

# Pelatihan Data Mining, Science & Perluasan Lini Bisnis, Consumer Data- Hacker, Cracker Game di Dhadhu Board Game & SMA Negeri 3, Semarang

Indra Gamayanto<sup>1</sup>, Sasono Wibowo<sup>2</sup>, Sendi Novianto<sup>3</sup>, Farrikh Al Zami<sup>4</sup>, Arta Moro Sundjaja<sup>5</sup>,  
Tamsir Hasudungan Sirait<sup>6</sup>, Ramadhan Rakhmat Sani<sup>7</sup>, Asih Rohmani<sup>8</sup>

<sup>1,2,3,4,7</sup>Fakultas Ilmu Komputer, Departemen Sistem Informasi & Teknik Informatika,  
Universitas Dian Nuswantoro (UDINUS), Imam Bonjol 207, Semarang

<sup>5</sup>Departemen Manajemen, BINUS Business School, Master Program, Bina Nusantara University  
(BINUS), Jakarta

<sup>6</sup>Departemen Sistem Informasi, Institut Teknologi Harapan Bangsa (ITHB), Dipatiukur 80-84,  
Bandung

E-mail: <sup>1</sup>indra.gamayanto@dsn.dinus.ac.id, <sup>2</sup>sasono.wibowo@dsn.dinus.ac.id,  
<sup>3</sup>sendi.novianto@dsn.dinus.ac.id, <sup>4</sup>alzami@dsn.dinus.ac.id, <sup>5</sup>asundjaja@binus.edu,  
<sup>6</sup>tamsir@ithb.ac.id, <sup>7</sup>ramadhan\_rs@dsn.dinus.ac.id, <sup>8</sup>aseharsoyo@dsn.dinus.ac.id<sup>8</sup>

## Abstrak

Data mining, data science, perluasan lini, hacker, cracker dan game merupakan factor-faktor penting dalam pengembangan kompetensi sumber daya manusia di masa depan. Pengabdian ini disebut megatron pengabdian masyarakat karena meliputi banyak hal yang saling terkait satu sama lain dan melibatkan satu bisnis dan satu institusi pendidikan. Hal ini merupakan kolaborasi yang sangat baik dalam mengembangkan bisnis, sumber daya manusia dan kompetensi yang berkelanjutan. Pada jurnal pengabdian ini, kami tentunya tidak bisa menjelaskan secara details karena akan sangat panjang dalam penjelasannya, tetapi gambaran besar dari materi akan dijelaskan. Lebih jauh lagi, pengabdian masyarakat ini akan dilanjutkan sampai pada level advanced, dimana pada pengabdian ini, struktur dari penerapannya membutuhkan waktu karena bersifat konprehensif dan akan menghasilkan sesuatu untuk memberikan keuntungan pada café dan peningkatan kompetensi secara signifikan terhadap SMAN 3, Semarang. Hasil dari pengabdian ini adalah Dhadhu board game akan dapat menerapkan dan mengembangkan data mining, science, consumer dan perluasan lini bisnis mereka, sedangkan untuk SMAN 3, Semarang, siswa dan guru akan memperoleh manfaat yang besar untuk meningkatkan kompetensi di bidang hacker, cracker, dan dalam menghadapi social engineering. Hal ini juga berguna untuk Dhadhu board game café karena akan dapat mengelola datanya dengan baik sehingga dapat menghindari hal yang tidak baik pada social engineering juga.

Kata kunci: Hacker, Cracker, Lini bisnis, Data mining, Data Science

## Abstract

*Data mining, data science, line expansion, hackers, crackers and games are important factors in developing human resource competencies in the future. This service is called megatron community service because it covers many things that are interrelated and involve a business and an educational institution. This is an excellent collaboration in developing sustainable business, human resources and competencies. In this service journal, we certainly cannot explain in detail because the explanation will be very long, but the big picture of the material will be explained. Furthermore, this community service will be continued to the advanced level, where in this service, the implementation structure takes time because it is comprehensive and will produce something to provide benefits to the café and significantly increase competency at SMAN 3, Semarang. The result of this service is that Dhadhu board games will be able to apply and develop data mining, science, consumer and expand their business lines, while for SMAN 3, Semarang, students and teachers will gain great benefits to increase competence in the fields of hackers, crackers and in dealing with social engineering. This is also useful for the Dhadhu*

*board game café because it will be able to manage its data well so that it can avoid bad things in social engineering too.*

*Keywords: Hacker, Cracker, Lini bisnis, Data mining, Data Science*

## 1. PENDAHULUAN

Salah satu hal yang terpenting di dalam pengabdian masyarakat adalah bahwa kita tidak hanya melakukan pelatihan, tetapi dapat memberikan yang terbaik kepada tempat dimana kita melakukan pengabdian masyarakat. Perubahan dibutuhkan agar dapat meningkatkan kompetensi dan sebuah perubahan yang signifikan akan dapat terjadi jika apa yang diberikan dapat menghasilkan dampak yang besar terhadap sumber daya manusia serta hal lainnya yang bersifat crucial. Pengabdian masyarakat ini berada di dua tempat, yaitu SMA Negeri 3, Semarang, dimana diberikan pelatihan tentang social engineering seperti cracker, hacker dan juga board game, dan hal ini menyambung ke Dhadhu Board game café yang akan meliputi data mining, data science dan perluasan lini bisnis serta konsumen. Keduanya tidak dapat dipisahkan satu sama lain dan akan dapat menghasilkan sesuatu yang baik bagi kedua tempat tersebut. Hasil dari pengabdian masyarakat ini adalah pemahaman yang lebih tinggi mengenai hal-hal yang telah disebutkan di atas dan akan meningkatkan sumber daya manusia secara signifikan.

Data mining adalah proses mengekstraksi informasi, pola, dan tren yang berguna yang melampaui analisis sampel dari database besar dan menyajikan informasi yang relevan dan dapat digunakan untuk memecahkan masalah bisnis. Sebaliknya, ilmu data didefinisikan sebagai proses memperoleh wawasan berharga dari data terstruktur dan tidak terstruktur dengan menggunakan berbagai alat dan Teknik. Sedangkan data science adalah menggabungkan beberapa aspek Data seperti Teknologi, pengembangan Algoritma, dan interferensi data untuk mempelajari data, menganalisisnya, dan menemukan solusi inovatif untuk masalah sulit. Ilmu Data adalah tentang Menganalisis data dan mendorong pertumbuhan bisnis dengan menemukan cara-cara kreatif. Social engineering adalah seni memanipulasi orang sehingga mereka memberikan informasi rahasia. Jenis informasi yang dicari para penjahat ini dapat bervariasi, namun ketika individu menjadi sasaran, para penjahat tersebut biasanya mencoba menipu Anda agar memberikan mereka kata sandi atau informasi bank Anda, atau mengakses komputer Anda untuk secara diam-diam menginstal perangkat lunak berbahaya – yang akan memberi mereka akses ke informasi Anda. kata sandi dan informasi bank serta memberi mereka kendali atas komputer Anda. Penjahat menggunakan taktik rekayasa sosial karena biasanya lebih mudah mengeksploitasi kecenderungan alami Anda untuk percaya daripada menemukan cara untuk meretas perangkat lunak Anda. Misalnya, jauh lebih mudah untuk membodohi seseorang agar memberikan kata sandinya kepada Anda daripada Anda mencoba meretas kata sandinya (kecuali kata sandinya benar-benar lemah)[1].

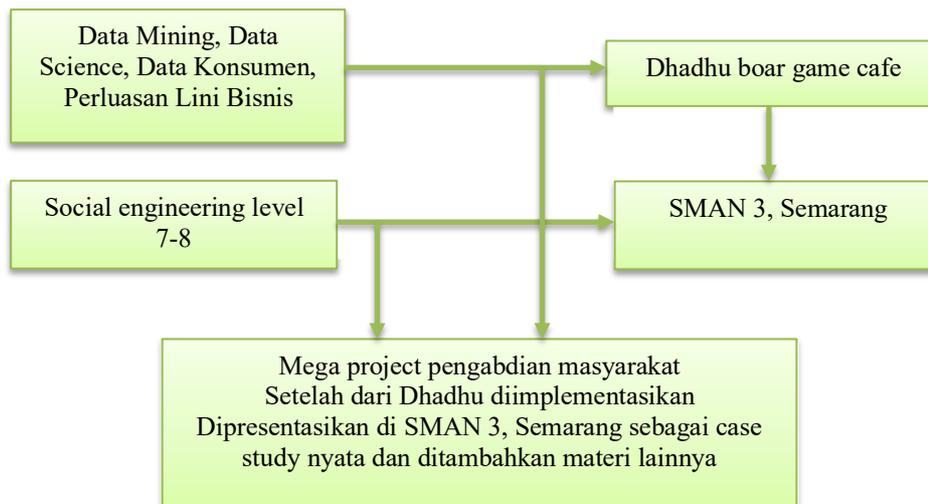
## 2. METODE



Gambar 1. Proses pengabdian masyarakat

Gambar 1, menjelaskan proses pengabdian masyarakat yang kami lakukan di Dhadhu board game café dan SMAN 3, Semarang. Pada awal pengabdian kami melakukan pelatihan dan menerapkan data mining, data science dan perbaikan pada data konsumen serta lini bisnis, setelah kamu selesai kami melakukan pengabdian di SMAN 3 Semarang mengenai social engineering 7.0, dan setelah selesai kami melakukan pelatihan data mining, data science, contoh studi kasus, dan hal ini sudah diterapkan di Dhadhu board game café, sehingga siswa dan guru akan dapat memiliki contoh nyata. Ini yang disebut mega pengabdian masyarakat, dimana dua tempat akan dapat disatukan untuk saling membantu dalam mengembangkan kompetensi, yang pertama tempat untuk menerapkan, yang kedua untuk diberikan contoh nyata, sehingga hal ini bukan lagi pelatihan tetapi pengabdian terapan yang dapat digunakan untuk meningkatkan kompetensi sumber daya manusia melalui proses perubahan yang signifikan.

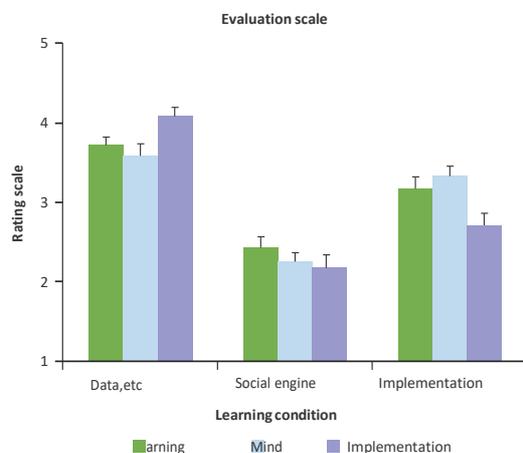
Pola mega proyek pengabdian masyarakat untuk meningkatkan kompetensi secara maksimum:



Gambar 2. Mega proyek pengabdian masyarakat – proses

### 3. HASIL DAN PEMBAHASAN

#### 3.1. Pre test dan Post test



Gambar 3. Pre test dan Post test

Gambar 3, menjelaskan setelah dilakukan pelatihan data mining dan beberapa hal penting di Dhadhu board game café, maka seluruh staff khususnya dalam bidang IT dapat memahami penerapan hal tersebut, berikutnya pelatihan yang dilakukan oleh SMAN 3, Semarang juga menemui progress yang sangat baik. Hasil akhirnya adalah kombinasi kedua tempat tersebut menghasilkan hal yang mengubah tingkat kompetensi menjadi semakin baik karena dihadirkan studi kasus nyata yang sudah diimplementasikan

#### 3.2. Kegiatan pengabdian masyarakat

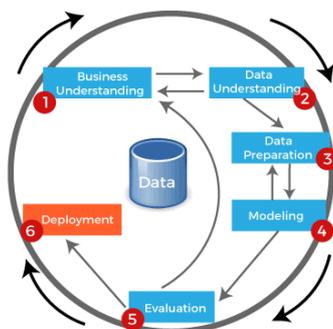


Gambar 4. Dhadhu Board Game Café & SMAN 3, Semarang

#### 3.3. Materi pengabdian masyarakat dan penjelasan

Data mining adalah proses mengekstraksi informasi, pola, dan tren yang berguna dari data mentah. Penambangan data menggunakan algoritma matematika yang canggih untuk

membagi data dan mengevaluasi kemungkinan kejadian di masa depan. Ada berbagai jenis layanan dalam proses penambangan data, seperti penambangan teks, penambangan web, penambangan audio, penambangan video, penambangan data bergambar, dan penambangan data jaringan sosial. Penambangan data dilakukan melalui perangkat lunak sederhana atau canggih. Penambangan data disebut Knowledge Discovery in Data (KDD)[2],[3]. Berikut ini adalah Ini adalah langkah-langkah tertentu yang terlibat dalam proses data mining:



Gambar 5. Proses data mining

**Pemahaman Bisnis:** Yang menonjol, aspek utamanya adalah memahami tujuan dan pekerjaan. Tujuan bisnis diperkenalkan, dan faktor-faktor penting yang membantu mencapai target ditemukan.

**Pemahaman Data:** Pengumpulan data dilakukan pada langkah ini, dan semua data yang dikumpulkan diakumulasikan dalam alat (jika Anda menggunakan alat apa pun). Kemudian data dicantumkan beserta sumber datanya, lokasinya, dan cara pencapaiannya, jika terjadi masalah, data divisualisasikan dan diminta untuk diperiksa kelengkapannya[4],[5].

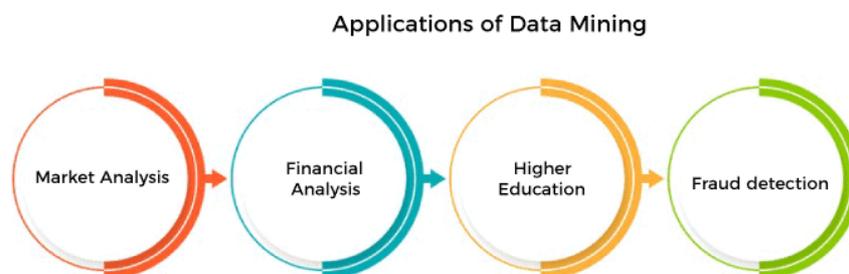
**Persiapan data:** Persiapan data melibatkan pemilihan data yang berguna, pembersihan data, pembuatan atribut dari data, dan integrasi data dari beberapa database.

**Pemodelan:** Pemodelan melibatkan pemilihan teknik penambangan data, misalnya induksi pohon keputusan, pembuatan desain pengujian untuk evaluasi model yang dipilih, pembuatan model dari kumpulan data, dan penilaian model yang dibuat dengan para ahli untuk mengetahui hasilnya[6].

**Evaluasi:** Seperti namanya, evaluasi menentukan sejauh mana model yang dihasilkan memenuhi tuntutan bisnis. Hal ini dilakukan dengan menguji model berdasarkan aplikasi nyata.

**Penyebaran:** Pada tahap ini dibuat rencana penerapan, strategi untuk memelihara dan memantau hasil model data mining, memeriksa kegunaannya.

### Aplikasi data mining



Gambar 6. Aplikasi data mining

**Analisis Pasar:** Analisis pasar menyediakan berbagai macam data untuk membantu Anda merencanakan strategi pemasaran Anda. Meskipun data yang terkait dengan ukuran pasar

memungkinkan Anda memutuskan apakah pasar tersebut bagus untuk berinvestasi atau tidak, Anda juga perlu mengetahui cara kerja pasar.

**Analisa keuangan:** Sistem perbankan dan keuangan bergantung pada data yang berkualitas baik dan akurat. Di departemen pinjaman, data yang berkaitan dengan keuangan dan pengguna dapat digunakan untuk berbagai tujuan, seperti menghitung peringkat kredit.

**Pendidikan yang lebih tinggi:** Seiring dengan meningkatnya persyaratan untuk studi lebih tinggi di seluruh dunia, institusi mencari berbagai solusi untuk memenuhi kebutuhan yang meningkat. Institusi menggunakan data mining untuk menganalisis siswa mana yang akan mendaftar dalam program tertentu, dan siapa yang memerlukan bantuan lebih lanjut.

**Deteksi penipuan:** Mekanisme yang digunakan untuk mendeteksi aktivitas penipuan terbukti memakan waktu. Setelah diperkenalkannya data mining, deteksi penipuan menjadi lebih mudah. Data Mining mempermudah identifikasi pola dan membantu mengambil langkah-langkah untuk memastikan privasi informasi pengguna.

**Penerapan data science**

**Kesehatan:** Penerapan ilmu data di berbagai sektor berkembang pesat. Layanan kesehatan adalah salah satu sektor utama yang diubah secara bertahap oleh ilmu data,

**Pencarian internet:** Banyak mesin pencari seperti Yahoo, Google, dan Bing menggunakan algoritma ilmu data untuk memberikan hasil terbaik untuk permintaan pencarian kami dalam hitungan detik.

**Deteksi Penipuan dan Risiko:** Ilmu data memberikan pemikiran kreatif, ilmiah, dan investigatif terhadap data besar. Data diambil secara acak dari berbagai sektor dan platform seperti survei melalui telepon, email, platform media sosial, dll.

**Pengenalan gambar:** Di era digital ini, alat data science sudah mulai mengenali wajah manusia dengan semua gambar yang tersedia di databasenya[7].

Perbedaan antara ilmu data dan penambangan data

Data mining

- Proses mengekstraksi informasi, pola, dan tren yang berguna dari database yang sangat besar.
- Sebuah teknik.
- Terutama digunakan untuk tujuan bisnis
- Ini terlibat dengan prosesnya
- Bertujuan untuk membuat data lebih penting dan berguna; itu berarti hanya mengekstraksi Informasi yang berguna.
- Merupakan satu Teknik, bagian dari KDD (Knowledge Discovery in Database Process).
- Berkaitan dengan data terstruktur.

Data science[8]

- Mengacu pada proses memperoleh wawasan berharga dari data terstruktur dan tidak terstruktur dengan menggunakan berbagai alat dan metode.
- sebuah bidang
- Terutama digunakan untuk tujuan ilmiah.
- Ini menekankan ilmu data
- Untuk menciptakan produk data yang dominan.
- Bidang studi seperti Teknik Mesin, Arsitektur Cloud, dll.
- Berkaitan dengan segala jenis data seperti terstruktur, semi-terstruktur, dan tidak terstruktur.

Seperti Apa Serangan Rekayasa Sosial Itu?

Email dari seorang teman-Jika penjahat berhasil meretas atau merekayasa kata sandi email seseorang, mereka memiliki akses ke daftar kontak orang tersebut – dan karena kebanyakan

orang menggunakan satu kata sandi di mana pun, mereka mungkin juga memiliki akses ke kontak jejaring sosial orang tersebut. Setelah penjahat menguasai akun email tersebut, mereka mengirim email ke semua kontak orang tersebut atau meninggalkan pesan di semua halaman sosial temannya, dan mungkin di halaman teman teman orang tersebut[9],[10].

Memanfaatkan kepercayaan dan keingintahuan Anda, pesan-pesan ini akan: -Berisi tautan yang hanya perlu Anda periksa—dan karena tautan tersebut berasal dari teman dan Anda penasaran, Anda akan memercayai tautan tersebut dan mengkliknya—dan terinfeksi malware sehingga penjahat dapat mengambil alih mesin Anda dan mengumpulkannya. info kontak dan menipu mereka sama seperti Anda ditipu Berisi unduhan gambar, musik, film, dokumen, dll., yang mengandung perangkat lunak berbahaya. Jika Anda mengunduh – yang kemungkinan besar Anda lakukan karena Anda mengira itu dari teman Anda – Anda terinfeksi. Sekarang, penjahat memiliki akses ke mesin Anda, akun email, akun jaringan sosial dan kontak, dan serangan menyebar ke semua orang yang Anda kenal. Dan seterusnya, dan seterusnya. Email dari sumber tepercaya lainnya-Serangan phishing adalah bagian dari strategi rekayasa sosial yang meniru sumber tepercaya dan menyusun skenario yang tampaknya logis untuk menyerahkan kredensial login atau data pribadi sensitif lainnya. Menurut data Webroot , lembaga keuangan mewakili sebagian besar perusahaan yang meniru identitas dan, menurut Laporan Investigasi Pelanggaran Data tahunan Verizon , serangan rekayasa sosial termasuk phishing dan pretexting (lihat di bawah) bertanggung jawab atas 93% pelanggaran data yang berhasil[11].

Dengan menggunakan cerita atau dalih yang menarik, pesan-pesan ini dapat:-Segera minta bantuan Anda. 'Teman' Anda terjebak di negara X, dirampok, dipukuli, dan dirawat di rumah sakit. Mereka membutuhkan Anda untuk mengirim uang agar mereka bisa pulang dan memberi tahu Anda cara mengirim uang ke penjahat. Gunakan upaya phishing dengan latar belakang yang tampak sah . Biasanya, seorang phisher mengirimkan email, IM, komentar, atau pesan teks yang tampaknya berasal dari perusahaan, bank, sekolah, atau institusi yang sah dan populer. Meminta Anda untuk menyumbang ke penggalangan dana amal mereka, atau tujuan lainnya. Kemungkinan besar berisi instruksi tentang cara mengirim uang ke penjahat. Memangsa kebaikan dan kemurahan hati, para phisher ini meminta bantuan atau dukungan untuk bencana, kampanye politik, atau kegiatan amal apa pun yang menjadi prioritas utama mereka.

Sajikan masalah yang mengharuskan Anda untuk "memverifikasi" informasi Anda dengan mengklik link yang ditampilkan dan memberikan informasi dalam formulirnya. Lokasi tautan mungkin terlihat sangat sah dengan semua logo dan konten yang tepat (pada kenyataannya, penjahat mungkin telah menyalin format dan konten yang sama persis dari situs yang sah). Karena semuanya terlihat sah, Anda memercayai email dan situs palsu tersebut dan memberikan informasi apa pun yang diminta penjahat. Jenis penipuan phishing ini sering kali menyertakan peringatan tentang apa yang akan terjadi jika Anda tidak segera bertindak karena penjahat tahu bahwa jika mereka dapat membuat Anda bertindak sebelum berpikir, kemungkinan besar Anda akan tertipu oleh upaya phishing mereka.

Memberi tahu Anda bahwa Anda adalah 'pemenang'. Mungkin email tersebut mengaku berasal dari lotere, atau kerabat yang sudah meninggal, atau orang ke-sejuta yang mengklik situs mereka, dll. Untuk memberi Anda 'kemenangan', Anda harus memberikan informasi tentang perutean bank Anda sehingga mereka tahu caranya kirimkan kepada Anda atau berikan alamat dan nomor telepon Anda agar mereka dapat mengirimkan hadiahnya, dan Anda mungkin juga diminta untuk membuktikan siapa Anda sering kali termasuk nomor jaminan sosial Anda. Ini adalah 'phishing keserakahan' yang meskipun dalih ceritanya tipis, orang-orang menginginkan apa yang ditawarkan dan tertipu dengan memberikan informasi mereka, kemudian rekening bank mereka dikosongkan, dan identitas mereka dicuri.

Berpose sebagai bos atau rekan kerja. Ini mungkin meminta pembaruan tentang proyek penting dan eksklusif yang sedang dikerjakan perusahaan Anda, informasi pembayaran yang berkaitan dengan kartu kredit perusahaan, atau pertanyaan lain yang menyamar sebagai urusan sehari-hari.

Skenario umpan-Skema rekayasa sosial ini mengetahui bahwa jika Anda memberikan sesuatu yang diinginkan orang, banyak orang akan terpancing. Skema ini sering ditemukan di situs Peer-to-Peer yang menawarkan pengunduhan sesuatu seperti film atau musik baru yang sedang hangat. Namun skema tersebut juga ditemukan di situs jejaring sosial, situs web jahat yang Anda temukan melalui hasil pencarian, dan sebagainya. Atau, skema tersebut mungkin muncul sebagai penawaran yang sangat bagus di situs rahasia, situs lelang, dll. Untuk menghilangkan kecurigaan Anda, Anda dapat melihat penjual memiliki peringkat yang bagus (semuanya direncanakan dan dibuat sebelumnya). Orang-orang yang terpancing bisa saja terinfeksi perangkat lunak berbahaya yang dapat menghasilkan sejumlah eksploitasi baru terhadap diri mereka sendiri dan kontak mereka, mungkin kehilangan uang tanpa menerima barang yang dibeli, dan, jika mereka cukup bodoh untuk membayar dengan cek, mungkin akan menemukan rekening bank mereka kosong[12],[13].

Jawaban atas pertanyaan yang belum pernah Anda miliki-Penjahat mungkin berpura-pura menanggapi 'permintaan bantuan' Anda dari perusahaan sambil juga menawarkan lebih banyak bantuan. Mereka memilih perusahaan yang digunakan jutaan orang seperti perusahaan perangkat lunak atau bank. Jika Anda tidak menggunakan produk atau layanan tersebut, Anda akan mengabaikan email, panggilan telepon, atau pesan tersebut, namun jika Anda kebetulan menggunakan layanan tersebut, kemungkinan besar Anda akan merespons karena Anda mungkin menginginkan bantuan untuk suatu masalah[14],[15]

Misalnya, meskipun Anda tahu bahwa pada awalnya Anda tidak mengajukan pertanyaan, Anda mungkin mengalami masalah dengan sistem operasi komputer Anda dan Anda memanfaatkan kesempatan ini untuk memperbaikinya. Gratis! Saat Anda merespons, Anda telah mempercayai cerita si penjahat, memberi mereka kepercayaan Anda dan membuka diri untuk dieksploitasi. Perwakilan tersebut, yang sebenarnya adalah penjahat, perlu 'mengotentikasi Anda', apakah Anda sudah masuk ke 'sistem mereka' atau, apakah Anda sudah masuk ke komputer Anda dan memberi mereka akses jarak jauh ke komputer Anda sehingga mereka bisa 'memperbaikinya'. Anda, atau memberi tahu Anda perintahnya sehingga Anda dapat memperbaikinya sendiri dengan bantuan mereka—di mana beberapa perintah yang mereka minta untuk Anda masukkan akan membuka jalan bagi penjahat untuk kembali ke komputer Anda nanti.

Menciptakan ketidakpercayaan-Beberapa rekayasa sosial bertujuan untuk menciptakan ketidakpercayaan, atau memulai konflik; Hal ini sering kali dilakukan oleh orang-orang yang Anda kenal dan sedang marah kepada Anda, namun hal ini juga dilakukan oleh orang-orang jahat yang hanya mencoba membuat kekacauan, orang-orang yang ingin terlebih dahulu menciptakan ketidakpercayaan dalam pikiran Anda terhadap orang lain sehingga mereka kemudian dapat bertindak sebagai a pahlawan dan mendapatkan kepercayaan Anda, atau oleh pemeran yang ingin memanipulasi informasi dan kemudian mengancam Anda dengan pengungkapannya. Bentuk rekayasa sosial ini sering dimulai dengan mendapatkan akses ke akun email atau akun komunikasi lain di klien IM, jejaring sosial, obrolan, forum, dll. Mereka melakukannya dengan meretas, rekayasa sosial, atau sekadar menebak kata sandi yang sangat lemah. Orang jahat kemudian dapat mengubah komunikasi sensitif atau pribadi (termasuk gambar dan audio) menggunakan teknik pengeditan dasar dan meneruskannya ke orang lain untuk menciptakan drama, ketidakpercayaan, rasa malu, dll. Mereka mungkin membuatnya tampak seperti terkirim secara tidak sengaja, atau tampak seperti mereka memberi tahu Anda apa yang 'sebenarnya' sedang terjadi. Alternatifnya, mereka dapat menggunakan materi yang diubah untuk memeras uang baik dari orang yang mereka retas atau dari penerima yang diduga. Ada ribuan variasi serangan rekayasa sosial. Satu-satunya batasan dalam jumlah cara mereka dapat merekayasa pengguna secara sosial melalui eksploitasi semacam ini adalah imajinasi penjahat. Dan Anda mungkin mengalami berbagai bentuk eksploitasi dalam satu serangan. Kemudian penjahat tersebut kemungkinan besar akan menjual informasi Anda kepada orang lain sehingga mereka juga dapat melakukan eksploitasi terhadap Anda, teman Anda, teman teman Anda, dan seterusnya ketika penjahat memanfaatkan kepercayaan orang yang salah tempat.

Jangan menjadi korban-Meskipun serangan phishing merajalela, berumur pendek, dan hanya memerlukan sedikit pengguna untuk mengambil umpan agar kampanye berhasil, ada beberapa metode untuk melindungi diri Anda sendiri. Kebanyakan tidak memerlukan lebih dari sekedar memperhatikan detail di depan Anda. Ingatlah hal-hal berikut untuk menghindari phishing.

Kiat yang Perlu Diingat:-Pelan - pelan. Spammer ingin Anda bertindak terlebih dahulu dan berpikir kemudian. Jika pesan tersebut menyampaikan rasa urgensi atau menggunakan taktik penjualan bertekanan tinggi, bersikaplah skeptis; jangan biarkan urgensinya memengaruhi tinjauan cermat Anda.

Teliti faktanya-Curiga terhadap pesan apa pun yang tidak diminta. Jika email tersebut sepertinya berasal dari perusahaan yang Anda gunakan, lakukan riset sendiri. Gunakan mesin pencari untuk membuka situs perusahaan sebenarnya, atau direktori telepon untuk menemukan nomor telepon mereka. Jangan biarkan tautan mengendalikan tempat Anda mendarat. Tetap memegang kendali dengan menemukan sendiri situs web tersebut menggunakan mesin pencari untuk memastikan Anda mendarat di tempat yang Anda inginkan. Mengarahkan kursor ke tautan di email akan menampilkan URL sebenarnya di bagian bawah, tetapi URL palsu yang bagus masih bisa membuat Anda salah. Pembajakan email merajalela. Peretas, pengirim spam, dan insinyur sosial yang mengambil alih kendali akun email seseorang (dan akun komunikasi lainnya) semakin merajalela. Begitu mereka mengontrol akun email, mereka memangsa kepercayaan dari kontak orang tersebut. Meskipun pengirimnya tampaknya adalah seseorang yang Anda kenal, jika Anda tidak mengharapkan email berisi tautan atau lampiran, tanyakan kepada teman Anda sebelum membuka tautan atau mengunduh. Waspadai unduhan apa pun. Jika Anda tidak mengenal pengirimnya secara pribadi DAN mengharapkan file dari mereka, mengunduh apa pun adalah suatu kesalahan. Tawaran asing itu palsu. Jika Anda menerima email dari lotere atau undian asing, uang dari kerabat yang tidak dikenal, atau permintaan untuk mentransfer dana dari negara asing untuk mendapatkan bagian dari uang tersebut, dijamin itu adalah penipuan.

Cara Melindungi Diri Anda- Hapus segala permintaan informasi keuangan atau kata sandi. Jika Anda diminta membalas pesan dengan informasi pribadi, itu adalah penipuan. Tolak permintaan bantuan atau tawaran bantuan. Perusahaan dan organisasi yang sah tidak menghubungi Anda untuk memberikan bantuan. Jika Anda tidak secara khusus meminta bantuan dari pengirim, pertimbangkan tawaran apa pun untuk 'membantu' memulihkan nilai kredit, membiayai kembali rumah, menjawab pertanyaan Anda, dll., sebagai penipuan. Demikian pula, jika Anda menerima permintaan bantuan dari badan amal atau organisasi yang tidak memiliki hubungan dengan Anda, hapus permintaan tersebut. Untuk memberi, carilah sendiri organisasi amal yang memiliki reputasi baik untuk menghindari penipuan. Setel filter spam Anda ke tinggi . Setiap program email memiliki filter spam. Untuk menemukannya, lihat opsi pengaturan Anda, dan setel ke tinggi–ingatlah untuk memeriksa folder spam Anda secara berkala untuk melihat apakah email yang sah secara tidak sengaja terperangkap di sana. Anda juga dapat mencari panduan langkah demi langkah untuk menyetel filter spam dengan menelusuri nama penyedia email Anda ditambah frasa 'filter spam'. Amankan perangkat komputasi Anda . Instal perangkat lunak anti-virus, firewall, filter email, dan selalu diperbarui. Atur sistem operasi Anda agar diperbarui secara otomatis, dan jika ponsel cerdas Anda tidak diperbarui secara otomatis, perbarui secara manual setiap kali Anda menerima pemberitahuan untuk melakukan pembaruan. Gunakan alat anti-phishing yang ditawarkan oleh browser web Anda atau pihak ketiga untuk mengingatkan Anda akan risiko. Basis data ancaman Webroot memiliki lebih dari 600 juta domain dan 27 miliar URL yang dikategorikan untuk melindungi pengguna dari ancaman berbasis web. Kecerdasan ancaman yang mendukung semua produk kami membantu Anda menggunakan web dengan aman, dan solusi keamanan seluler kami menawarkan penjelajahan web yang aman untuk mencegah serangan phishing yang berhasil.

#### 4. KESIMPULAN DAN SARAN

Kesimpulan yang dapat diambil setelah melakukan pengabdian masyarakat, antara lain:

1. Data mining, data science, merupakan salah satu cabang ilmu yang sangat baik diterapkan dalam lini bisnis apapun
2. Social engineering merupakan salah satu cabang ilmu untuk dapat membantu kita dalam mengatasi kejahatan cyber. Penerapan ini akan dapat membantu kita untuk terhindari dari kejahatan cyber
3. Menggabungkan dua tempat pengabdian merupakan salah satu Teknik untuk dapat meningkatkan kompetensi sumber daya manusia dan akan dapat mengubah banyak paradigma secara signifikan

#### UCAPAN TERIMA KASIH

Terima kasih kepada Dhadhu Board game café yang telah memberikan kesempatan kepada kami agar dapat menerapkan pengabdian masyarakat yang sudah kami rancang, dan terima kasih juga kepada SMAN 3, Semarang yang sudah menerima kami sehingga kami dapat menjelaskan contoh kasus nyata

#### DAFTAR PUSTAKA

- [1] I. Gamayanto *et al.*, *Social Media Profiling*.
- [2] S. L. Lim, J. Sreevalsan-Nair, and B. S. Daya Sagar, "Multispectral data mining: A focus on remote sensing satellite images," *WIREs Data Mining and Knowledge Discovery*, vol. 14, no. 2, p. e1522, 2024, doi: 10.1002/widm.1522.
- [3] S. Sweta, "An Overview of Sentiment Analysis and Educational Data Mining," in *Sentiment Analysis and its Application in Educational Data Mining*, S. Sweta, Ed., Singapore: Springer Nature, 2024, pp. 1–18. doi: 10.1007/978-981-97-2474-1\_1.
- [4] "A survey of episode mining - Ouarem - 2024 - WIREs Data Mining and Knowledge Discovery - Wiley Online Library." Accessed: Jun. 06, 2024. [Online]. Available: <https://wires.onlinelibrary.wiley.com/doi/abs/10.1002/widm.1524>
- [5] H. S. Moula, S. H. Yaghoubyan, R. Malekhosseini, and K. Bagherifard, "Customer type discovery in hotel revenue management: a data mining approach," *J Revenue Pricing Manag*, Apr. 2024, doi: 10.1057/s41272-024-00474-w.
- [6] L. Jian, K. Shao, Y. Liu, J. Li, and X. Liang, "OEC: an online ensemble classifier for mining data streams with noisy labels," *Data Min Knowl Disc*, vol. 38, no. 3, pp. 1101–1124, May 2024, doi: 10.1007/s10618-023-00990-0.
- [7] "Difference between Data mining and Data Science - Javatpoint," [www.javatpoint.com](http://www.javatpoint.com). Accessed: Jun. 06, 2024. [Online]. Available: <https://www.javatpoint.com/data-mining-vs-data-science>
- [8] L. Igual and S. Seguí, "Introduction to Data Science," in *Introduction to Data Science: A Python Approach to Concepts, Techniques and Applications*, L. Igual and S. Seguí, Eds., Cham: Springer International Publishing, 2024, pp. 1–4. doi: 10.1007/978-3-031-48956-3\_1.
- [9] T. Bratanić, *Graph Algorithms for Data Science: With Examples in Neo4j*. Simon and Schuster, 2024.
- [10] N. Hollmann, S. Müller, and F. Hutter, "Large Language Models for Automated Data Science: Introducing CAAFE for Context-Aware Automated Feature Engineering," *Advances in Neural Information Processing Systems*, vol. 36, pp. 44753–44775, Dec. 2023.
- [11] "What is Social Engineering? Examples and." Accessed: Jun. 06, 2024. [Online]. Available: <https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering>

- [12]“Cognition in Social Engineering Empirical Research: A Systematic Literature Review | ACM Transactions on Computer-Human Interaction.” Accessed: Jun. 06, 2024. [Online]. Available: <https://dl.acm.org/doi/full/10.1145/3635149>
- [13]N. Tsinganos, P. Fouliras, I. Mavridis, and D. Gritzalis, “CSE-ARS: Deep Learning-Based Late Fusion of Multimodal Information for Chat-Based Social Engineering Attack Recognition,” *IEEE Access*, vol. 12, pp. 16072–16088, 2024, doi: 10.1109/ACCESS.2024.3359030.
- [14]A.-M. Gagné-Julien, “Beyond Conceptual Analysis: Social Objectivity and Conceptual Engineering to Define Disease,” *The Journal of Medicine and Philosophy: A Forum for Bioethics and Philosophy of Medicine*, vol. 49, no. 2, pp. 147–159, Apr. 2024, doi: 10.1093/jmp/jhae002.
- [15]M. G. Isaac, “Post-truth conceptual engineering,” *Inquiry*, vol. 67, no. 1, pp. 199–214, Jan. 2024, doi: 10.1080/0020174X.2021.1887758.