Jintech: Journal of Information Technology **E-ISSN : 2746-2331**
Februari 2024, Halaman: 12 - 24 **P-ISSN : 2746-234X**

ANALISIS TINGKAT KESADARAN MAHASISWA TERHADAP SERANGAN REKAYASA SOSIAL

(STUDI KASUS: MAHASISWA TEKNOLOGI INFORMASI UNIVERSITAS ISLAM NEGERI AR-RANIRY)

Malahayati[1)], NuraNabilah[3)]
[123)]*Teknologi Informasi, Universitas Islam Negeri Ar-Raniry, Banda Aceh, Indonesia*
malahayati_umar@ar-raniry.ac.id [1)]
nuranabila953@gmail.com [3)]

Abstract: The problem we face today is that there are still many cases where people spread information about money, internet quotas, free travel, scholarships, or other valuable items on social media. One of them in the dissemination of this information is students of the Information Technology Study Program at the State Islamic University (UIN) Ar-Raniry, who should understand technology and always be in contact with the world of information technology, still disseminating information whose origins are not clear. This raises concerns that if the link is accessed carelessly, then the victim will be phished. The purpose of this study is to analyze students' awareness of social engineering attacks using descriptive methods. The result of this research is that the respondents who input data on the phishing web are 13 respondents, or 10.7%, and those who do not input data on the phishing web are 108 respondents, or 89.3%. Then respondents who accessed the phishing link and input data on the phishing web were 13 respondents, or 10.7%; then, 83 respondents, or 68.6%, who accessed the link but did not input phishing web data and did not access it at all, were 25 respondents, or 20.7%. This means that students of the Information Technology Study Program at State Islamic University (UIN) Ar-Raniry are well aware of phishing-based social engineering attacks.

Keywords: *Phishing, Awareness, Students*

Abstrak: Permasalahan yang kita hadapi saat ini adalah masih banyaknya kasus yang menyebarkan informasi mengenai uang, kuota internet, perjalanan gratis, beasiswa atau barang berharga lainnya di media sosial. Salah satunya dalam penyebaran informasi tersebut adalah mahasiswa Prodi Teknologi Informasi Universitas Islam Negeri (UIN) Ar-Raniry yang seharusnya mengerti teknologi dan selalu berhubungan dengan dunia teknologi informasi masih menyebarkan informasi yang asal usulnya tidak jelas. Hal ini menimbulkan rasa khawatir jika tautan diakses secara sembarangan maka korbannya akan terkena *phising*. Tujuan penelitian ini adalah menganalisis kesadaran mahsiswa terhadap serangan rekayasa sosial dengan menggunakan metode deskriptif. Hasil penelitian ini bahwa para responden yang yang menginput data pada web *phising* tersebut terdapat 13 orang responden atau 10,7% dan yang tidak menginput data pada web *phising* terdapat 108 orang responden atau 89,3%. Kemudian responden yang mengakses tautan *phising* dan menginput data pada web *phising* terdapat 13 orang responden atau 10,7%, lalu 83 orang responden atau 68,6% yang mengakses tautan tetapi tidak menginput data web *phising*, dan tidak mengakses sama sekali terdapat 25 orang responden atau 20,7%. Artinya, mahasiswa Prodi Teknologi Informasi Universitas Islam Negeri (UIN) Ar-raniry sudah paham betul akan serangan rekayasa sosial berbasis *phising.*

Kata kunci : *Phising*, Kesadaran, Mahasiswa

1. Pendahuluan

Rekayasa sosial atau lebih dikenal dengan *social engineering* merupakan cara untuk memanipulasi seseorang dengan mencari salah satu kelemahan target agar mendapat informasi, akses serta mendorong target untuk melakukan aksinya (Wahyuni et al., 2022). *Social engineering* mempunyai banyak teknik penyerangan salah satunya ialah *phising*. *Phising* merupakan suatu bentuk perbuatan yang bersifat mengancam atau menjebak seseorang dengan cara memancing orang tersebut. Yaitu dengan menipu seseorang sehingga orang tersebut secara tidak langsung memberikan semua informasi yang di butuhkan oleh sang penjebak (Fatimah, 2017).

Namun, masalah yang kita hadapi sekarang ini ialah masih ditemukannya kasus menyebarkan informasi yang mengiming-imingkan uang, kuota internet dan tak jarang juga berupa jalan-jalan gratis, beasiswa ataupun barang berharga lainnya di media sosial. Salah satunya dalam menyebarkan informasi tersebut adalah mahasiswa jurusan Teknologi Informasi UIN Ar-Raniry yang seharusnya paham akan teknologi dan selalu berhubungan dengan dunia IT masih menyebarkan informasi yang belum jelas asalnya. Hal ini menimbulkan rasa khawatir jika salah mengakses tautan secara sembarangan maka korban akan terkena *phising*. Informasi yang dikirim oleh salah satu mahasiswa Prodi Teknologi Informasi melalui media sosial whatsapp.

2. Kajian Kepustakaan

2.1 Kesadaran

Menurut Kamus Besar Bahasa Indonesia (KBBI), kesadaran ialah keadaan mengerti hal yang dirasakan atau dialami oleh seseorang. Kemudian kesadaran menurut (Patricia Kalis Jati Sekar Agri, 2019) ialah suatu keadaan yang dirasakan dan diwujudkan ataupun dikerjakan dalam sebuah aktivitas. Sedangkan kesadaran menurut (King, 2014) kesadaran adalah keawasan individu tentang keadaan eksternal dan sensasi internal di bawah kondisi tergugah, meliputi keawasan diri dan pikiran akan pengalaman individu (King, 2014) membagi kesadaran menjadi lima tingkatan keawasan yaitu, kesadaran tingkat tinggi, kesadaran tingkat rendah, kondisi kesadaran yang berubah, keawasan bawah sadar dan tidak ada keawasan. Berikut lima tingkatan keawasan menurut (King, 2014):

1. Kesadaran Tingkat Tinggi

Kesadaran tingkat tinggi merupakan kesadaran yang melibatkan pemrosesan terkontrol. Pemrosesan terkontrol adalah kondisi kesadaran manusia sepenuhnya ketika individu secara aktif memfokuskan usahanya untuk mencapai tujuan. Dalam pemrosesan terkontrol terdapat aspek penting yaitu fungsi eksekutif. Fungsi eksekutif merupakan proses kognitif yang kompleks dan berada dalam tingkat yang lebih tinggi, meliputi berpikir, merencanakan, dan memecahkan masalah.

2. Kesadaran Tingkat Rendah

Kesadaran tingkat rendah ialah kesadaran yang meliputi pemrosesan otomatis dan melamun. Proses otomatis adalah kondisi kesadaran yang hanya memerlukan sedikit atensi dan tidak mengganggu kegiatan lain yang sedang dilakukan. Sedangkan melamun ialah kondisi kesadaran lain yang melibatkan usaha sadar tingkat rendah yang terletak di antara kesadaran aktif dan bermimpi ketika tidur.

3. Kondisi Kesadaran yang Berubah

Kondisi kesadaran yang berubah/keawasan yang berubah adalah kondisi mental yang terlihat berbeda dari keawasan normal. Kondisi ini biasanya disebabkan oleh trauma, demam, kelelahan, masalah sensoris, meditasi, hypnosis, dan gangguan psikologis.

4. Keawasan Bawah Sadar

Keawasan bawah sadar terbagi menjadi dua yaitu, keawasan bawah sadar ketika terjaga dan keawasan bawah sadar ketika tidur dan bermimpi. Keawasan bawah sadar ketika terjaga adalah proses yang terjadi tepat di bawah permukaan keawasan seseorang. Sedangkan keawasan bawah sadar ketika tidur dan bermimpi ialah tingkat keawasan seseorang lebih rendah dibandingkan ketika seseorang melamun, namun tidur dan mimpi bukan berarti seseorang tidak dalam kondisi sadar.

5. Tidak ada Keawasan

Tidak ada keawasan atau disebut dengan bawah sadar. Istilah bawah sadar diberikan kepada orang yang pingsan ataupun di bawah pengaruh obat bius, atau orang yang berada dalam kondisi ketidaksadaraan yang mendalam dan belangsung lama.

2.2 Serangan siber

Serangan siber menurut (Luthfah, 2021) merupakan sebuah cara yang dilakukan oleh seseorang maupun organisasi untuk melakukan penyerangan dengan tujuan tertentu misalnya untuk mencuri, merusak dan menghancurkan target spesifik dengan cara masuk kedalam sistem atau network komputer. Sedangkan definisi serangan siber menurut Peraturan Menteri Pertahanan (Permenhan) Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber ialah: serangan siber adalah segala bentuk perbuatan, perkataan, pemikiran baik yang dilakukan dengan sengaja maupun tidak sengaja oleh pihak mana pun, dengan motif dan tujuan apa pun, yang dilakukan di lokasi mana pun, yang disasarkan pada sistem elektronik atau muatannya (informasi) maupun peralatan yang sangat bergantung pada teknologi dan jaringan dalam skala apa pun, terhadap objek vital maupun non vital dalam lingkup militer dan nonmiliter, yang mengancam kedaulatan negara, keutuhan wilayah dan keselamatan bangsa.

2.3 Social engineering

Social engineering merupakan suatu perbuatan untuk memanipulasi seseorang dengan menggunakan salah satu cara mencari kelemahan target agar mendapat informasi, akses serta mendorong target untuk melakukan aksinya (Wahyuni et al., 2022). Sedangkan menurut (GUNAWAN, 2019) rekayasa sosial merupakan suatu cara mengambil atau mencuri data maupun informasi dari seseorang yang bersifat rahasia dengan cara interaksi sosial. Dalam artian lain rekayasa sosial adalah cara mendapatkan data ataupun informasi penting dengan memanfaatkan kelemahan manusia.

Dikarenakan *sosial engineering* ini memanfaatkan kelemahan manusia, (Prof. Richardus Eko Indrajit, 2013) mendefinisikan kelemahan manusia menjadi tiga bagian:

1. Rasa Percaya

   Biasanya peretas mengaku sebagai orang yang sangat akrab dengan korban. Seperti saudara, sahabat, keluarga, teman kantor, sehingga korban langsung memberikan tanpa merasa ragu.

2. Rasa Menolong

   Merupakan sifat dasar manusia, jika seseorang terkena musibah dan sedang dalam kesedihan, seperti menjadi korban kecelakaan lalu lintas. Biasanya korban tanpa sadar langsung memberikan informasi tanpa mengkonfirmasi terlebih dahulu.

3. Rasa Takut

   Hal yang biasa dipakai dalam *social engineering*, jika seseorang diminta data atau informasi yang mengaku sebagai atasan, penegak hukum akan memberikan informasi yang diminta.

Menurut (Rafizan, 2013) terdapat empat pola dalam *social engineering* yang sering dipraktikkan oleh para hacker adalah sebagai berikut:

a. Pengumpulan Informasi

   Informasi yang dikumpulkan oleh peretas dapat dilakukan dengan banyak cara. Bisa berupa struktur organisasi, tanggal ulang tahun atau kebiasaan lainnya yang dapat mengembangkan relasi dengan target sasaran.

b. Mengembangkan Relasi atau Hubungan

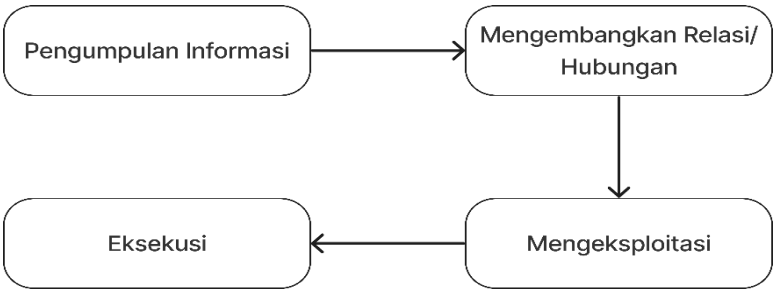
   Setelah tahapan informasi selesai, selanjutnya peretas akan mendekati target yang paling rentan di instansi atau orang yang bisa mengantarkan peretas kepada informasi sasaran. Bisa saja peretas mendekati karyawan dengan mengaku suruhan,saudara kenalan dari atasan instasi tersebut.

c. Eksploitasi

Setelah relasi sudah terbangun dengan target, kemudian tahap eksploitasi dijalankan dengan berusaha menggali informasi rahasia agar dapat masuk ke sistem. Informasi tersebut berupa *username,* kata sandi dan lain-lain.

d. Eksekusi

Setelah selesai mengekspolitasi data-data penting, peretas telah siap menjalankan serangannya. Tahap inilah pola *social engineering* telah selesai dan berlanjut akan melakukan penyerangan sistem seperti merubah, mencuri bahkan bisa merusak sistemkeamanan.



Gambar 1. Pola *social engineering (*Rafizan, 2013)

2.4 Klasifikasi *Social Engineering*

Menurut (Ivaturi & Janczewski, 2011) di dalam jurnal A Taxonomy for Social Engineering Attack yang di terbitkan oleh Internasional Conference on Informasi Resource Management mengklasifikasi tipe serangan *social engineering*:

1. Individu ke Individu

   Jenis serangan ini dikategorikan sebagai rekayasa sosial yang menyerang individu-individu umumnya melibatkan langsung peretas dengan korban dengan cara menipu dan memanfaatkan ketidaktahuan, kepercayaan serta kelemahan perilaku (Ivaturi & Janczewski, 2011).

   a. Meniru

      Meniru adalah teknik yang paling penting bagi peretas dikarenakan kegiatanini hanya memerlukan sedikit persiapan tetapi memiliki keuntungan tanpa mengungkapkan indentitas asli (Ivaturi & Janczewski, 2011).

   b. *Pretexting*

      Pretexting adalah salah satu teknik peniruan indentitas yang paling popular dan merupakan teknik untuk mendapatkan informasi dengan alasan yang tidak sebenarnya.

Sering kali tidak hanya sekedar kebohongan, teknik ini terlebih dahulu melakukan riset terhadap korban terlebih dahulu (Ivaturi & Janczewski, 2011). Salah satu contoh dari pretexting adalah menyamar sebagai pegawai bank dan mendekati korban yang sedang kesulitan dengan mesin ATM.

c. *Reverse social engineering* atau *quid pro quo*

Reverse social engineering ini mencakup tiga tahapan, yaitu sabotase, periklanan, bantuan. Misalnya, pada tahapa awal si penyerang melakukan sabotase jaringan yang dituju, kemudian ia mempromosikan dirinya sebagai orang yang dapat mengatasi masalah yang korban hadapi. Pada tahap akhir si penyerang meminta akses untuk masuk ke jaringan dengan alasan agar permasalahan dapat diselesaikan. Serangan ini cenderung efektif dikarenakan korban merasa puas masalahnya teratasi dan sedikit alasan untuk merasa curigakepada si penyerang (Ivaturi & Janczewski, 2011). Peretasan quid pro quo terkadang memasukan malware ke dalam sistem pengguna (Conteh & Schmick,2016).

d. *Tailganting*

Tailganting adalah teknik yang berupaya mencari celah untuk masuk ke area yang terbatas, teknik ini juga dikenal sebagai piggybacking. Dalam serangan ini mereka menyamar sebagai seorang karyawan ataupun sebagai petugas pengiriman paket yang memiliki akses masuk sementara (Tyas Darmaningrat etal., 2022).

2. Individu ke individu via teks

Kategori ini meliputi semua jenis serangan yang menggunakan teks sebagai media komunikasi. Contoh yang menggunakan jaringan internet (online) seperti browsing, media sosial, pesan (chat) dan Short Messanging Services (SMS) atau yang tidak menggunakan jaringan internet (offline) seperti surat dan surat kabar (Ivaturi & Janczewski, 2011).

a. *Phising*

Phising adalah perbuatan kriminal yang menggunakan teknik rekayasasosial. Phisher adalah sebutan untuk pelaku kejahatan phishing. Para phisher akan berusaha memperoleh informasi korban, seperti nama pengguna, kata sandi, dan kartu kredit yang bisa digunakan untuk mencuri indentitas (Vadila & Pratama, 2021).

b. SMSishing

Smsishing adalah jenis serangan ini sangat menyerupai phishing namun berbeda dalam pesan penipuan. Serangan ini tidak menggunakan email namun mengirimkan pesan SMS ke ponsel korban (Yeboah-Boateng & Amanor, 2014).

c. *Cross site request forgery* (CSRF)

CSRF adalah jenis serangan yang menipu browser korban dengan cara mengirimkan email kepada korban yang terlihat resmi ternyata membawa malware dalam bentuk elemen HTML seperti gambar, skrip dan lain-lain. Setelah korban membuka email palsu tersebut, browser akan menjalankan malware dalam bentuk HTML tanpa konfirmasi dari pengguna. Ini disebabkan browser mengira pengguna masih dalam keadaan login (Ivaturi & Janczewski, 2011).

d. Malware

Malware adalah penipuan yang akan dijalankan pada komputer pengguna. Malware rata-rata menempel pada email yang dikirimkan phisher kepada korban. Sesudah korban mengklik pada tautan, maka malware akan mulai berkerja. Malware tersebut biasanya terdapat di dalam file yang di download (Ginanjar et al., 2018).

3. Individu ke individu via suara

Semua jenis serangan yang tidak memperlihatkan fisik si peretas dan hanya menggunakan suara sebagai media komunikasi (Ivaturi & Janczewski, 2011). *Vishing* atau *Voice phishing* adalah tipe serangan yang menggunakan telepon atau suara sebagai media utamanya dan dapat juga menggunakana VOIP (*Voice Over Internet Protocol*). Serangan ini membuat korban yakin untuk memberikan data pribadi seperti akun bank (Ivaturi & Janczewski, 2011).

4. Individu ke individu via video

Jenis serangan ini menggunakan video sebagai media komunikasi. Dengan kesuksesan youtube, peretas dapat membuat video tutorial untuk menyelesaikan suatu persoalan di komputer, peretas juga memasukkan tautan untuk mengunduh perangkat lunak palsu berdasarkan video tutorial yang dapat menyelesaikan masalah pada komputer (Ivaturi & Janczewski, 2011).

2.5 Web

Menurut KBBI (2022), web merupakan sistem untuk mengakses, memanipulasi, dan mengunduh dokumen hipertaut yang terdapat dalam komputer yang dihubungkan melalui internet; jejaring; jaringan. Sedangkan menurut (Siregar & Sari, 2018) web adalah sebuah system yang saling terhubung dalam sebuah dokumen yang berbentuk hypertext yang di dalamnya terdapat berbagai informasi yaitu, berupa tulisan, gambar, suara, video, dan informasi multimedia lainnya dan dapat diakses melalui sebuah perangkat yang disebut web browser.

2.6 Phising

Saat ini banyaknya pengguna media sosial membuat para penjahat siber makin gencar dalam melakukan aksinya. Salah satunya ialah dengan *phising*. *Phising* adalah jenis serangan untuk mendapatkan informasi penting dari pihak tertentu dengan cara menyamar seperti orang yang dipercaya. Lazimnya *phising* dilakukan pada tahap awal serangan untuk mendapatkan data target (Ahmadian & Sabri, 2021). *Phising* termasuk dalam kejahatan siber, dimana sekarang ini marak terjadi tindak kriminal melalui jaringan komputer (Fatimah, 2017).

2.7 Web *phising*

Web *phising* merupakan salah satu ancaman kejahatan siber yang tujuannya adalah untuk mengambil informasi penting dari targetnya seperti username, password, data kartu kredit, maupun data-data serta informasi pribadi lainnya. Web *phising* bekerja dengan cara menjebak korban untuk klik sebuah tautan yang nantinya akan diarahkan pada halaman palsu yang didesain semirip mungkin dengan website asli yang diharapkan oleh targetnya. Umumnya, pengguna yang terkena serangan web *phising* tidak akan menyadari bahwa dirinya sedang berada pada jebakan web *phising*, dan baru akan tersadar setelah mengalami berbagai kerugian material (Nugraha et al., 2022)**.**

3. Metode Penelitian

Metode yang digunakan adalah metode deskriptif. Metode deskriptif digunakan untuk menggambarkan data sesuai dengan jawaban yang diberikan oleh responden.

4. Metode Pengumpulan Data

Penelitian ini menggunakan *Purposive Sampling* dikarenakan sampel pada penelitian ini mempunyai kriteria tertentu, yaitu responden yang terpilih adalah yang sedang mengambil mata kuliah keamanan data dan informasi serta mata kuliah jaringan komputer lanjut. Penelitian ini memiliki jumlah responden sebanyak 121 orang responden dengan masing-masing responden memiliki jumlah responden yang berbeda beda. Untuk mata kuliah keamanan data dan informasi memiliki jumlah responden sebanyak 23 orang responden dan untuk mata kuliah jaringan komputer lanjut memiliki responden sebanyak 98 orang responden.

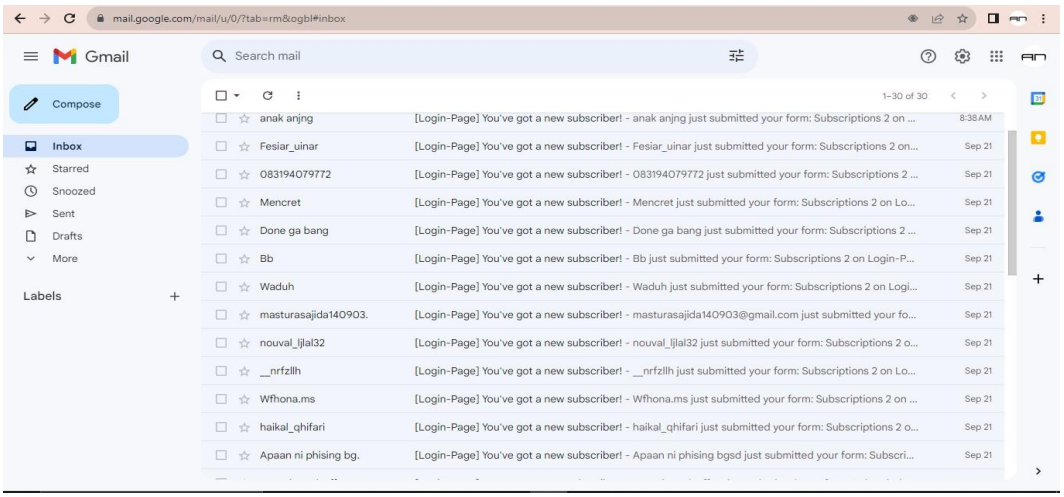
5. Analisa dan Hasil

Web *phising* berupa halaman login instagram dibuat menggunakan platform web hosting gratis wix.com. Penggunaan platform ini dipilih karena efisiensi dan kemudahan dalam membuat sebuah desain web secara mandiri. Halaman login instagram dipilih oleh peneliti karena media sosial tersebut cukup populer dan digandrungi kawula muda.

Penyebaran tautan *phising* dilakukan pada media sosial whatsapp dengan memberikan informasi yang meyakinkan responden untuk mengakses tautan tersebut.

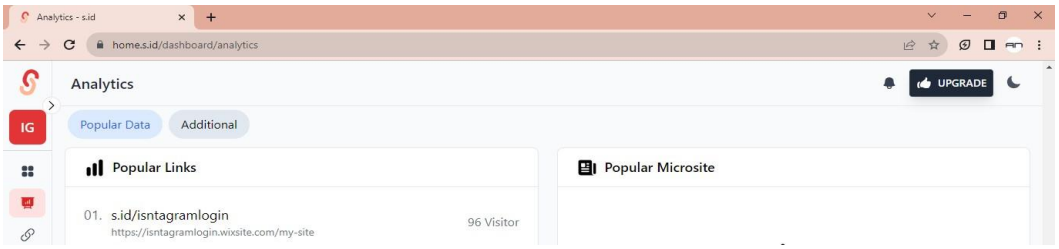
Jika responden tergerak untuk mengisi *username* dan *password*, maka dapat disimpulkan bahwa responden gagal mengidentifikasi sebuah web *phising*. Dari hasil penyebaran tautan *phising* tersebut, didapatkan 13 orang responden yang menginput data pada web *phising*.

Hasil tersebut dapat disimpulkan bahwa terdapat 13 orang atau 10,7% dari jumlah total responden sebanyak 121 orang mahasiswa Program Studi Teknologi Informasi UIN Ar-Raniry yang tergerak untuk mengisi data pada web *phising*. Sebanyak 108 orang responden atau 89,3% dari jumlah total responden sebanyak 121 orang mahasiswa Program Studi Teknologi Informasi UIN Ar-Raniry yang tidak tertarik untuk mengisi data pada web *phising*



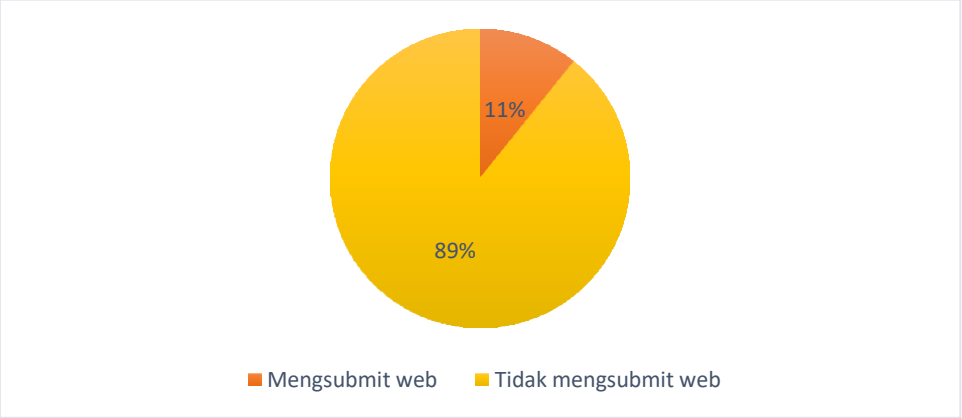
Gambar 3. Responden yang menginput data pada web *phising*

Setelah tautan *phising* disebarkan melalui media sosial whatsapp dan diberikan sedikit informasi mengenai tautan tersebut, kemudian peneliti dapat melihat responden yang mengakses tautan tersebut. Ternyata dari 121 orang responden ditemukan 96 orang responden yang mengakses tautan web *phising* tersebut. Respoden yang mengakses tautan *phising* dapat dilihat pada gambar 4.



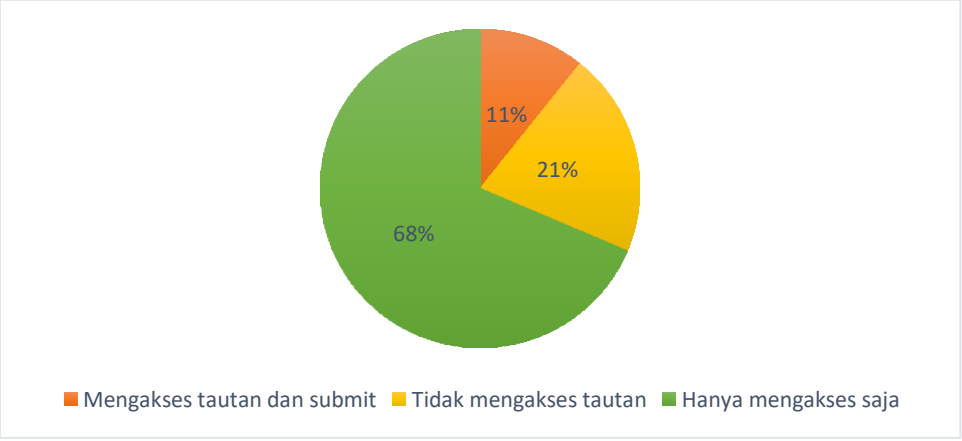
Gambar 4. Responden yang mengakses tautan *phising*

Hasil analisis deskriptif pada penelitian ini menujukkan bahwa responden yang menginput data pada web *phising* tersebut berjumlah 13 orang responden atau 10,7% dan yang tidak menginput data pada web *phising* tersebut berjumlah 108 orang responden atau 89,3% dari jumlah keseluruhan responden 121 orang responden. Hasil jawaban responden yang menginput data pada web *phising* dan tidaknya dapat dilihat pada gambar 5.



Gambar 5. Hasil responden web *phising*

Kemudian pada gambar 6 terdapat 13 orang responden atau 10,7% yang mengakses tautan lalu menginput data pada web *phising* tersebut, 83 orang responden atau 68,6% mengakses tautan tetapi tidak menginput data pada web *phising*, dan 25 orang responden atau 20,7% yang sama sekali tidak mengakses tautan web *phising* tersebut. Artinya, mahasiswa Teknologi Informasi UIN Ar-raniry memiliki kesadaran tinggi terhadap serangan rekayasa sosial berbasis *phising*. Hasil jawaban para responden pada tautan *phising* dapat dilihat pada gambar 6.



Gambar 6. Hasil responden tautan *phising*

6. Kesimpulan dan Saran

6.1 Kesimpulan

Berdasarkan hasil jawaban dari para responden yang menginput data pada web *phising* tersebut terdapat 13 orang responden atau 10,7% dan yang tidak menginput data pada web *phising* terdapat 108 orang responden atau 89,3%. Kemudian responden yang mengakses tautan *phising* dan menginput data terdapat 13 orang responden atau 10,7%, lalu 83 orang responden atau 68,6% yang mengakses tautan tetapi tidak menginput data pada web tersebut, dan tidak mengakses sama sekali terdapat 25 orang responden atau 20,7%. Artinya, mahasiswa Prodi Teknologi Informasi Universitas Islam Negeri (UIN) Ar-raniry sudah paham betul akan serangan rekayasa sosial berbasis *phising.*

6.2 Saran

Analisis kesadaran mahasiswa terhadap serangan rekayasa sosial (studi kasus mahasiswa Teknologi Informasi UIN Ar-Raniry) dimungkinkan bagi peneliti lain untuk melakukan penelitian menggunakan metode yang berbeda.

Daftar Kepustakaan

Ahmadian, H., & Sabri, A. (2021). Teknik Penyerangan Phishing Pada Social Engineering Menggunakan Set Dan Pencegahannya. *Djtechno Jurnal Teknologi Informasi*, *2*(1), 13–20. https://doi.org/10.46576/djtechno.v2i1.1251

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23), 31–38. https://doi.org/10.19101/ijacr.2016.623006

Fatimah, M. H. W. dan N. (2017). Ancaman phishing terhadap pengguna sosial media dalam dunia cyber crime. *JOEICT(Jurnal of Education and Information Communication Technology)*, *1*, 1–5.

Ginanjar, A., Widiyasono, N., & Gunawan, R. (2018). Analisis Serangan Web Phishing pada Layanan E-commerce dengan Metode Network Forensic Process. *JUTEI, Volume.2*.

GUNAWAN, T. (2019). *DENGAN PENDEKATAN SKENARIO TERSTRUKTUR (Studi Kasus : Mahasiswa Departemen Sistem Informasi ITS) ANALYSIS OF STUDENT BEHAVIOR TOWARD SOCIAL ENGINEERING WITH STRUCTURED SCENARIO APPROACH (Case Study : Student Of ITS Information System*.

Ivaturi, K., & Janczewski, L. (2011). A Taxonomy for Social Engineering attacks A Taxonomy for Social Engineering attacks. *AIS Electronic Library*, 0–10.

Luthfah, D. (2021). Serangan Siber Sebagai Penggunaan Kekuatan Bersenjata dalam Perspektif Hukum Keamanan Nasional Indonesia (Cyber Attacks as the Use of Force in the Perspective of Indonesia National Security Law). *TerAs Law*

Review : Jurnal Hukum Humaniter Dan HAM, *3*(1), 11. https://doi.org/10.25105/teras-lrev.v3i1.10742

Nugraha, A. F., Aziza, R. F. A., & ... (2022). Penerapan metode Stacking dan Random Forest untuk Meningkatkan Kinerja Klasifikasi pada Proses Deteksi Web Phishing. *Jurnal Infomedia: Teknik …*, *7*(1).

Patricia Kalis Jati Sekar Agri. (2019). *EVALUASI TINGKAT KESADARAN KEAMANAN INFORMASI MAHASISWA AKUNTANSI UNIVERSITAS SANATA DHARMA*.

Prof. Richardus Eko Indrajit. (2013). Social Engineering. *SISTEM DAN TEKNOLOGI INFORMASI*, 1–6.

Rafizan, O. (2013). Analisis Penyerangan Social Engineering. *Peneliti Bidang Teknologi Informatika Di Puslitbang Aptika & IKP Balitbang SDM Kominfo*, 115–126.

Siregar, H. F., & Sari, N. (2018). Rancang Bangun Aplikasi Simpan Pinjam Uang Mahasiswa Fakultas Teknik Universitas Asahan Berbasis Web. *Jurnal Teknologi Informasi*, *2*(1), 53. https://doi.org/10.36294/jurti.v2i1.409

Tyas Darmaningrat, E. W., Noor Ali, A. H., Herdiyanti, A., Subriadi, A. P., Muqtadiroh, F. A., Astuti, H. M., & Susanto, T. D. (2022). Sosialisasi Bahaya dan Upaya Pencegahan Social Engineering untuk Meningkatkan Kesadaran Masyarakat tentang Keamanan Informasi. *Sewagati*, *6*(2). https://doi.org/10.12962/j26139960.v6i2.92

Vadila, N., & Pratama, A. R. (2021). Analisis Kesadaran Keamanan Terhadap Ancaman Phishing. *Automata*, *2*(2).

Wahyuni, S., Raazi, I. M., & Dwitawati, I. (2022). Analisis Teknik Penyerangan Phishing Pada Social Engineering Terhadap Keamanan Informasi di Media Sosial Profesional Menggunakan Kombinasi Black Eye dan Setoolkit. *Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI)*, *5*(1), 49–55. https://doi.org/10.32672/jnkti.v5i1.3962

Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing , SMiShing & Vishing : An Assessment of Threats against Mobile Devices. *Journal of Emerging Trends in Computing and Information Sciences*, *5*(4), 297–307.