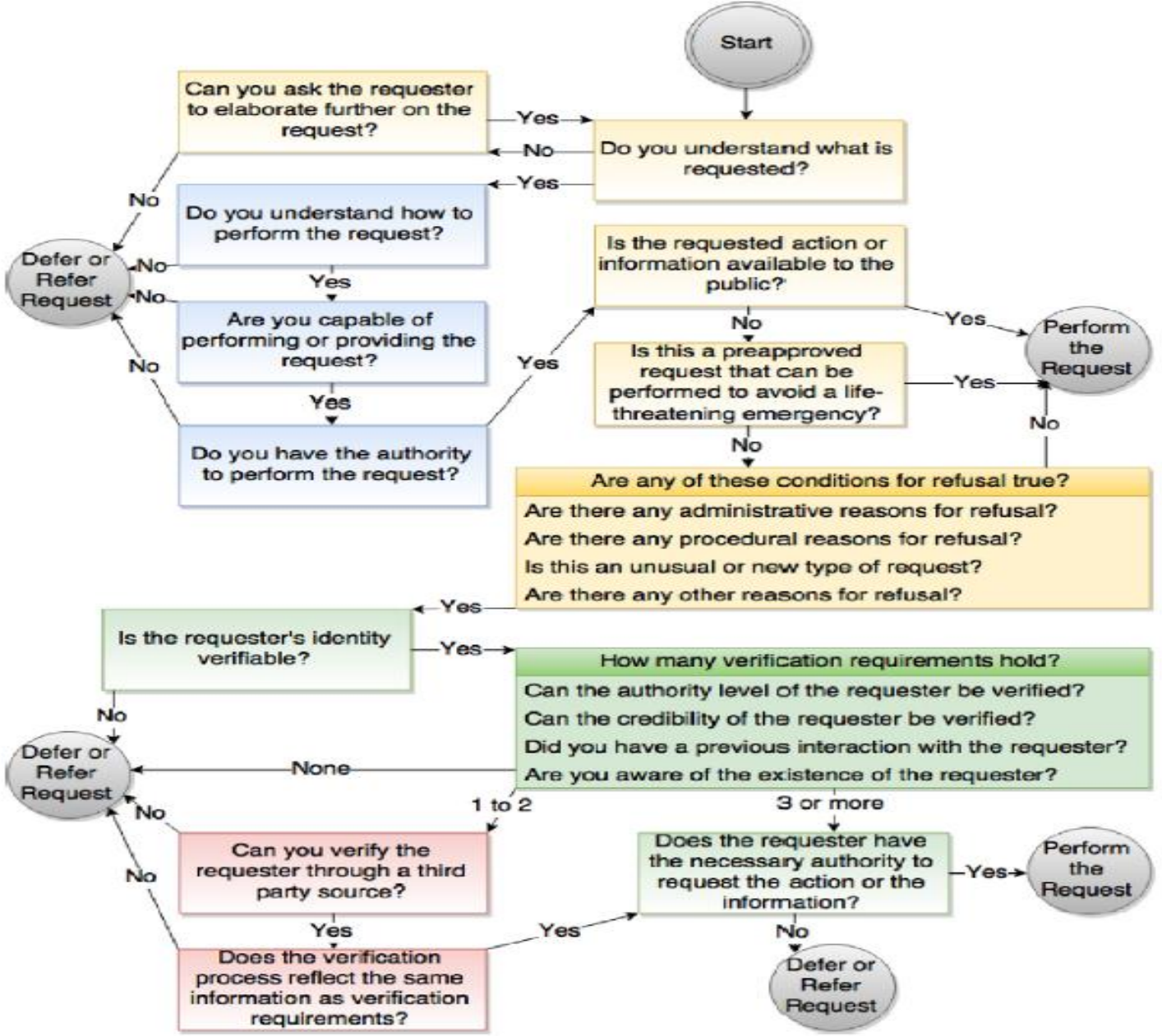


Fig. 3 – Social engineering attack detection model (Mouton et al., 2015).

3. Skenario dan Antisipasi Social Engineering

- Seorang karyawan menerima email yang tampaknya berasal dari manajernya yang meminta dia untuk mengklik tautan dan memperbarui informasi akun. Karena tampak seperti email resmi, karyawan tersebut mengklik tautan, tanpa menyadari bahwa itu adalah situs palsu yang digunakan untuk mencuri kredensial login.
- **Termasuk Teknik apa ?? Cara mengantisipasinya bagaimana ??**

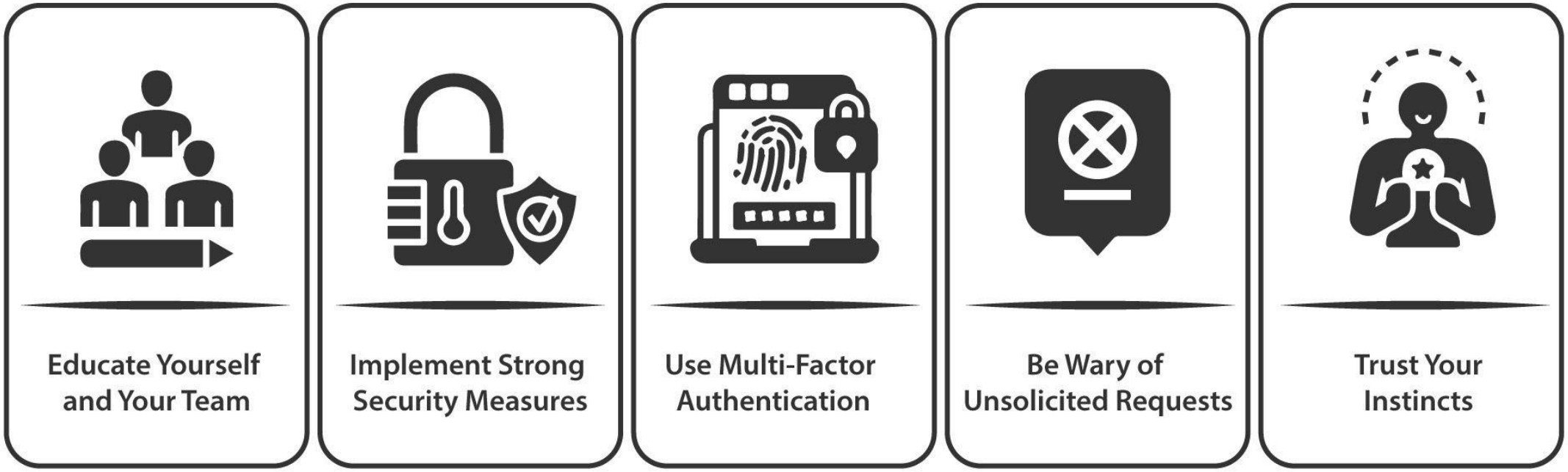
1. Edukasi dan pelatihan tentang cara mengenali email phishing.
2. Penerapan kebijakan email yang ketat (verifikasi email, otentikasi multi-faktor).
3. Filter spam dan sistem keamanan email yang canggih.

3. Skenario dan Antisipasi Social Engineering

- Penyerang menelepon resepsionis sebuah perusahaan dan berpura-pura menjadi teknisi IT yang membutuhkan akses ke sistem server untuk perbaikan darurat. Penyerang berhasil meyakinkan resepsionis untuk memberikan kredensial login.
- **Termasuk Teknik apa ?? Cara mengantisipasinya bagaimana ??**

1. Penerapan prosedur verifikasi identitas bagi pihak eksternal.
2. Pelatihan staf tentang skenario social engineering.
3. Penggunaan otentikasi ganda dan audit akses.

Ways To Prevent Social Engineering Attacks



How to prevent social engineering attacks

- **Kesadaran dan pelatihan:** Berikan edukasi kepada karyawan dan individu tentang taktik rekayasa sosial seperti phishing dan pretexting. Dorong budaya skeptisisme saat menghadapi permintaan informasi atau tindakan yang tidak diminta. Jalankan pengujian phishing dan sesi pelatihan secara berkala untuk menjaga organisasi Anda tetap waspada terhadap potensi ancaman.
- **Verifikasi identitas:** Selalu verifikasi identitas individu yang meminta informasi sensitif atau akses. Misalnya, jika seseorang mengaku dari dukungan TI, konfirmasikan identitas mereka dengan departemen TI sebelum memberikan informasi apa pun.
- **Autentikasi multifaktor (MFA):** Terapkan perlindungan kata sandi yang kuat dan MFA sedapat mungkin. Ini menambahkan lapisan keamanan ekstra dengan mengharuskan pengguna untuk memberikan beberapa metode autentikasi sebelum mendapatkan akses ke akun atau sistem.
- **Perangkat lunak keamanan siber**: Berinvestasilah pada perangkat lunak anti-virus dan anti-malware yang kuat untuk mendeteksi dan mencegah instalasi perangkat lunak berbahaya. Pastikan semua perangkat lunak diperbarui dan ditambal untuk mengatasi kerentanan yang diketahui.
- **Penyaringan email:** Gunakan sistem penyaringan email yang dapat mengidentifikasi dan mengkarantina email phishing dan berbahaya. Sistem ini dapat mengurangi kemungkinan karyawan menjadi korban serangan phishing.
- **Enkripsi data:** Terapkan enkripsi data untuk melindungi informasi sensitif saat dikirim dan tidak digunakan. Enkripsi AES 256-bit adalah standar enkripsi yang paling canggih.

PRAKTEK ENSKRIPSI AES 256 bit

- thisis32charactersecretkey!!!123
- https://colab.research.google.com/drive/1eivqRfN8OSERaYAT_5zkX3_KCTZ1k5SZ?usp=sharing

yoga sahria

- ZFrekuPB7nk8307E9yWppGucvxkeSM3f1pUwnypu9o8=
- FUH9XkKV8SEa9oEdaOavG+aZYI7vxBNds1ubO8+dP7w=

Kesimpulan

- **Social engineering dalam cyber security** adalah ancaman serius karena memanfaatkan faktor manusia yang sering kali merupakan titik lemah dalam sistem keamanan. Dengan memahami teknik, framework, dan skenario yang digunakan, organisasi dapat menerapkan langkah-langkah pencegahan yang tepat untuk mengurangi risiko serangan social engineering.
- Edukasi yang terus-menerus, prosedur keamanan yang ketat, dan pemantauan yang cermat menjadi kunci untuk menjaga keamanan informasi dan infrastruktur perusahaan.

Praktek

- https://linktr.ee/amanbergerak

UNIVERSITAS
AMIKOM
YOGYAKARTA