ANALISIS KESADARAN MAHASISWA TERHADAP SERANGAN REKAYASA SOSIAL (STUDI KASUS : MAHASISWA TEKNOLOGI INFORMASI UNIVERSITAS ISLAM NEGERI AR-RANIRY)

TUGAS AKHIR

Diajukan Oleh :

NURA NABILAH
NIM. 180705008
Mahasiswa Fakultas Sains dan Teknologi
Program Studi Teknologi Informasi

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI AR-RANIRY
BANDA ACEH
2023/1445

LEMBAR PERSETUJUAN TUGAS AKHIR

ANALISIS KESADARAN MAHASISWA TERHADAP SERANGAN REKAYASA SOSIAL (STUDI KASUS : MAHASISWA TEKNOLOGI INFORMASI UNIVERSITAS ISLAM NEGERI AR-RANIRY)

TUGAS AKHIR

Diajukan kepada Fakultas Sains dan Teknologi
Universitas Islam Negeri (UIN) Ar-Raniry Banda Aceh
Sebagai Salah Satu Beban Studi Memperoleh Gelar Sarjana (S1)
dalam Prodi Teknologi Informasi

Oleh:
NURA NABILAH
180705008
Mahasiswa Fakultas Sains dan Teknologi
Program Studi Teknologi Informasi

Disetujui Untuk Dimunaqasyahkan Oleh:

Pembimbing I,	**Pembimbing II,**
Khairan AR, M.Kom	Malahayati, M.T
NIP.198607042014031001	**NIP.198301272015032003**

Mengetahui,
Ketua Program Studi

Ima Dwitawati, MBA
NIP.198210132014032002

LEMBAR PENGESAHAN TUGAS AKHIR

ANALISIS KESADARAN MAHASISWA TERHADAP SERANGAN REKAYASA SOSIAL (STUDI KASUS : MAHASISWA TEKNOLOGI INFORMASI UNIVERSITAS ISLAM NEGERI AR-RANIRY)

TUGAS AKHIR

Telah Diuji Oleh Panitia Ujian Munaqasah Skripsi
Fakultas Sains dan Teknologi UIN Ar-Raniry Banda Aceh dan Dinyatakan Lulus
Serta Diterima Sebagai Salah Satu Beban Studi Program Sarjana (S-1)
dalam Prodi Teknologi Informasi

Pada Hari/Tanggal: Hari, 30 Agustus 2023
13 Shafar 1445 H
di Darussalam, Banda Aceh

Panitia Ujian Munaqasah Skripsi:

Ketua,	Sekretaris,
Khairan AR, M. Kom	**Malahayati, M.T**
NIP. 198607042014031001	**NIP.198301272015032003**
Penguji I,	Penguji II,
Hendri Ahmadian, M.I.M	**Mulkan Fadhli, S.T.,M.T**
NIP.198301042014031002	**NIP.198811282020121006**

Mengetahui:
Dekan Fakultas Sains dan Teknologi
UIN Ar-Raniry Banda Aceh,

Dr.Ir. Muhammad Dirhamsyah, M.T., IPU
NIP. 19621002198811100

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan di bawah ini:

Nama	:	Nura Nabilah
Nim	:	180705008
Program Studi	:	Teknologi Informasi
Fakultas	:	Sains dan Teknologi
Judul	:	Analisis Kesadaran Mahasiswa Terhadap Serangan Rekayasa Sosial (Studi Kasus: Mahasiswa Teknologi Informasi Universitas Islam Negeri Ar-Raniry)

Dengan ini menyatakan bahwa dalam penulisan tugas akhir/skripsi ini, saya:

1. Tidak menggunakan ide orang lain tanpa mampu mengembangkan dan mempertanggungjawabkan;
2. Tidak melakukan plagiasi terhadap naskah karya orang lain;
3. Tidak menggunakan karya orang lain tanpa menyebutkan sumber asli atau tanpa izin pemilik karya;
4. Tidak memanipulasi dan memalsukan data;
5. Mengerjakan sendiri karya ini dan mampu bertanggungjawab atas karya ini.

Bila dikemudian hari ada tuntutan dari pihak lain atas karya saya, dan telah melalui pembuktian yang dapat dipertanggungjawabkan dan ternyata memang ditemukan bukti bahwa saya telah melanggar pernyataan ini, maka saya siap dikenai sanksi berdasarkan aturan yang berlaku di Fakultas Sains dan Teknologi UIN Ar-Raniry Banda Aceh.

Demikian pernyataan ini saya buat dengan sesungguhnya dan tanpa paksaan dari pihak manapun.

Banda Aceh, 30 Agustus 2023

Yang Menyatakan

Nura Nabilah

ABSTRAK

Nama	:	Nura Nabilah
NIM	:	180705008
Program Studi	:	Teknologi Informasi
Judul	:	Analisis Kesadaran Mahasiswa Terhadap Serangan Rekayasa Sosial (Studi Kasus: Mahasiswa Teknologi Informasi Universitas Islam Negeri Ar-Raniry)
Tanggal Sidang	:	30 Agustus 2023
Jumlah Halaman	:	50 Halaman
Pembimbing I	:	Khairan AR, M. Kom
Pembimbing II	:	Malahayati, M.T
Kata Kunci	:	*Phising*, Kesadaran, Mahasiswa

Phising adalah jenis serangan untuk mendapatkan informasi penting dari pihak tertentu dengan cara menyamar seperti orang yang dipercaya. 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 Prodi Teknologi Informasi Universitas Islam Negeri (UIN) Ar-Raniry yang seharusnya paham akan teknologi dan selalu berhubungan dengan dunia Teknologi Informasi masih menyebarkan informasi yang belum jelas asalnya. Hal ini menimbulkan rasa khawatir jika salah mengakses tautan secara sembarangan maka korban akan terkena *phising*. Penelitian ini bertujuan untuk menganalisis kesadaran mahasiswa terhadap serangan rekayasa sosial menggunakan metode deksriptif. Hasil penelitian ini bahwa para responden yang yang memasukkan data pada web *phising* tersebut terdapat 13 orang responden atau 10,7% dan yang tidak memasukkan data pada web *phising* terdapat 108 orang responden atau 89,3%. Kemudian responden yang mengakses tautan *phising* dan memasukkan data pada web *phising* terdapat 13 orang responden atau 10,7%, lalu 83 orang responden atau 68,6% yang mengakses tautan tetapi tidak memasukkan 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 memiliki kesadaran yang tinggi terhadap serangan rekayasa sosial berbasis *phising*.

KATA PENGANTAR

Syukur Alhamdulillah dipanjatkan ke hadirat Allah SWT yang telah melimpahkan rahmat-Nya sehingga Tugas Akhir yang berjudul **Analisis Kesadaran Mahasiswa Terhadap Serangan Rekayasa Sosial (Studi Kasus : Mahasiswa Teknologi Informasi Universitas Islam Negeri Ar-Raniry)** dapat diselesaikan. Selawat dan salam disanjungkan kepada Nabi Besar Muhammad SAW.

Tugas Akhir ini merupakan salah satu syarat yang harus dipenuhi untuk memperoleh gelar sarjana pada Fakultas Sains dan Teknologi (FST) di Universitas Islam Negeri (UIN) Ar-Raniry. Penyelesaian penulisan Tugas Akhir ini tidak terlepas dari bantuan dan dorongan dari berbagai pihak, baik secara moril maupun materiel. Pada kesempatan ini, ucapan terima kasih diucapkan kepada:

1. Ayahanda Asnawi dan Ibunda Raziah yang telah senantiasa mendoakan, membimbing, mendidik, serta memberikan semangat dan dukungan kepada penulis dalam menyelesaikan studi di Fakultas Sains dan Teknologi, Universitas Islam Negeri Ar-Raniry.
2. Bapak Dekan Fakultas Sains dan Teknologi Dr. Ir. Muhammad Dirhamsyah, M.T., IPU yang selalu mendukung dan memberi motivasi untuk kami.
3. Bapak Khairan AR, M.Kom sebagai pembimbing pertama dan Ibu Malahayati, M.T sebagai pembimbing kedua, yang telah meluangkan waktunya dan mencurahkan pemikirannya dalam membimbing penulis untuk menyelesaikan tugas akhir ini.
4. Ketua Prodi Teknologi Informasi Ibu Ima Dwitawati, MBA. Sekretaris Prodi Teknologi Informasi Bapak Khairan AR, M.Kom, serta staf Prodi yang telah ikut membantu proses pelaksanaan penelitian.
5. Bapak Mulkan Fadhli, S.T., M.T yang telah membimbing dan menyemangati saya sedari awal menjadi mahasiswa baru hingga saat ini.

6. Bapak dan Ibu dosen Program Studi Teknologi Informasi yang telah memberikan ilmu pengetahuan dalam bidang teknologi informasi kepada penulis sehingga penulis mampu menyelesaikan tugas akhir ini.
7. Kepada Staf Prodi Ibu Cut Ida Rahmadiana S.Si yang telah membantu membantu penulis dalam hal pengurusan administrasi dan surat-surat untuk keperluan penyelesaian tugas akhir.
8. Muhammad Alfarisyi telah banyak membantu serta memberikan dukungan sehingga penulis dapat menyelesaikan tugas akhir ini.
9. Teman-teman seperjuangan Teknologi Informasi, terima kasih banyak penulis ucapkan kepada Miskatur Rahman, Nisa Afdhila dan seluruh teman-teman 18 yang telah memberikan motivasi serta semangat.
10. Kepada seluruh mahasiswa/mahasiswi Prodi Teknologi Informasi yang telah membantu dan memberi dukungan kepada penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

I.1 Latar Belakang

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 dapat dilihat pada gambar I.I.

Gambar I.1 Informasi yang dikirim melalui whatsapp

Seperti penelitian yang dilakukan (Ramadhan et al., 2022) ternyata para mahasiswa UNINUS pernah menerima tautan *phising* yang dapat mengancam data pribadi mereka. Salah satunya ialah tautan *phising* kuota Kemendikbud yang mengincar data pribadi pelajar, mahasiwa dan orang yang membutuhkan kuota pada saat pandemi berlangsung. Hasil penelitian ini bahwa mahasiswa pernah mendapatkan tautan *phising* berupa kuota Kemendikbud.

Kemudian penelitian yang dilakukan oleh (Batmetan et al., 2018) ternyata masih ada mahasiswa yang tidak peduli akan keamanan privasinya akan tetapi tidak sedikit pula yang peduli akan hal itu. Selanjutnya didukung oleh penelitian (Akraman et al., 2018) dengan meningkatnya para pengguna android ternyata

ditemukan pengguna android yang memiliki tingkat kesadaran yang buruk dalam menjaga keamanan informasi dan privasinya. Hal ini dapat mengancam data pribadi pengguna android. Ada berbagai macam ancaman yang dapat mengancam data pribadi salah satunya ialah *phising.* Oleh karena itu, penelitian ini berjudul **"Analisis Kesadaran Mahasiswa Terhadap Serangan Rekayasa Sosial (Studi Kasus: Mahasiswa Teknologi Informasi Universitas Islam Negeri Ar-Raniry)"**.

I.2 Rumusan Masalah

Merujuk latar belakang tersebut, rumusan masalah dalam penelitian ini adalah:

1. Bagaimana analisis kesadaran mahasiswa terhadap serangan rekayasa sosial menggunakan metode deskriptif ?
2. Bagaimana tingkat kesadaran mahasiswa Prodi Teknologi Informasi terhadap serangan rekayasa sosial?

I.3 Tujuan Penelitian

Tujuan dilakukannya penelitian ini adalah:

1. Menganalisis kesadaran mahasiswa terhadap serangan rekayasa social menggunakan metode deksriptif.
2. Mengetahui tingkat kesadaran Mahasiswa Prodi Teknologi Informasi UIN Ar-Raniry terhadap serangan rakayasa sosial.

I.4 Batasan Masalah

Fokus penelitian ini adalah:

1. Responden merupakan mahasiswa Prodi Teknologi yang sedang mengambil mata kuliah keamanan data dan informasi serta mata kuliah jaringan komputer lanjut.
2. Menggunakan platform wix.com.

I.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah:

1. Bagi Peneliti
    a. Memberikan informasi kepada peneliti tentang tingkat kesadaran mahasiswa Prodi Teknologi Informasi terhadap serangan rekayasa sosial berbasis *phising*.
    b. Bagi peneliti selanjutnya penelitian ini diharapkan menjadi tambahan untuk referensi dalam melakukan penelitian selanjutnya
2. Bagi Mahasiswa

    Dapat memberikan informasi mengenai kesadaran mahasiswa Prodi Teknologi Informasi UIN Ar-Raniry ketika berhadapan dengan kejahatan siber berbasis serangan rekayasa sosial. Dengan demikian dapat menyadarkan mahasiswa untuk selalu waspada dan dapat mendeteksi serangan *social engineering* berbasis *phising*.
3. Bagi Kampus

    Memberikan gambaran nyata bagi Fakultas Sains dan Teknologi dan UIN Ar-Raniry mengenai kesadaran mahasiswa Program Studi Teknologi Informasi UIN Ar-Raniry terhadap kejahatan siber (*cybercrime*) berbasis serangan rekayasa sosial (*social engineering*). Dengan demikian pihak Fakulas Sains dan Teknologi dan UIN Ar-Raniry dapat menentukan langkah yang tepat dalam mewaspadai dan menanggulangi serangan *social engineering* khususnya *phising*.

BAB II
TINJAUAN PUSTAKA

II.1 Definisi 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.

II.2 Definisi 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.

II.3 Definisi Rekayasa Sosial *(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). Menurut KKBI (2021), rekayasa memiliki arti penerapan kaidah-kaidah ilmu dalam pelaksanaan, rencana jahat atau persengkongkolan untuk merugikan dan sebagainya pihak lain. Sedangkan sosial ialah berkenaan dengan masyarakat, suka memperhatikan kepentingan umum (KBBI, 2021). Dengan demikian rekayasa sosial bermakna kejahatan yang merugikan seseorang dengan cara masuk ke dalam sistem target yang dituju. 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

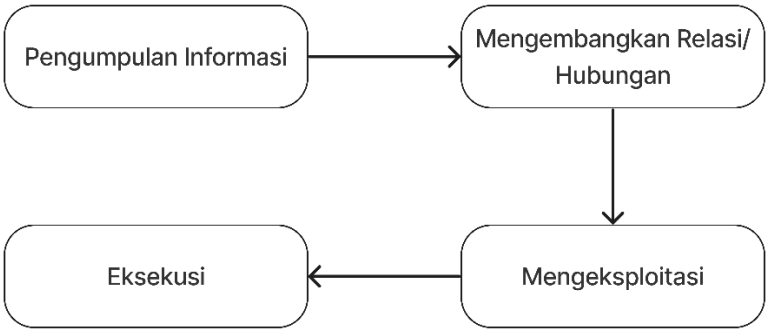
Setelah tahapan informasi selesai, selanjutnya peretas akan mendekati target yang paling rentan di instansi atau orang yang bisa mengantarkan peretas kepada informasi sasaran. Bisa saja peretas mendekati karyawan dengan mengaku suruhan, saudara kenalan dari atasan instasi tersebut.

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 sistem keamanan. Pola dalam *social engineering* dapat dilihat pada gambar II.1.



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

II.4 Klasifikasi Serangan Rekaya Sosial *(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 kegiatan ini 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 curiga kepada 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 et al., 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 rekayasa sosial. 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)

Cross site request forgery 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).

a. Vishing

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).

II.5 Definisi 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.

II.6 Definisi *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).

II.7 Definisi 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).

II.8 Penelitian Terdahulu

Berhubung dengan penelitian yang dilakukan pada kesadaran terhadap *social engineering*. Dibutuhkan referensi atau penelitian terkait guna terhindar dari duplikasi dan plagiarisme, sehingga penulis dapat mengembangkan suatu hal yang berbeda pada penelitian ini. Berikut ini adalah beberapa penelitian terkait yang berhubungan dengan penelitian penulis.

Penelitian mengenai "Penyebaran Link Phising Kuota Kemendikbud Terhadap Kesadaran Informasi Pribadi Di Kalangan Mahasiswa UNINUS" (Ramadhan et al., 2022). Dalam penelitian ini untuk mengetahui kesadaran mahasiswa UNINUS terhadap informasi pribadi menggunakan pendekatan kualitatif dengan metode deskriptif, dan teknik pengambilan datanya melalui wawancara juga kueisioner. Hasilnya, para informan mengaku mereka pernah menerima link *phising* kuota kemendikbud dan mengetahui bahwa link *phising* dapat mengancam data pribadi juga bisa menimbulkan kerugian materi maupun non materi. Berdasarkan hasil penelitian tersebut, maka kesadaran mahasiswa terhadap link *phising* sudah baik.

Penelitian mengenai "Peningkatan Literasi Digital Masyarakat Terhadap *Social Engineering* Dalam Masa Pandemi Covid-19" (Rochadiani et al., 2021). Penelitian ini bertujuan untuk meningkatkan literasi digital masyarakat, khususnya akan *social engineering*, sehingga dapat menekan jumlah kejahatan siber. Hasil penelitian ini melalui survei yang dilaksanakan sebelum dan sesudah edukasi dapat dilihat adanya peningkatan literasi digital masyarakat akan social engineering, yaitu terjadi peningkatan dengan rata-rata persentase peningkatan dari 3 video edukasi sekitar 63.29%.

Penelitian mengenai "Analisis Kesadaran Keamanan Terhadap Ancaman *Phishing*", (Vadila & Pratama, 2021). Penelitian ini bertujuan untuk melakukan penilaian terhadap tingkat kesadaran masyarakat terhadap ancaman *phishing*. Sebanyak 254 repsonden dengan berbagai latar belakang berbeda ikut berpartisipasi dalam penelitian ini. Analisis dilakukan dengan menggunakan metode ANOVA (*Analysis of Variance*) dengan bahasa pemrograman R, analisis yang berfokus pada aspek demografi jenis kelamin dan kelompok usia tertentu. Hasil penelitian ini

menemukan bahwa masyarakat Indonesia masih belum bisa mengenali ancaman *phishing* yang ada.

Penelitian mengenai "Tinjauan Kriminologi Dan Hukum Pidana Islam Terhadap Kejahatan *Cybercrime* Bermodus *Phishing* Di Sidoarjo", (Saputra, 2022). Penelitian ini menggunakan metode penelitian empiris dengan pendekatan kualitatif, dengan sumber data premier yang diambil dari wawancara aparat penegak hukum instansi kepolisian, korban kejahatan penipuan online bermodus *phishing* di Sidoarjo, dan laporan spkt yang masuk terkait serangan *phishing* yang merupakan hasil pengamatan terkait jumlah kejahatan yang terjadi di sidoarjo berdasarkan data kepolisian Sidoarjo. Hasilnya berupa para pengguna internet yang kurang teliti dan minimnya pemahaman terhadap kejahatan siber yang sangat rentan untuk menjadi korban serangan kejahatan siber.

Penelitian mengenai "Pengukuran Kesadaran Keamanan Informasi dan Privasi Pada Pengguna Smartphone Android di Indonesia", (Akraman et al., 2018). Penelitian ini menggunakan metode *analytical hierarchy process* (AHP) untuk mengukur tingkat kesadaran keamanan informasi dan privasi dari pengguna smartphone. Berdasarkan temuan tersebut, dapat disimpulkan bahwa pengguna smartphone di Indonesia memiliki tingkat kesadaran yang buruk dalam menjaga keamanan informasi dan privasinya.

Penelitian mengenai "Evaluasi Tingkat Kesadaran Keamanan Informasi Mahasiswa Akuntansi Universitas Sanata Dharma", (Patricia Kalis Jati Sekar Agri, 2019). Penelitian ini bertujuan untuk mengevaluasi tingkat kesadaran keamanan informasi yang dimiliki mahasiswa Akuntansi, Fakultas Ekonomi, Universitas Sanata Dharma. Hasil penelitian menunjukkan bahwa tingkat kesadaran keamanan informasi yang dimiliki oleh mahasiswa Akuntansi Universitas Sanata Dharma berada pada kategori baik.

Penelitian mengenai "Analisis Perilaku Mahasiswa Terhadap Rekayasa Sosial Dengan Pendekatan Skenario Terstruktur (Studi Kasus: Mahasiswa Departemen Sistem Informasi ITS)", (GUNAWAN, 2019). Penelitian ini menggunakan metode skenario terstruktur dimana skenario akan diberikan ke masing-masing mahasiswa sebagai responden. Dimana responden akan diminta

merespon dalam setiap skenario tersebut. Kemudian hasil jawaban dari responden akan dikelompokkan berdasarkan kelompok jawaban berdasarkan cara mereka menjawab setiap skenario yang diberikan. Hasil penelitian ini berupa mahasiswa mempuyai tingkat kesadaran yang baik.

Penelitian mengenai "Analisis Kesadaran Mahasiswa UMRI Terkait Penggunaan Teknologi & Media Sosial Terhadap Bahaya *Cybercrime*", (Soni et al., 2019). Dalam penelitian ini, analisis kesadaran mahasiswa di program studi teknik informatika, fakultas ilmu komputer, universitas muhammadiyah riau untuk mengetahui seberapa besar tingkat kesadaran mahasiswa tentang bahaya *cybercrime* didasarkan pada kategori media sosial dan kesadaran pengguna. Dari hasil penelitian, disimpulkan bahwa mahasiswa Jurusan Teknik Informatika memiliki tingkat kesadaran yang cukup baik. Hal ini dibuktikan dari hasil rata-rata yang diperoleh pada kategori media sosial, 83,4% mahasiswa mempunyai kesadaran yang cukup baik sedangkan pada kategori kesadaran pengguna rata-rata sebanyak 72,7%.

Penelitian mengenai "Tingkat Kesadaran Privasi Atas Masalah Keamanan Informasi (*Lack Of Security Awareness*)", (Batmetan et al., 2018). Tujuan dari penelitian ini adalah untuk menganalisis dan mengukur pemahaman Mahasiswa tentang pentingnya pemahaman tentang kebijakan privasi pada layanan publik. Hasil penelitian ini menunjukan bahwa sebagian besar mahasiswa menyadari pentingnya keamanan privasi dalam layanan public, mahasiswa juga menyadari resiko yang dapat terjadi jika melakukan pelanggaran dalam kebijakan privasi orang lain. Namun tidak sedikit juga mahasiswa yang merasa tidak peduli dengan keamanan privasi mereka.

Penelitian mengenai "Kesadaran Keamanan Privasi Dan Masyarakat 5.0", (Setiawan et al., 2019). Penelitian ini bertujuan untuk mengetahui apakah terdapat hubungan antara Masyarakat 5.0 dengan kesadaran privasi di indonesia. Hasilnya berupa lima puluh sembilan persen dari responden mengubah *privacy setting* dengan berbagai alasan diantaranya alasan keamanan, menghindari pengikut yang tidak dikenal, dan mencegah mendapat komentar dari orang tidak dikenal.

Tabel II.1 Penelitian Terdahulu

No	Nama Peneliti	Judul penelitian	Hasil Penelitian
1	Ramadhan et al., 2022	Penyebaran Link Phising Kuota Kemendikbud Terhadap Kesadaran Informasi Pribadi Di Kalangan Mahasiswa UNINUS	Hasilnya, para informan mengaku mereka pernah menerima link *phising* kuota kemendikbud dan mengetahui bahwa link *phising* dapat mengancam data pribadi juga bisa menimbulkan kerugian materi maupun non materi.
2	Rochadiani et al., 2021	Peningkatan Literasi Digital Masyarakat Terhadap *Social Engineering* Dalam Masa Pandemi Covid-19	Hasil penelitian ini melalui survei yang dilaksanakan sebelum dan sesudah edukasi dapat dilihat adanya peningkatan literasi digital masyarakat akan social engineering, yaitu terjadi

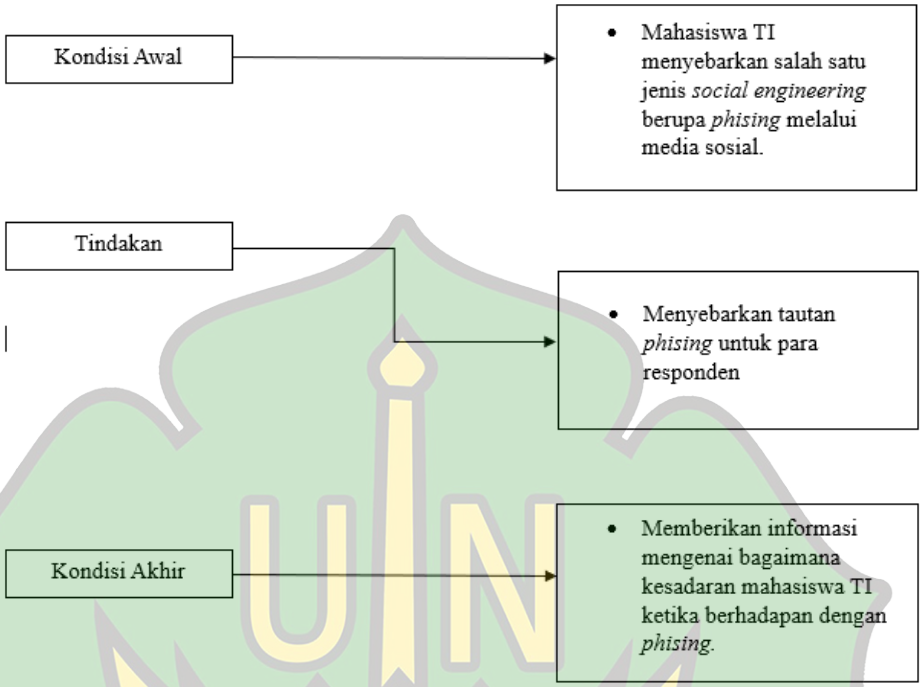
			peningkatan dengan rata-rata persentase peningkatan dari 3 video edukasi sekitar 63.29%.
3	Vadila & Pratama, 2021	Analisis Kesadaran Keamanan Terhadap Ancaman *Phishing*	Hasil penelitian ini menemukan bahwa masyarakat Indonesia masih belum bisa mengenali ancaman *phishing* yang ada.
4	Saputra, 2022	Tinjauan Kriminologi Dan Hukum Pidana Islam Terhadap Kejahatan *Cybercrime* Bermodus *Phishing* Di Sidoarjo	Hasilnya berupa para pengguna internet yang kurang teliti dan minimnya pemahaman terhadap kejahatan siber yang sangat rentan untuk menjadi korban serangan kejahatan siber
5	Akraman et al., 2018	Pengukuran Kesadaran Keamanan Informasi dan	Dapat disimpulkan

		Privasi Pada Pengguna Smartphone Android di Indonesia.	bahwa pengguna smartphone di Indonesia memiliki tingkat kesadaran yang buruk dalam menjaga keamanan informasi dan privasinya.
6	Patricia Kalis Jati Sekar Agri, 2019	Evaluasi Tingkat Kesadaran Keamanan Informasi Mahasiswa Akuntansi Universitas Sanata Dharma	Hasil penelitian menunjukkan bahwa tingkat kesadaran keamanan informasi yang dimiliki oleh mahasiswa Akuntansi Universitas Sanata Dharma berada pada kategori baik.
7	GUNAWAN, 2019	Analisis Perilaku Mahasiswa Terhadap Rekayasa Sosial Dengan Pendekatan Skenario Terstruktur (Studi Kasus: Mahasiswa Departemen Sistem Informasi ITS)	Hasil penelitian ini berupa mahasiswa mempuyai tingkat kesadaran yang baik.

8	Soni et al., 2019	Analisis Kesadaran Mahasiswa UMRI Terkait Penggunaan Teknologi & Media Sosial Terhadap Bahaya *Cybercrime*	Hasil rata-rata yang diperoleh pada kategori media sosial, 83,4% mahasiswa mempunyai kesadaran yang cukup baik sedangkan pada kategori kesadaran pengguna rata-rata sebanyak 72,7%.
9	Batmetan et al., 2018	Tingkat Kesadaran Privasi Atas Masalah Keamanan Informasi (*Lack Of Security Awareness*)	Hasilnya mahasiswa juga menyadari resiko yang dapat terjadi jika melakukan pelanggaran dalam kebijakan privasi orang lain. Namun tidak sedikit juga mahasiswa yang merasa tidak peduli dengan keamanan privasi mereka.

10	Setiawan et al., 2019	Kesadaran Keamanan Privasi Dan Masyarakat 5.0	Hasilnya berupa lima puluh sembilan persen dari responden mengubah *privacy setting* dengan berbagai alasan diantaranya alasan keamanan, menghindari pengikut yang tidak dikenal, dan mencegah mendapat komentar dari orang tidak dikenal.

II.9 Kerangka Berpikir



Gambar II.2 Kerangka berpikir

II.10 Hipotesis

Hipotesis merupakan jawaban sementara dari penelitian dikarenakan jawaban tersebut belum final dan perlu dibuktikan kebenarannya. Menurut (Sugiyono, 2016) hipotesis merupakan jawaban sementara terhadap rumusan masalah penelitian, di mana rumusan masalah penelitian telah dinyatakan dalam bentuk kalimat pertanyaan. Dikatakan sementara karena kebenaran jawaban akan terjawab ketika didapatkanya data-data melalui penelitian yang akan dilakukan. Oleh karena itu hipotesis dari penelitian ini adalah:

H_0 Kesadaran mahasiswa Prodi Teknologi Informasi terhadap serangan rekayasa sosial tidak tinggi.

H_1 Kesadaran mahasiswa Prodi Teknologi Informasi terhadap serangan rekayasa sosial tinggi.

BAB III
METODE PENELITIAN

III.1 Rancangan Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah deskriptif. Analisis deskriptif menurut (Mutmainnah, 2018) penelitian deskriptif adalah suatu metode dalam penelitian sekelompok manusia, suatu objek, suatu kondisi, suatu sistem pemikiran pada masa sekarang. Penelitian deskriptif merupakan penelitian yang berusaha mendeskripsikan dan menginterpretasikan sesuatu, misalnya kondisi atau hubungan yang ada, pendapat yang berkembang, proses yang sedang berlangsung, akibat atau efek yang terjadi, atau tentang kecendrungan yang sedang berlangsung. Berdasarkan pengertian tersebut dapat disimpulkan bahwa penelitian deskriptif digunakan untuk menggambarkan data sesuai dengan jawaban yang diberikan oleh responden

III.2 Waktu dan Lokasi Penelitian

Penelitian ini dilakukan selama kurang lebih lima bulan, dimulai dari April 2023 sampai dengan Agustus 2023. Tempat pelaksanaan penelitian pada Prodi Teknologi Informasi UIN Ar-Raniry.

III.3 Populasi dan Sampel

1. Populasi

Menurut (Sugiyono, 2016) populasi adalah wilayah generalisasi yang terdiri atas: objek/subjek yang mempunyai kualitas dan karakteristik tertentu yang ditetapkan oleh peneliti untuk dipelajari dan kemudian ditarik kesimpulannya. Populasi yang diteliti dalam penelitian ini adalah mahasiswa aktif Program Studi Teknologi Informasi UIN Ar-Raniry tahun ajaran 2022/2023 yang telah mengambil mata kuliah keamanan data dan jaringan komputer lanjut sebanyak 121 mahasiswa. Data mahasiswa aktif Prodi Teknologi Informasi yang sudah mengambil mata kuliah keamanan data dan informasi serta mata kuliah jaringan komputer lanjut dapat dilihat pada tabel III.1.

Tabel III.1 Mahasiswa aktif tahun ajaran 2022/2023 Program Studi Teknologi Informasi

No	Mata Kuliah	Jumlah Mahasiswa
1	Keamanan Data dan Informasi	23
2	Jaringan Komputer Lanjut	98
Total		121

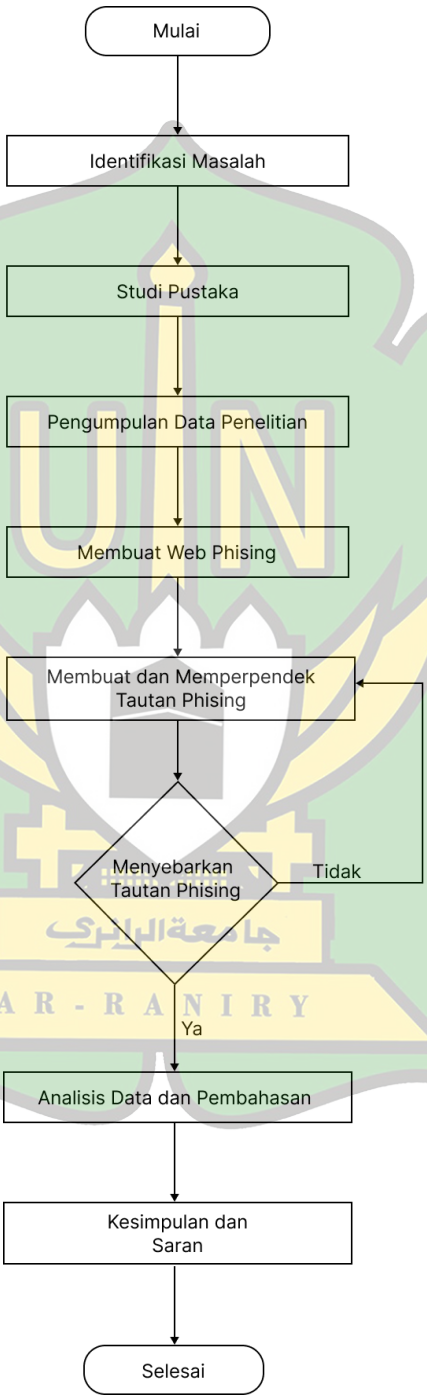
2. Sampel

Sampel adalah bagian dari jumlah dan karakteristik yang dimiliki oleh populasi (Sugiyono, 2016). Sampel pada penelitian ini, peneliti menggunakan teknik *Purposive Sampling.* Berdasarkan pendapat (Ir.Syofian Siregar, 2013), *Purposive Sampling* adalah metode penetapan responden untuk dijadikan sampel berdasarkan pada kriteria-kriteria tertentu.

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.

III.4 Teknik Pengumpulan Data

Tahapan penelitian yang dilakukan oleh peneliti dapat dilihat pada gambar III.1.



Gambar III.1 Tahapan penelitian

Adapun penjelasan tahapan penelitian yang dilakukan adalah sebagai berikut:

1. Identifikasi Masalah

   Identifikasi masalah merupakan langkah awal yang dilakukan peneliti sebelum melakukan dan menuliskan hasil penelitiannya.

2. Studi Pustaka

   Studi pustaka yaitu menelaah berbagai macam buku referensi serta hasil dari penelitian sebelumnya yang sejenis dan berguna untuk mendapatkan landasan teori mengenai masalah yang akan diteliti.

3. Pengumpulan Data Penelitian

   Pada tahap pengumpulan data menjelaskan bagaimana cara data yang diperlukan dapat dikumpulkan, sehingga di akhir penelitian mampu menyajikan informasi yang akurat. Data yang dikumpulkan peneliti dalam penelitian ini adalah mahasiswa aktif Program Studi Teknologi Informasi UIN Ar-Raniry ajaran 2022/2023 dengan jumlah responden sebanyak 121 mahasiswa.

4. Membuat web *phising*

   Membuat web *phising* dengan semirip mungkin dengan web aslinya bertujuan untuk menipu serta mengambil informasi dari responden yang memasukkan data pada web *phising*.

5. Membuat dan memperpendek tautan *phising*

   Tahapan membuat dan memperpendek tautan phising berguna untuk lebih meyakinkan korban mengakses tautan tersebut.

6. Menyebarkan tautan *phising*

   Menyebarkan tautan *phising* yang berisikan informasi penting bertujuan untuk menipu korban supaya mengakses tautan tersebut.

7. Analisis Data dan Pembahasan

   Analisis data merupakan metode pengolahan data yang bertujuan untuk mendapatkan informasi penting yang dapat dijadikan dasar dalam pengambilan keputusan untuk solusi suatu permasalahan.

8. Kesimpulan dan Saran

   Kesimpulan dan saran merupakan tahap akhir dalam menganalisis data.

III.5 Analisis Data

Analisis data dalam penelitian ini menggunakan metode deskriptif.

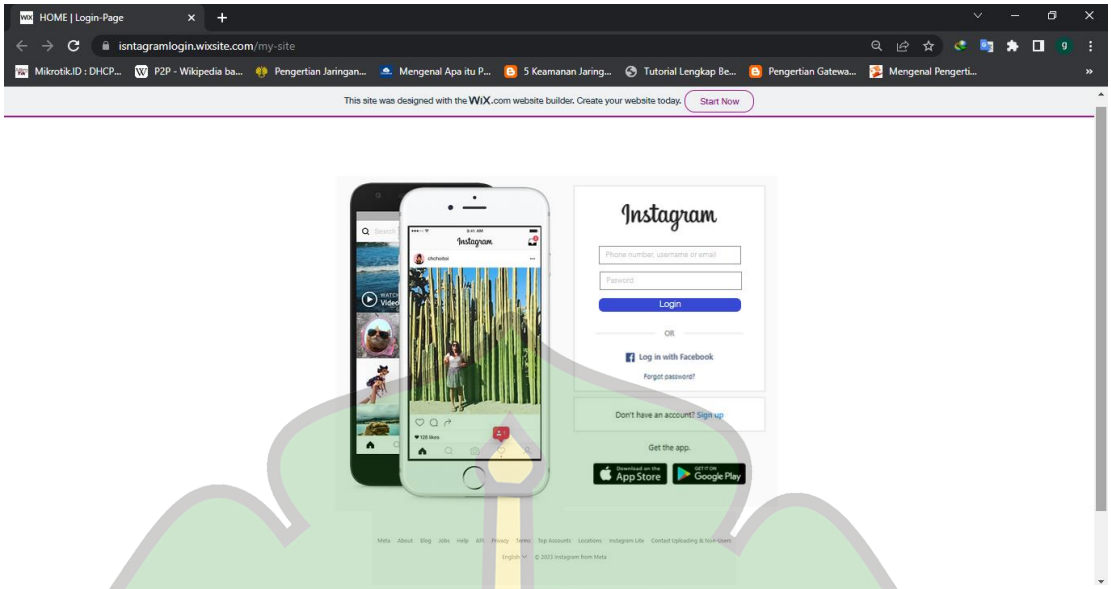
III.5.1 Membuat Web *Phising*

Web phising dibuat untuk menipu serta 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 mengakses 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).

Web *phising* dibuat menggunakan platform gratis yaitu berupa wix yang dimana wix tersebut bisa merupakan website builder berbasis *cloud* yang berfungsi membantu pengguna untuk membangun dan mengembangkan website mereka dengan mudah dan cepat. Platform ini sangat cocok untuk pemula dan belum memiliki kemampuan coding, karena wix sangat mudah untuk digunakan dan dipelajari. Sejak awal, website ini memang ditujukan untuk orang awam yang ingin membuat website tapi tidak mengerti bagaimana caranya.

Tampilan web *phising* instagram dipilih dikarenakan media sosial tersebut cukup populer dikalangan mahasiswa Program Studi Teknologi Informasi UIN Ar-Raniry.

Tampilan web *phising* instagram menggunakan wix.com dapat dilihat pada gambar III.1.



Gambar III.2 Tampilan web *phising* instagram menggunakan wix.com

III.5.2 Membuat Tautan *Phising*

Membuat tautan *phising* bertujuan untuk menipu korban serta meyakinkan korban untuk mengakses tautan tersebut. Tautan *phising* yang telah peneliti buat ialah https://isntagramlogin.wixsite.com/my-site. Agar tampak tautan lebih meyakinkan, peneliti menggunakan web s.id untuk memperpendek tautan tersebut. S.id merupakan platform yang memberikan layanan perpendek tautan atau link serta platform tersebut dapat melihat statistik pengujung yang mengakses tautan tersebut. Tautan yang sudah diperpendek menjadi: https://s.id/isntagramlogin.

III.5.3 Menyebarkan Tautan *Phising*

Tautan *phising* disebarkan di dalam grup whatsapp mata kuliah keamanan data dan jaringan komputer lanjut. Kemudian para responden diminta untuk mengakses web *phising* instagram yang telah dibuat.

BAB IV
HASIL DAN PEMBAHASAN

IV.1 Identifikasi Subjek Penelitian

Penelitian ini dilakukan pada mahasiswa Prodi Teknologi Informasi yang sedang mengambil mata kuliah keamanan data dan informasi serta mata kuliah jaringan komputer lanjut dan dari kalangan laki-laki maupun perempuan.

IV.1.1 Berdasarkan Jenis Kelamin

Pada penelitian ini yang menjadi subjek penelitian berdasarkan jenis kelamin dapat dilihat pada tabel IV.1, responden yang berjenis kelamin laki-laki sebanyak 72 orang responden (59,50%), yang mana lebih banyak dari responden yang berjenis kelamin perempuan sebanyak 49 orang responden (40,50%). Dapat disimpulkan bahwa responden berjenis kelamin laki-laki lebih banyak daripada responden berjenis kelamin perempuan dapat dilihat pada tabel IV.1.

Tabel IV.1 Karakteristik responden berdasarkan jenis kelamin

No	Jenis Kelamin	Jumlah Mahasiswa	Persentase
1	Laki-laki	72	59,50%
2	Perempuan	49	40,50%
	Total	121	100%

IV.1.2 Berdasarkan Mata Kuliah

Berdasarkan nilai mata kuliah, mahasiswa yang menjadi responden dalam penelitian ini dapat dilihat pada tabel IV.2:

Tabel IV.2 Karakteristik responden berdasarkan yang sudah mengambil mata kuliah keamanan data

No	Mata Kuliah	Jumlah Mahasiswa
1	Keamanan Data	23

Tabel IV.2 memperlihatkan responden dari penelitian yang mengambil mata kuliah keamanan data berjumlah 23 orang. Dengan laki-laki berjumlah 12 orang responden dan perempuan berjumlah 11 orang responden.

Tabel IV.3 Karakteristik responden berdasarkan yang sudah mengambil mata kuliah jaringan komputer lanjut

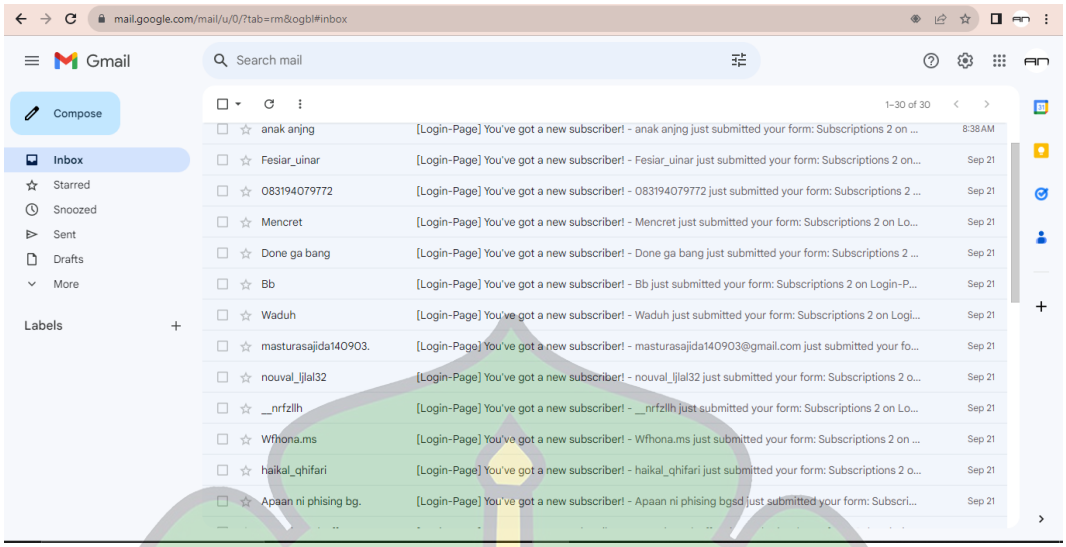
No	Mata Kuliah	Jumlah Mahasiswa
1	Jaringan Komputer Lanjut	98

Tabel IV.3 memperlihatkan responden dari penelitian yang mengambil mata kuliah jaringan komputer lanjut berjumlah 98 orang. Dengan laki-laki berjumlah 60 orang dan perempuan berjumlah 38 orang.

IV.2 Analisis Data

IV.2.1 Hasil Web *Phising*

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 memasukkan 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*. Respoden yang memasukkan data pada web *phising* dapat dilihat pada gambar IV.1.



Gambar IV.1 Responden yang memasukkan data pada web *phising*

IV.2.2 Hasil Tautan *Phising*

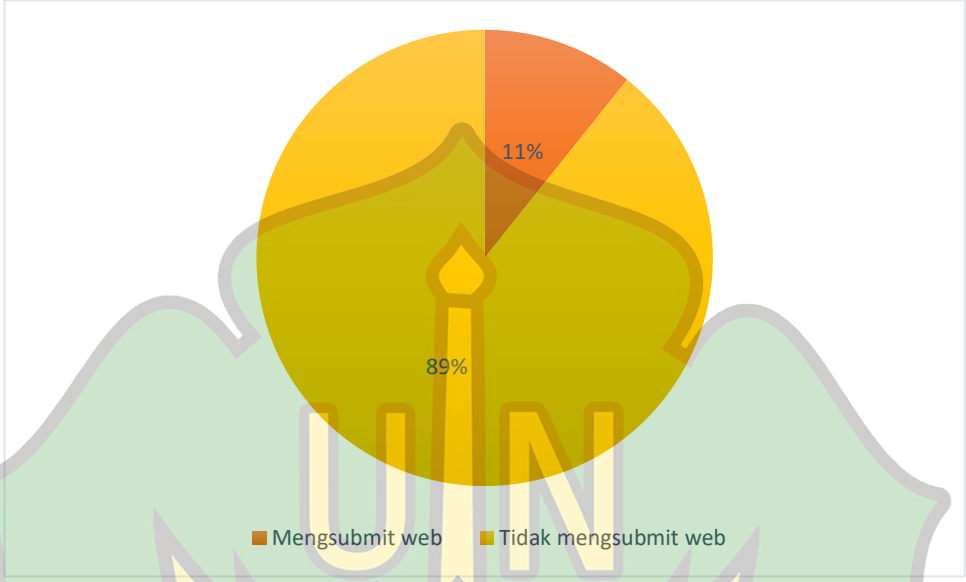
Setelah tautan *phising* disebarkan melalui media sosial whatsapp dan diberikan sedikit informasi mengenai tautan tersebut, kemudian peneliti dapat melihat responden yang mengakses tautan tersebut. Ternyata dari 121 orang responden ditemukan 96 orang responden yang mengakses tautan web *phising* tersebut. Respoden yang mengakses tautan *phising* dapat dilihat pada gambar IV.2.

Gambar IV.2 Responden yang mengakses tautan *phising*

IV.3 Hasil Analisis Deskriptif

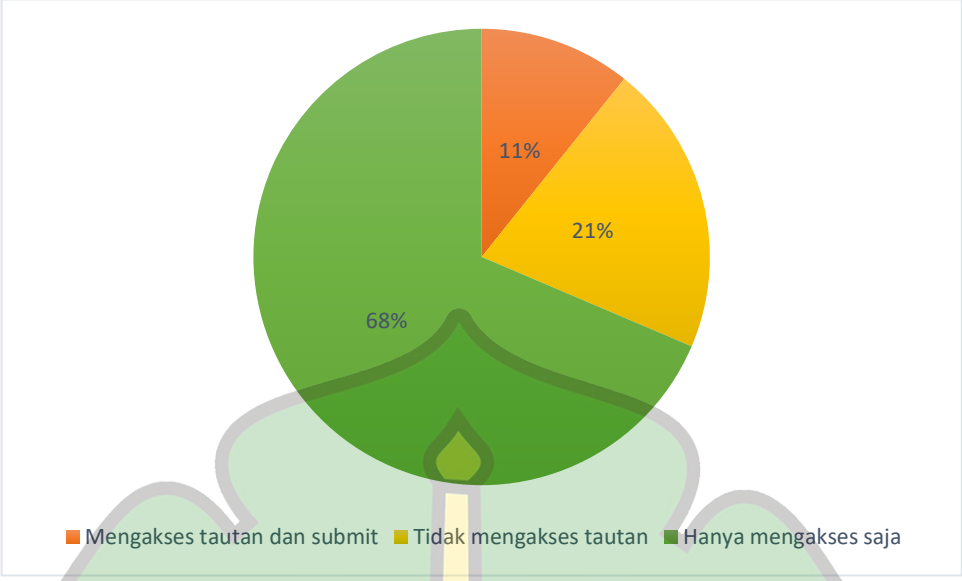
Hasil analisis deskriptif pada penelitian ini menujukkan bahwa responden yang memasukkan data pada web *phising* tersebut berjumlah 13 orang responden atau 10,7% dan yang tidak memasukkan data pada web *phising* tersebut berjumlah

108 orang responden atau 89,3% dari jumlah keseluruhan responden 121 orang responden. Hasil jawaban responden yang memasukkan data pada web *phising* dan tidaknya dapat dilihat pada gambar IV.3.



Gambar IV.3 Hasil responden web *phising*

Kemudian pada gambar IV.4 terdapat 13 orang responden atau 10,7% yang mengakses tautan lalu memasukkan data pada web *phising* tersebut, 83 orang responden atau 68,6% mengakses tautan tetapi tidak memasukkan 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 IV.4.



Gambar IV.4 Hasil responden tautan *phising*

BAB V
KESIMPULAN DAN SARAN

V.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan, dapat diambil kesimpulan yaitu sebagai berikut:

1. Berdasarkan hasil jawaban dari para responden yang memasukkan data pada web *phising* tersebut terdapat 13 orang responden atau 10,7% dan yang tidak memasukkan data pada web *phising* terdapat 108 orang responden atau 89,3%. Kemudian responden yang mengakses tautan *phising* dan memasukkan data terdapat 13 orang responden atau 10,7%, lalu 83 orang responden atau 68,6% yang mengakses tautan tetapi tidak memasukkan data pada web tersebut, dan tidak mengakses sama sekali terdapat 25 orang responden atau 20,7%. Artinya, mahasiswa Teknologi Informasi UIN Ar-raniry memiliki kesadaran tinggi terhadap serangan rekayasa sosial berbasis *phising*.

V.2 Saran

Adapun saran yang dapat dilaksanakan pada penelitian lainnya adalah:

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

DAFTAR PUSTAKA

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

Akraman, R., Candiwan, C., & Priyadi, Y. (2018). Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia. *Jurnal Sistem Informasi Bisnis*, *8*(2), 115. https://doi.org/10.21456/vol8iss2pp115-122

Batmetan, J. R., Kariso, B., Moningkey, M., & Tumembow, A. (2018). *Tingkat Kesadaran Privasi Atas Masalah Keamanan Informasi*. 4. https://doi.org/10.31219/OSF.IO/CAHZR

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

Fahmeyzan, D., Soraya, S., & Etmy, D. (2018). Uji Normalitas Data Omzet Bulanan Pelaku Ekonomi Mikro Desa Senggigi dengan Menggunakan Skewness dan Kurtosi. *Jurnal VARIAN*, *2*(1), 31–36. https://doi.org/10.30812/varian.v2i1.331

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.

Ir.Syofian Siregar, M. . (2013). *Metode Penelitian Kuantitatif* (Pertama). KENCANA.

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

Mutmainnah. (2018). *RESPON MAHASISWA JURUSAN KOMUNIKASI DAN PENYIARAN ISLAM UIN ALAUDDIN MAKASSAR TERHADAP HOAX DI MEDIA SOSIAL*. 1–185.

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.

Ramadhan, A., Alhafidh, M. A., & Firmansyah, M. D. (2022). Penyebaran Link Phising Kuota Kemendikbud Terhadap Kesadaran Informasi Pribadi Di Kalangan Mahasiswa UNINUS. *Kampret Journal*, *1*(1), 11–15. https://doi.org/10.35335/kampret.v1i1.9

Rochadiani, T. H., Santoso, H., Plaudo, D. A., Setiawan, R., & Fiones, V. G. (2021). *Peningkatan Literasi Digital Masyarakat Terhadap Social Engineering Dalam Masa Pandemi Covid-19*. *4*, 87–93.

Saputra, G. A. (2022). *TINJAUAN KRIMINOLOGI DAN HUKUM PIDANA ISLAM*.

Setiawan, A., Lusanjaya, G., & Kurnia, T. (2019). Kesadaran Keamanan Privasi Dan Masyarakat 5.0. *Journal of Accounting and Business Studies*, *4*(2), 1–12.

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

Soni, S., Afdhil Hafid, & Didik Sudyana. (2019). Analisis Kesadaran Mahasiswa Umri Terkait Penggunaan Teknologi & Media Sosial Terhadap Bahaya Cybercrime. *Jurnal Fasilkom*, *9*(3), 28–34. https://doi.org/10.37859/jf.v9i3.1664

Sugiyono. (2016). *METLIT SUGIYONO.pdf* (p. 336).

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).

Wahyudi, W. (2022). Analisis Motivasi Belajar Siswa Dengan Menggunakan Model Pembelajaran Blended Learning Saat Pandemi Covid-19 (Deskriptif Kuantitatif Di Sman 1 Babadan Ponorogo). *KadikmA*, *13*(1), 68. https://doi.org/10.19184/kdma.v13i1.31327

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.

LAMPIRAN

Lampiran 1: Kuesioner Penelitian

KUESIONER PENELITIAN

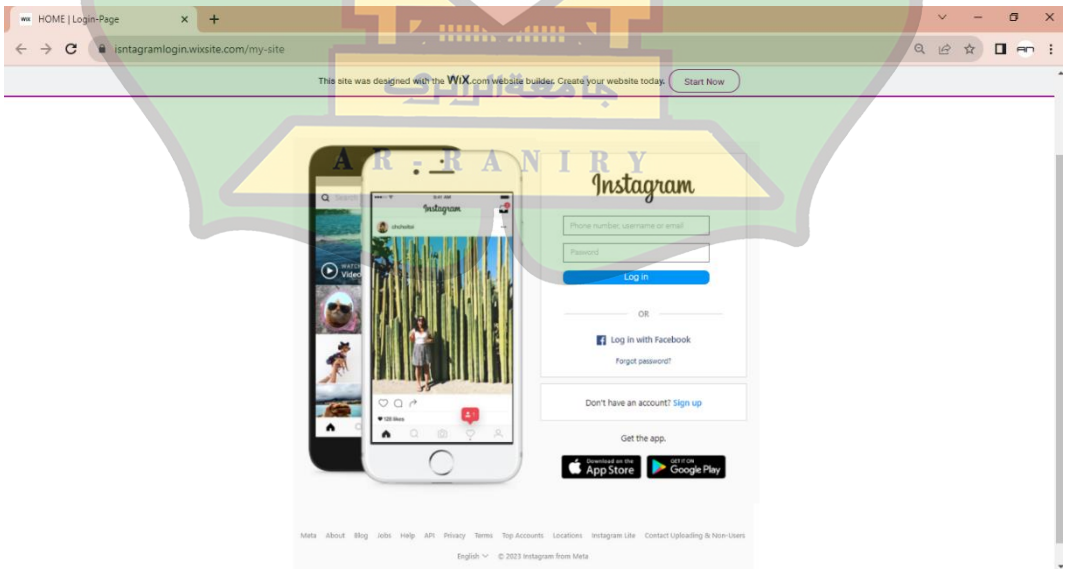
Assalamu'alaikum Bapak/Ibu dan rekan sekalian.

Sehubungan penyelenggaraan kegiatan Anugerah Academic Leaders 2023 oleh Ditjen Diktiristek Kemdikbudristek, agar mahasiswa dapat mendukung Bapak Mulkan pada penganugerahan tersebut dengan cara menyukai postingan di instagram dengan tautan berikut https://s.id/isntagramlogin.

Salah satu aspek penilaiannya ialah jumlah suport di platform instagram. Atas perhatian dan dukungannya, saya ucapkan terima kasih.

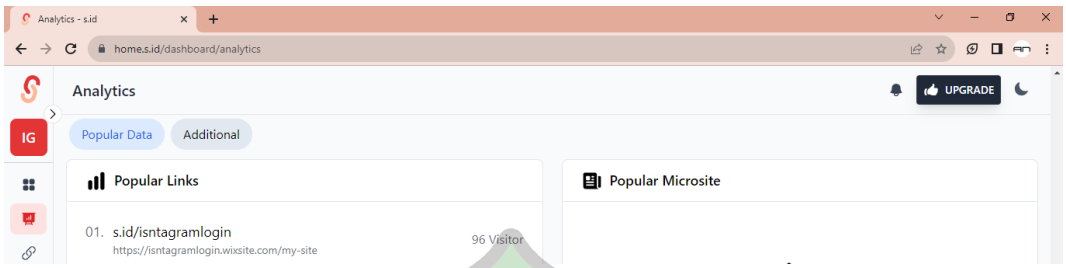
Lampiran 2 : Tampilan Web *Phising*

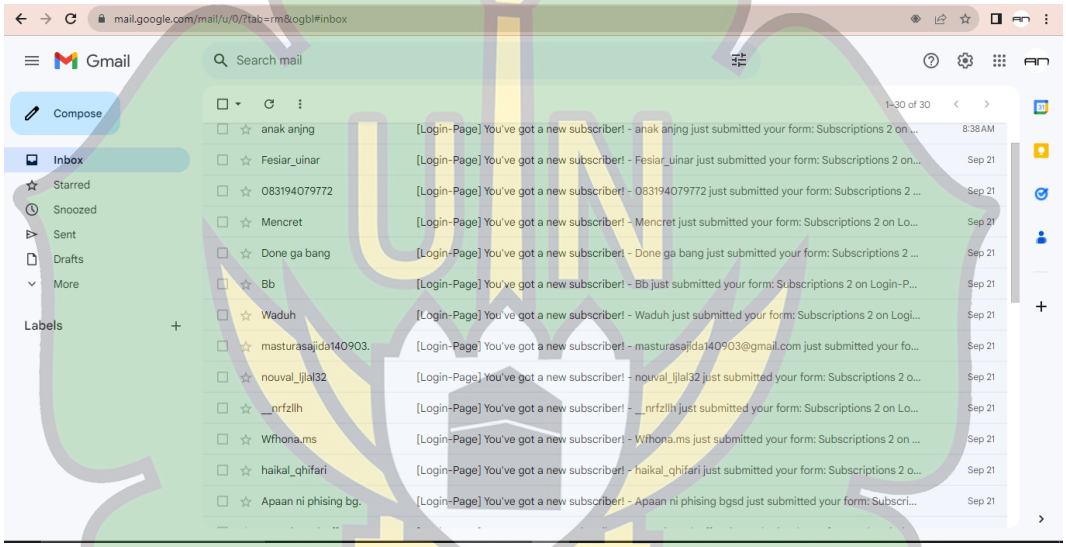
a. Dekstop



b. Mobile

lampiran 3 : Jawaban Responden





RIWAYAT HIDUP

Nura Nabilah lahir di Sigli, pada tanggal 2 April 2000. Anak kedua dari tiga bersaudara, dari pasangan Bapak Asnawi dan Ibu Raziah. Penulis menyelesaikan pendidikan Sekolah Dasar di SD Unggulan Iqro' Sigli dan lulus pada tahun 2012. Kemudian melanjutkan pendidikan di jenjang Sekolah Menengah Pertama di MTSN 1 Sigli dan lulus tahun 2015. Penulis menempuh pendidikan jenjang Sekolah Menengah Atas di MAN 1 Sigli dan lulus pada tahun 2018. Pada tahun yang sama penulis melanjutkan Strata-1 (S1) di perguruan Tinggi Negeri, tepatnya di Universitas Islam Negeri Ar-Raniry Fakultas Sains dan Teknologi pada Studi Teknologi Informasi.