JUSTIN
Jurnal Sistem dan Teknologi Informasi
p-ISSN : 2460-3562 / e-ISSN : 2620-8989
DOI: 10.26418/justin.v10i1.44280
Vol. 10, No. 1, Januari 2022

Mencegah Serangan Rekayasa Sosial dengan Human Firewall

Muhammad Zulfahmi Huwaidi[#1], Senie Destya[#2]
[#] *Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta*
Jl. Ring Road Utara, Ngringin, Condongcatur, Kec. Depok, Kab. Sleman, Daerah Istimewa Yogyakarta, Indonesia.
[1]Muhammad.huwaidi@students.amikom.ac.id
[2]Seniedestya@amikom.ac.id

Abstrak

Manusia adalah elemen paling rentan yang ada pada sistem keamanan informasi. Seringkali orang menganggap bahwa apa yang dibagikan di dunia maya atau dunia siber adalah hal yang tidak penting, tetapi bagi sebagian orang, data dan informasi yang sangat banyak di internet bisa digunakan untuk tindak kejahatan yang membuat kerugian yang besar. Salah satu teknik yang digunakan pelaku tindak kejahatan dunia siber disebut dengan teknik rekayasa sosial. Hal ini menuntut orang-orang agar selalu waspada dan berhati-hati karena pada dasarnya serangan ini memanfaatkan dan maminupalisi manusia agar memberikan data dan informasi tanpa disadari. Pemdekatan fisik dan teknik yang berarti serangan rekayasa sosial bisa terjadi di dunia siber maupun di dunia nyata. Maka dari itu dibutuhkan sebuah model atau panduan yang dapat meningkatkan kesadaran kemanan manusia itu sendiri. *Human Firewall*, bentuk pertahanan diri yang didapatkan dari memingkatkan kesadaran kemanan data dan informasi melalui pemilihan keputusan yang tepat saat serangan rekayasa sosial terjadi.

Kata kunci: Rekayasa Sosial, *Human Firewall*, Pohon Keputusan, Keamanan Informasi, Keamanan Siber

Preventing Social Engineering Attacks with Human Firewalls

Abstract

Humans are the most vulnerable element that exists in information security systems. Often people assume that what is shared in cyberspace or cyberspace is not important, but for some people, a lot of data and information on the internet can be used for crimes that make a huge loss. One of the techniques used by cybercriminals is called social engineering techniques. This requires people to always be vigilant and cautious because basically these attacks exploit and maminupalisi humans to provide data and information unwittingly. Physical and engineering approaches that mean social engineering attacks can occur in the cyber world as well as in the real world. Therefore, a model or guide is needed that can raise awareness of human security itself. Human Firewall, a form of self-defense obtained from raising awareness of data and information security through the right decision-making when social engineering attacks occur.

Keywords: Social Engineering Attacks, Human Firewall, Decision Trees, Information Security, Cyber Security.

I. PENDAHULUAN

Perkembangan teknologi dan informasi sangatlah cepat, mulai dari proses pembuatan teknologi itu sendiri hingga proses pertukaran informasi di berbagai media *online*. Hal ini dipicu oleh ketatnya persaingan antara individu atau kelompok yang terus menciptakan inovasi pada bidang teknologi dan informasi. BYOD *(Bring Your Own Device)*, istilah ini muncul 10 tahun yang lalu menggambarkan tentang kondisi dimana setiap orang bisa mengerjakan sesuatu tanpa terhalang oleh jarak dan waktu karena teknologi yang semakin hari semakin canggih sehingga dapat dibawa kemana saja. [1] Semua bisa diakses dengan mudah dimana dan kapan saja. Hal tersebut menimbulkan kekhawatiran bagi para pakar kemanan teknologi dan informasi, pasalnya ketika semua orang dapat mengakses informasi dengan sangat mudah, disaat yang bersamaan tidak sedikit pelaku kejahatan memanfaatkan situasi ini untuk mendapatkan informasi penting dari pengguna yang kemudian digunakan untuk kepentingan sendiri, seperti masuk ke sebuah sistem, membuat akun palsu, dan masih banyak lagi. Teknik yang digunakan pelaku kejahatan siber sangatlah beragam seperti *phising*, *spam*, dan *social engineering*. [2] Tercatat bahwa negara Indonesia berada diperingkat ke-2 dunia kejahatan kasus siber [3] Kejahatan siber di Indonesia bisa sangat banyak dikarenakan banyak masyarakat yang belum paham tentang bagaimana bentuk kejahatan di dunia siber.

Dalam berbagai tulisan dinyatakan bahwa manusia adalah elemen yang paling rentan dalam sistem keamanan. [4], [5] Teknik paling efektif yang digunakan oleh pelaku kejahatan siber yaitu rekayasa sosial. Rekayasa sosial atau biasa dikenal dengan sebutan *social engineering* adalah sebuah teknik yang memanfaatkan kelemahan individu (manusia) untuk memperoleh informasi yang digunakan untuk menerobos sistem keamanan. Mayoritas masyarakat tidak mengetahui cara kerja dari teknik ini sehingga para pelaku kejahatan siber memperoleh informasi yang

diinginkan dengan mudah, bahkan sebagian korban serangan teknik rekayasa sosial tidak sadar bahwa dirinya sedang menjadi target dari pelaku penyerangan rekayasa sosial. [6]

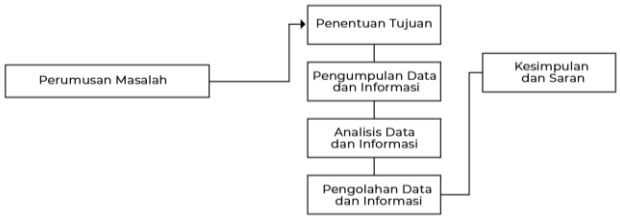
Serangan rekayasa sosial pada umumnya menyiratkan interaksi langsung dengan individu lain baik itu bertatap muka langsung atau secara *online*. Pada saat berintaraksi inilah pelaku kejahatan yang menggunakan teknik rekayasa sosial mempengaruhi psikologi korban. Pemahaman yang cukup tentang pemicu-pemicu psikologis dapat mencegah pelaku kejahatan rekayasa sosial. [7] Kasus penyerangan menggunakan teknik rekayasa sosial pertama kali dilakukan oleh Kevin Mitnick yang berasal dari negara Amerika. Mitnick seorang *hacker* yang hampir tidak menyentuh komputer dalam mengeksploitasi kelemahan targetnya dengan kata lain Mitnick menggunakan teknik rekayasa sosial sepenuhnya. [8] Kevin Mitnick kemudian ditangkap pada tahun 1995 yang kemudian memberikan pernyataan dalam bukunya *The Art of Deception* bahwa *Social Engineering* adalah bagian yang sederhana dalam pendekatannya. Para pelaku kejahatan dunia siber yang menggunakan teknik rekayasa sosial sangat mahir memanipulasi targetnya dengan berpura-pura menjadi sosok penting dan akrab agar target tidak curiga.

Tidak banyak yang bisa mengetahui proses serangan rekayasa sosial terjadi. Maka dari itu diperlukan perlindungan yang dibentuk dari diri sendiri untuk mengatasi "mata rantai terlemah" pada sistem keamanan yaitu manusia. [8] Perlindungan ini dinamakan *human firewall*. Sama halnya seperti *firewall* yang melindungi jaringan komputer, *human firewall* adalah sebuah bentuk perlindungan yang sengaja dibentuk untuk mencegah berbagai serangan dari *hacker*, terutama serangan yang menggunakan teknik *social engineering*. Sebagaimana dijelaskan pada paragraf sebelumnya bahwa manusia adalah bagian yang rentan pada sistem keamanan. Pernyataan tersebut sangatlah jelas mengingat bahwa manusia adalah makhluk sosial yang tentu akan berfikir sebelum melakukan tindakan. Peneliti akan membentuk *human firewall* pada manusia itu sendiri dengan menggunakan metode Pohon Keputusan (*decision trees*).

II. METODOLOGI

Kajian ini menggunakan metode pohon keputusan (*decision trees*). Metode pohon keputusan digunakan untuk memberikan keputusan yang tepat untuk mencegah serangan *social engineering*. Pengambilan keputusan manuisa adalah hal yang sangat kompleks. Tiap keputusan yang dibuat tentu memiliki lebih dari satu pilihan yang ideal menurut manusia itu sendiri dan keputusan yang telah dibuat pasti akan berbeda dengan manusia yang lainnya. [9]

Penelitian sebelumnya menggunakan metode *decision trees* untuk mendeteksi serangan *social engineering*. Hasil akhirnya berupa model deteksi serangan *social engineering* atau disebut juga dengan *Social Engineering Attacks Detection Model (SEADM)*. [6]



Gambar 1. Alur penelitian

Proses alur penelitian pada Gambar.1 diawali dengan perumusan masalah yaitu mencegah serangan social engineering dengan memutus rantai terlemah dalam sistem keamanan yaitu manusia. [4] Tujuan dilakukannya penelitian ini adalah untuk meningkatkan kehati-hatian dan pengambilan keputusan yang akurat guna mencegah serangan *social engineering*. Adapun proses pengumpulan data dan informasi menggunakan *literature review* untuk menemukan beberapa referensi dan penelitian terkait. Kemudian yang terakhir adalah proses analisis data dan pengolahan data, yang berarti data yang sebelumnya sudah dikumpulkan kemudian diolah menjadi sebuah penelitian yang terbaru yaitu pembentukan *Human Firewall* dengan menggunakan Pohon Keputusan seperti yang dijelaskan pada paragraf sebelumnya. Untuk membuat sebuah model yang nantinya akan membentuk *human firewall*, beberapa teknik pendekatan yang ada pada serangan rekayasa sosial terlebih dulu dikelompokkan menjadi 2 kelompok yaitu pendekatan fisik dan pendekatan teknik. [7]

Pendekatan fisik berarti pendekatan dimana penyerang melakukan berbagai jenis tindakan untuk mendekati target dan mengumpulkan informasi. Informasi yang dikumpulkan pada umumnya berupa nomor telefon, tanggal lahir, nama lengkap, dan yang berhubungan dengan data pribadi lainnya. Tidak hanya itu, pendekatan fisik yang sering dilakukan penyerang adalah teknik menelusuri sampah berkas organisasi perusahaan. [10] Sedangkan untuk pendekatan teknik, adalah pendekatan dengan tipe serangan yang dilakukan melalui internet. Para pelaku kejahatan rekayasa sosial sangat tertarik dengan informasi yang terdapat pada internet terutama pada sosial media. Seringkali banyak manusia yang tidak sadar memasang informasi penting pada sosial media mereka yang mengakibatkan terjadinya proses pengumpulan informasi oleh penyerang tanpa disadari. Penyerang menggunakan browser untuk mencari informasi korban.

III. HASIL DAN PEMBAHASAN

Seperti yang dijelaskan untuk membentuk sebuah *Human Firewall* pada individu dibutuhkan sebuah model sebagai pedoman untuk membentuk *Human Firewall* itu sendiri. Memanfaatkan pohon keputusan atau decision trees agar dapat dikelola dan menghasilkan pedoman yang dapat membantuk proses pengambilan keputusan kepada individu.

Serangan rekayasa sosial mempunyai beberapa jenis pendekatan, pendekatan fisik dan teknik adalah

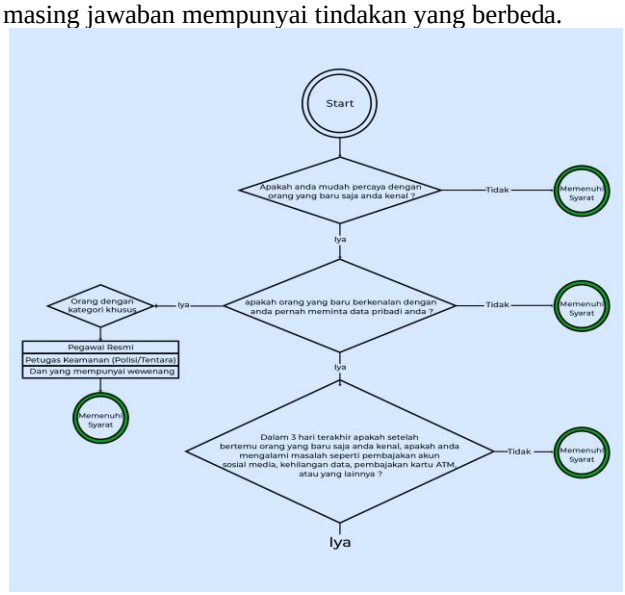
pendekatan yang paling umum dan paling sering digunakan para pelaku kejahatan rekayasa sosial. Maka dari itu penulis menggabungkan kedua pendekatan ini untuk mempermudah proses pengambilan keputusan yang kemudian membentuk Human Firewall pada invidu. Seperti yang ditunjukkan pada gambar.2 model penuh dimulai dengan beberapa pertanyaan sederhana yang seringkali digunakan pelaku kejahatan rekayasa sosial.

A. Pendekatan Fisik

TABEL I
PERTANYAAN MODEL PENDEKATAN FISIK

No	Pertanyaan
1	Apakah anda mudah percaya dengan orang yang baru saja anda kenal ?
2	Apakah orang yang baru berkenalan dengan anda pernah meminta data dan informasi pribadi anda ?
3	Dalam beberapa hari terakhir setelah bertemu orang yang baru saja anda kenal, apakah anda mengalami masalah seperti pembajakan akun sosial media atau yang berhubungan dengan dunia maya/siber ?

Pada tabel 1 dipaparkan 3 pertanyaan yang dikumpulkan dari penelitian terkait dengan serangan rekayasa sosial menggunakan pendekatan fisik yang paling umum. Selanjutnya pertanyaan tersebut akan dijawab oleh individu sesuai dengan kejadian yang sebenarnya. Ada 2 jawaban yang ditunjukkan pada gambar 2 yaitu 'Iya' dan 'Tidak' yang kemudian masing-masing jawaban mempunyai tindakan yang berbeda.



Gambar 2. Model pohon keputusan untuk mencegah serangan rekayasa social (Pendekatan Fisik)

1) Apakah anda mudah percaya dengan orang yang baru saja anda kenal ? : Pelaku kejahatan yang menggunakan teknik social engineering atau rekayasa sosial memang sudah menjadi keahliannya untuk memanipulasi dan memanfaatkan manusia. Langkah pada area kiri (gambar 2) adalah pohon keputusan untuk mencegah serangan rekayasa sosial yang menggunakan pendekatan fisik. Jika individu tidak mudah percaya dengan orang yang baru saja dikenalnya maka pada langkah ini dapat dikatakan memenuhi syarat dan jika sebaliknya, maka langsung lanjut ke langkah berikutnya untuk memastikan kriteria orang yang baru dikenal tersebut memiliki keperluan khusus atau tidak.

2) Apakah orang yang baru berkenalan dengan anda pernah meminta data pribadi anda ? : Data pribadi memang mempunyai kegunaan tersendiri bagi para pelaku serangan rekayasa sosial. Mereka mampu memanfaatkan data dan informasi yang mereka dapatkan untuk melakukan tindakan kejahatan. Pada langkah ini individu harus mengenali orang yang baru dikenalnya tersebut memang dapat dipercaya atau tidak. Jika individu dimintai data pribadi oleh orang yang baru saja dikenalnya, maka ada baiknya memeriksa tampilan luar orang tersebut. Pada gambar 2 terdapat beberapa kategori orang yang jika meminta data pribadim harus dipenuhi, seperti pegawai resmi kantor/perusahaan, petugas keamanan resmi, dan orang-orang yang memang mempunyai hak untuk meminta data pribadi. Perlu diketahui bahwa kemungkinan pelaku serangan rekayasa sosial menyamar menjadi pegawai resmi. Teknik ini dinamakan pretexting, dimana pelaku berpura-pura menjadi seorang ahli atau pegawai resmi dan menciptakan situasi yang mendesak korban untuk meminta pertolongan darinya kemudian ketika korban meminta tolong, pelaku langsung memanfaatkan situtasi ini untuk memintai data pribadi dari korban. [11], [12]

3) Dalam 3 hari terakhir, apakah setelah bertemu dengan orang yang baru saja anda kenal, apakah anda mengalami masalah seperti pembajakan akun sosial media, kehilangan data, pembajakan kartu ATM, atau yang lainnya ? : Sama seperti langkah yang ada pada area kanan dimana individu akan memeriksa apakah pada 3 hari setelah bertemu dengan orang yang baru saja dikenalnya dan meminta data pribadi, individu tersebut mengalami masalah seperti yang disebutkan pada langkah ini. Jika iya, maka segera lanjutkan ke langkah berikutnya untuk melakukan tindakan pengamanan yang telah dijelaskan pada poin berikutnya.

B. Pendekatan Teknik

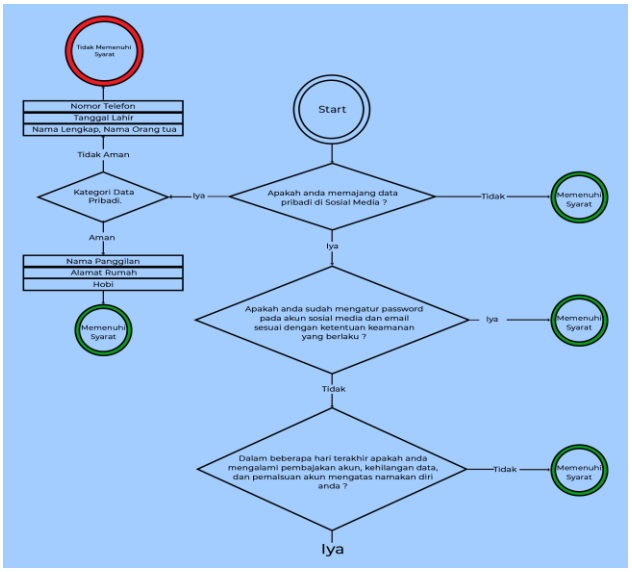
TABEL II
PERTANYAAN MODEL PENDEKATAN TEKNIK

No	Pertanyaan
1	Apakah anda memajang/ memposting/ membagikan data dan informasi pribadi anda di media sosial ?
2	Apakah anda sudah mengatur password pada akun sosial media dan email sesuai dengan ketentuan keamanan yang berlaku ?
3	Dalam beberapa hari terakhir, apakah anda mengalami pembajakan akun, pemalsuan akun sosial media atau email mengatas namakan diri anda ?

1) *Apakah anda memajang/ memposting/ membagikan data dan informasi pribadi anda di media sosial ? :* Model yang sudah jadi pada gambar.3 yaitu dengan pertanyaan, apakah anda membagikan data pribadi di Sosial Media ? sangat banyak yang menganggap

membagikan sesuatu di sosial media adalah hal yang biasa saja. Tetapi berbeda dengan yang dikemukakan bahwa serangan dengan pendekatan teknik pada umumnya berasal dari internet. Jika individu tersebut tidak membagikan data dan informasi yang menurutnya aman, maka pada pertanyaan ini, individu tersebut dikategorikan memenuhi syarat dan berhak lanjut ke langkah berikutnya. Jika invidu tersebut terlanjur membagikan data dan informasinya pada media sosial, maka langkah yang dapat diambil adalah melihat terlebih dahulu data dan informasi apa saja yang boleh dibagikan. Nama lengkap, tanggal lahir. Nama orang tua, nomor telefon dan email adalah beberapa informasi pribadi yang sering dicuri [13], [14] maka dari itu beberapa informasi yang tersebut sangat tidak boleh dibagikan. Kemudian informasi seperti nama pangggilan, alamat rumah, dan Hobi boleh dibagikan. Jika individu membagikan informasi yang tidak aman maka harus segera melakukan tindakan menghapus dan menghilangkan informasi tersebut pada sosial media, jika individu tersebut membagikan informasi yang aman maka syarat pada langkah pertama terpenuh dan lanjut ke langkah berikutnya.

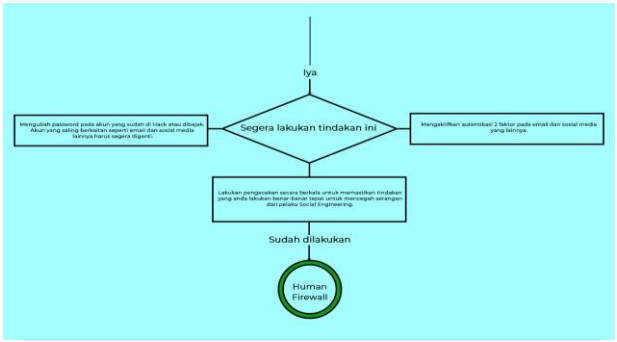
2) *Apakah anda sudah mengatur password pada akun sosial media dan email sesuai dengan ketentuan keamanan yang berlaku ? :* Kesalahan paling umum yang dilakukan seseorang adalah memilih kata sandi yang lemah dan umum. Penulisan password yang paling mudah ditebak adalah '123456', 'password' dan '12345678'. [15] langkah ini adalah yang paling penting, karena teknik yang paling popular digunakan untuk mengumpulkan informasi tentang password yang terdapat pada akun sosial media dan email. Pada langkah ini jika individu sudah mengatur password sesuai dengan ketentuan keamana yang berlaku, maka individu tersebut sudah memenuhi syarat dan berhak melanjutkan ke langkah berikutnya, Jika tidak, maka individu tersebut wajib mengganti password sesuai dengan ketentuan kemanan yang berlaku seperti, penggunaan huruf besar dan kecil, karakter khusus, serta angka. Jangan menyertakan tanggal lahir pada password, dan juga jangan menggunakan password dengan variable singkat. [15].



Gambar 3. Model pohon keputusan untuk mencegah serangan rekayasa social (Pendekatan Teknik)

3) Dalam 3 hari terakhir apakah anda mengalami pembajakan akun, kehilangan data, atau pemalsuan akun mengatas namanakan diri anda ? : Langkah terakhir adalah memastikan apakah individu tersebut sudah benar-benar aman dalam artian serangan rekayasa sosial dengan pendekatan teknik tidak berhasil dilakukan. Jika kedua langkah sebelumnya memenuhi syarat, maka kecil kemungkinan serangan rekyasa sosial tersebut berhasil dan dalam beberapa hari terakhir tidak mengalami masalah seperti pada poin yang disebutkan, maka individu sudah memenuhi syarat dan melanjutkan ke langkah selanjutnya. Tetapi jika individu kehilangan data, pembajakan akun, atau pemalsuan identitas (Fake Account) pada sosial media, karena dengan informasi pribadi yang telah dicuri para pelaku kejahatan rekayasa sosial membuat akun palsu dengan sangat mudah [16] maka segera lakukan tindakan selanjutnya yaitu mengaktifkan autentikasi 2 faktor pada email dan sosial media. Tidak hanya itu, mengganti password pada semua akun atau user pada komputer sangat diperlukan.

C. Tindakan Pencegahan



Gambar 4. Tindakan pencegahan dalam bentuk pohon keputusan.

Langkah ini adalah tindakan pencegahan jika individu sudah menjadi korban dari serangan rekayasa sosial. Sangat banyak dampak negatif dan merugikan yang

didapatkan seperti, kehilangan data, pemalsuan akun, bahkan kehilangan sejumlah uang. Sebelum terlambat, tindakan pencegahan ini sebaiknya dilakukan dengan baik. Pertama, mengubah password pada akun yang sudah dihack atau dibajak, akun yang saling berkaitan seperti email dan sosial media harus segera diganti. Kedua. Mengaktifkan autentikasi 2 faktor pada email, sosial media, dan perangkat. Ketiga, lakukan pengecekan secara berkala untuk memastikan tindakan yang dilakukan benar-benar tepat untuk mencegah dan menghentikan serangan ini.

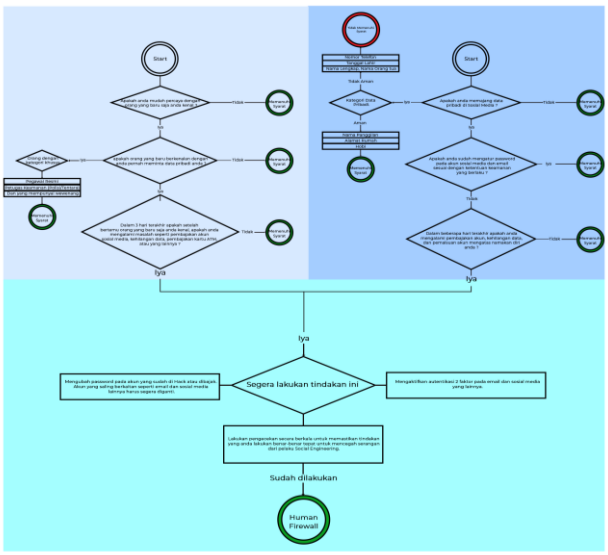
Tindakan pencegahan yang pertama adalah, mengaktifkan autentikasi 2 faktor pada email dan media sosial yang lainnya. Banyak orang yang hanya menggunakan email untuk kepentingan melengkapi data untuk pendaftaran pada media sosial lainnya. Disini para pelaku rekayasa sosial mengumpulkan informasi, menanyai korban dengan meminta email. Ada banyak cara yang mereka gunakan untuk mengelabui korban hanya dengan menggunakan email, salah satunya *phising* [2]. Teknik yang paling memungkinkan untuk menggiring korban kepada hal yang tidak diinginkan. Skenarionya sebagai berikut, ketika korban sudah dikirim email berisi pesan yang mengandung konteks phising oleh pelaku, kemudian korban terpancing untuk membuka email phising tersebut yang bisa jadi berisi halaman web yang meminta data penting dari korban, besar kemungkinan langkah selanjutnya yang dilakukan penyerang adalah langsung membobol masuk ke akun email anda. Maka dari itu, autentikasi 2 faktor pada sosial media terkhusus email sangatlah penting. Ketika akun email korban sudah diretas maka autentikasi 2 faktor sangat mungkin untuk memberhentikan peretas tersebut. Karena autentikasi 2 faktor akan memberitahu bahwa ada aktivitas yang mencurigakan pada akun email korban.

Kemudian tindakan pencegahan yang kedua adalah mengubah password lama yang sudah diketahui oleh pelaku rekayasa sosial. Password yang relative aman terdiri dari 15 karakter dengan kombinasi huruf, angka, dan karakter lainnya. [17]

Terakhir adalah pengecekan secara berkala, jangan sampai ada serangan yang berkelanjutan karena pelaku rekayasa sosial susah untuk dideteksi tanpa pengetahuan yang cukup.

IV. KESIMPULAN

Hasil dari penelitian ini berupa model yang memanfaatkan *decision trees* yang ada pada gambar 5 untuk membentuk *Human Firewall*. Model yang ada pada pembahasan sebelumnya berguna untuk membentuk Human Firewall karena pada dasarnya Human Firewall akan terbentuk jika kesadaran keamanan dari individu sudah memenuhi syarat.



Gambar 5. Model untuk membangun *human firewall*.

UCAPAN TERIMA KASIH

Peneliti mengucapkan terimakasih kepada teman-teman dan orang tua yang mendukung dalam penelitian ini. Tidak lupa juga kepada dosen pembimbing yang selalu sabar menuntun peneliti agar selalu rajin dan tidak bermalas-malasan.

DAFTAR PUSTAKA

[1] L. Gerhold, G. Bartl, and N. Haake, “Security culture 2030. How security experts assess the future state of privatization, surveillance, security technologies and risk awareness in Germany,” *Futures*, vol. 87, pp. 50–64, 2017.

[2] S. Destya, “Model Pengukuran Tingkat Kesadaran Keamanan,” pp. 19–24, 2018.

[3] “Kementerian Komunikasi dan Informatika.” [Online]. Available: https://kominfo.go.id/index.php/content/detail/3415/Kominfo+%3A+Pengguna+Internet+di+Indonesia+63+Juta+Orang/0/berita_satker.

[4] J. Scheeres, “Establishing the Human Firewall: Reducing an Individual’s Vulnerability to Social Engineering Attacks,” p. 49, Mar. 2008.

[5] G. Orgill, G. Romney, M. Bailey, and P. Orgill, *The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems*. 2004.

[6] F. Mouton, L. Leenen, and H. S. Venter, “Social Engineering Attack Detection Model: SEADMv2,” *Proc. - 2015 Int. Conf. Cyberworlds, CW 2015*, pp. 216–223, 2016.

[7] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, “Advanced social engineering attacks,” *J. Inf. Secur. Appl.*, vol. 22, pp. 113–122, 2015.

[8] M. Jensen, R. Wright, A. Durcikova, and S. Karumbaiah, “Building the Human Firewall: Combating Phishing through Collective Action of Individuals Using Leaderboards,” *SSRN Electron. J.*, Jan. 2020.

[9] A. V. Robins, L. E. Margulieux, and B. B. Morrison, *Cognitive Sciences for Computing Education*. 2019.

[10] S. Granger, “SecurityFocus HOME Infocus : Social Engineering Fundamentals , Part II : Combat SecurityFocus HOME Infocus : Social Engineering Fundamentals , Part II : Combat Page 2 of 4,” pp. 1–5, 2003.

[11] D. Airehrour, N. V. Nair, and S. Madanian, “Social engineering attacks and countermeasures in the New Zealand Banking System: Advancing a user-reflective mitigation

model," *Information (Switzerland)*, vol. 9, no. 5. 2018.
[12] F. L. Greitzer, J. R. Strozer, S. Cohen, A. P. Moore, D. Mundie, and J. Cowley, "Analysis of unintentional insider threats deriving from social engineering exploits," *Proc. - IEEE Symp. Secur. Priv.*, vol. 2014-Janua, pp. 236–250, 2014.
[13] D. I. Junaedi, "Antisipasi Dampak Social Engineering Pada Bisnis Perbankan," *Infoman's*, vol. 11, no. 1, pp. 1–10, 2017.
[14] C. C. Ciptohartono and M. K. Dermawan, "Pencegahan Viktimisasi Pencurian Data Pribadi," vol. 3, pp. 157–169, 2019.
[15] R. Komalasari, "KESADARAN AKAN KEAMANAN PENGGUNAAN USERNAME DAN PASSWORD," *J. Teknol. Inf. Dan Komun. Vol. 5, No. 2 Desember 2018*, vol. 5, no. 2, pp. 68–77, 2018.
[16] J. Allen, L. Gomez, M. Green, P. Ricciardi, C. Sanabria, and S. Kim, "Social Network Security Issues: Social Engineering and Phishing Attacks," pp. 1–7, 2012.
[17] S. Suendri, "Hashing Argon2 Untuk Keamanan Password Pada Sistem Berbasis Web Menggunakan Php," *JISTech (Journal Islam. Sci. Technol.*, vol. 4, no. 1, 2019.
[18] D. Ariyus, Kemanan Multimedia. Yogyakarta: ANDI, 2009.
[19] D. C. Islami, K. B. I.H, and C. Candiwan, "Kesadaran Keamanan Informasi pada Pegawai Bank x di Bandung Indonesia," J. INKOM, vol. 10, no. 1, p. 19, Nov. 2016.
[20] P. Jati Sekar Agri, "Evaluasi Tingkat Kesadaran Keamanan Informasi Mahasiswa Akuntansi Universitas Sanata Dharma," Universitas Sanata Dharma, 2019.