SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

MENINGKATKAN KESADARAN MASYARAKAT AKAN ANCAMAN PHISHING MELALUI WHATSAPP (STUDI KASUS DI RT.001 DUSUN CIKOLE, DESA RANGGON)

TUGAS AKHIR

KURNIAWAN

0110220082

PROGRAM STUDI TEKNIK INFORMATIKA

DEPOK

AGUSTUS 2024

SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

MENINGKATKAN KESADARAN MASYARAKAT AKAN ANCAMAN PHISHING MELALUI WHATSAPP (STUDI KASUS DI RT.001 DUSUN CIKOLE, DESA RANGGON)

TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana

KURNIAWAN

0110220082

PROGRAM STUDI TEKNIK INFORMATIKA

DEPOK

AGUSTUS 2024

HALAMAN PERNYATAAN ORISINALITAS

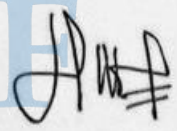
Skripsi/Tugas Akhir ini adalah hasil karya penulis, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama: Kurniawan

NIM : 0110220082

Depok, 25 Juni 2024

Tanda Tangan



Kurniawan

HALAMAN PENGESAHAN

Skripsi/Tugas Akhir ini diajukan oleh :

Nama : Kurniawan

NIM : 0110220082

Program Studi : Teknik Informatika

Judul Skripsi : MENINGKATKAN KESADARAN MASYARAKAT AKAN ANCAMAN PHISHING MELALUI WHATSAPP (STUDI KASUS DI RT.001 DUSUN CIKOLE, DESA RANGGON)

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Teknik Informatika Sekolah Tinggi Teknologi Terpadu Nurul Fikri

DEWAN PENGUJI

Pembimbing	Penguji
(APRIL RUSTIANTO, S.Komp., M.T.)	(EFRIZAL ZAIDA, S.KOM, M.M, M.KOM)

Ditetapkan di : Depok

Tanggal : 27 Juli 2024

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT, karena atas berkat dan rahmat-Nya, penulis dapat menyelesaikan skripsi/Tugas Akhir ini. Penulisan skripsi/Tugas Akhir ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana komputer Program Studi Teknik Informatika pada Sekolah Tinggi Teknologi Terpadu Nurul Fikri. Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi penulis untuk menyelesaikan skripsi/tugas akhir ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Allah SWT.
2. Orang tua dan semua anggota keluarga yang telah memberikan dorongan baik secara moril maupun materil dalam penyelesaian tugas ini.
3. Bapak Dr. Lukman Rosyidi selaku Ketua Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
4. Ibu TIFANI NABARIAN, S.Kom, M.T.i selaku Ketua Program Studi Teknik Informatika Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
5. Bapak Zaki Imaduddin, S.T, M.Kom. selaku Dosen Pembimbing Akademik yang telah membimbing penulis selama berkuliah di Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
6. Bapak APRIL RUSTIANTO, S.Komp., M.T selaku Dosen Pembimbing Tugas Akhir penulis dalam menyelesaikan penulisan ilmiah ini.
7. Para Dosen di lingkungan Sekolah Tinggi Teknologi Terpadu Nurul Fikri yang telah membimbing penulis dalam menuntut ilmu yang telah diberikan.
8. Pemerintah Desa Ranggon, Kepala Desa beserta karyawan yang telah meluangkan waktunya untuk memberikan data yang diperlukan bagi penulisan ilmiah ini.

Dalam penulisan ilmiah ini tentu saja masih banyak terdapat kekurangan-kekurangan yang mungkin disebabkan oleh keterbatasan kemampuan dan pengetahuan yang

penulis miliki. Walaupun demikian, penulis telah berusaha menyelesaikan penulisan ilmiah ini sebaik mungkin. Oleh karena itu apabila terdapat kekurangan di dalam penulisan ilmiah ini, dengan rendah hati penulis menerima kritik dan saran dari pembaca.

Akhir kata, penulis berharap Allah SWT berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga skripsi ini membawa manfaat bagi pengembangan ilmu.

Depok, 25 Juni 2024

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Sekolah Tinggi Teknologi Terpadu Nurul Fikri, saya yang bertanda tangan di bawah ini:

Nama : Kurniawan
NIM : 0110220082
Program Studi : Teknik Informatika
Jenis karya : Skripsi / Tugas Akhir

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada STT-NF **Hak Bebas Royalti Noneksklusif** (***Non-exclusive Royalty - Free Right***) atas karya ilmiah saya yang berjudul :

MENINGKATKAN KESADARAN MASYARAKAT AKAN ANCAMAN PHISHING MELALUI WHATSAPP (STUDI KASUS DI RT.001 DUSUN CIKOLE, DESA RANGGON) beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini STT-NF berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok
Pada tanggal : 9 Agustus 2024

Yang Menyatakan

(KURNIAWAN)

ABSTRAK

Nama : Kurniawan
NIM : 0110220082
Program Studi : Teknik Informatika
Judul : MENINGKATKAN KESADARAN MASYARAKAT AKAN ANCAMAN PHISHING MELALUI WHATSAPP (STUDI KASUS DI RT.001 DUSUN CIKOLE, DESA RANGGON)

Penelitian ini bertujuan untuk meningkatkan kesadaran masyarakat di RT. 001 Dusun Cikole, Desa Ranggon, terhadap ancaman *phishing* melalui aplikasi *WhatsApp* dengan pendekatan edukasi. Metode penelitian menggunakan pendekatan *pretest-posttest*. Peserta pertama-tama dinilai dengan kuesioner *pretest* untuk mengukur pengetahuan mereka tentang *phishing*. Selanjutnya, mereka menerima edukasi selama satu minggu melalui *WhatsApp* tentang definisi *phishing*, jenis-jenisnya, cara mengidentifikasinya, dan langkah-langkah pencegahannya. Setelah edukasi selesai, peserta mengisi kuesioner *posttest* yang sama untuk mengevaluasi peningkatan kesadaran mereka.

Hasil penelitian menunjukkan peningkatan signifikan dalam pengetahuan peserta tentang *phishing*, pemahaman akan risiko membuka link yang tidak dikenal, serta kesadaran akan tindakan yang harus diambil saat menerima pesan *phishing* setelah menerima edukasi. Pendekatan ini berhasil meningkatkan kesadaran terhadap ancaman *phishing* melalui aplikasi WhatsApp di wilayah yang diteliti.

Kata kunci : *phishing*, *WhatsApp*, edukasi, kesadaran, masyarakat

ABSTRACT

Name : Kurniawan
NIM : 0110220082
Study Program : *Informatics Engineering*
Title : *Enhancing Community Awareness of Phishing Threats via WhatsApp: A Case Study in RT. 001* Cikole *Hamlet,* Ranggon *Village*

This study aims to enhance community awareness in RT. 001 Cikole *Hamlet,* Ranggon *Village, regarding phishing threats through the WhatsApp application using an educational approach. The research employed a pretest-posttest approach. Participants initially underwent a pretest questionnaire to assess their knowledge of phishing. Subsequently, they received educational materials via WhatsApp for one week covering phishing definitions, types, identification methods, and preventive measures. After completing the education phase, participants filled out the same posttest questionnaire to evaluate the improvement in their awareness.*

The findings reveal a significant increase in participants' knowledge about phishing, understanding of the risks associated with clicking on unknown links, and awareness of appropriate actions to take upon receiving phishing messages post-education. This approach successfully heightened awareness of phishing threats through the WhatsApp application within the studied community.

Key words : *phishing, WhatsApp, education, awareness, community*

DAFTAR ISI

HALAMAN PERNYATAAN ORISINALITAS ii
HALAMAN PENGESAHAN iii
KATA PENGANTAR iv
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI vi
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS vi
ABSTRAK vii
ABSTRACT viii
DAFTAR ISI ix
DAFTAR GAMBAR xi
DAFTAR TABEL xiii
BAB I 1
PENDAHULUAN 1
1.1. Latar belakang 1
1.2. Rumusan Masalah 4
1.3. Tujuan 4
1.4. Manfaat 5
1.5. Batasan Masalah 6
1.6. Sistematika Penulisan 7
BAB II 11
KAJIAN LITERATUR 11
2.1. Definisi Variabel 11
2.2. Teori Analisis 12

BAB III 14
METODOLOGI PENELITIAN 14
3.1. Tahapan Penelitian 14
3.2. Jenis Penelitian 16
3.3. Metode Analisis Data 17
3.4. Metode Pengujian Data 17
3.5. Proses Edukasi 19
BAB IV 27
IMPLEMENTASI DAN EVALUASI 27
4.1.Rancangan Penelitian 27
4.2. Hasil Implementasi 30
4.4. Analisis Hasil 33
BAB V 38
KESIMPULAN DAN SARAN 38
5.1. Kesimpulan 38
5.2. Saran 38
DAFTAR PUSTAKA 40
LAMPIRAN 42

DAFTAR GAMBAR

Gambar 1. 1 Statistik Rincian Modus [14] 2
Gambar 1. 2 Statistik Jenis Media Sosial [15] 2
Gambar 1. 3 Statistik Kasus Phising di Indonesia [16] 3
Gambar 3. 1 Tahapan Penelitian 14
Gambar 3. 2 Materi edukasi hari ke-1 20
Gambar 3. 3 Edukasi video pendek 21
Gambar 3. 4 Edukasi video pendek (1) 21
Gambar 3. 5 Edukasi video pendek (2) 21
Gambar 3. 6 Edukasi video pendek (3) 22
Gambar 3. 7 Edukasi video pendek (4) 22
Gambar 3. 8 Edukasi video pendek (5) 22
Gambar 3. 9 Edukasi video pendek (6) 23
Gambar 3. 10 Edukasi video berita kasus phishing 23
Gambar 3. 11 Edukasi video langkah langkah menghindari phishing 24
Gambar 3. 12 Dampak phishing 24
Gambar 3. 13 Ringkasan materi edukasi 24
Gambar 3. 14 Halaman utama web 25
Gambar 3. 15 Halaman data berhasil disimpan 25
Gambar 4. 1 Rumus Slovin 28
Gambar 4. 2 Diagram alir penelitian 29
Gambar 4. 3 Data kuisioner pretest responden 1-29 30
Gambar 4. 4 Data kuisioner pretest responden 30-50 31
Gambar 4. 5 Rumus dasar menghitung persentasi 31
Gambar 4. 6 Data kuisioner posttest responden 1 – 29 32
Gambar 4. 7 Data kuisioner posttest responden 30 – 50 33
Gambar 4. 8 Grafik Perbandingan 36

Gambar A. 1 42
Gambar A. 2 42
Gambar A. 3 42
Gambar A. 4 43
Gambar A. 5 43
Gambar A. 6 43
Gambar A. 7 44
Gambar A. 8 44
Gambar A. 9 44
Gambar A. 10 45
Gambar A. 11 45
Gambar A. 12 45
Gambar A. 13 46

DAFTAR TABEL

Tabel 2. 1 Penelitian terkait 13
Tabel 4. 2 Pengetahuan phsihing 33
Tabel 4. 3 Tingkat pemahaman phsihing 33
Tabel 4. 4 Sumber informasi phsihing 34
Tabel 4. 5 Pengalaman pesan mencurigakan 34
Tabel 4. 6 Respon terhadap pesan mencurigakan 34
Tabel 4. 7 Pemahaman pencegahan phishing 35
Tabel 4. 8 Keyakinan mengenali pesan phishing 35
Tabel 4. 9 Keinginan meningkatkan pengetahuan 36

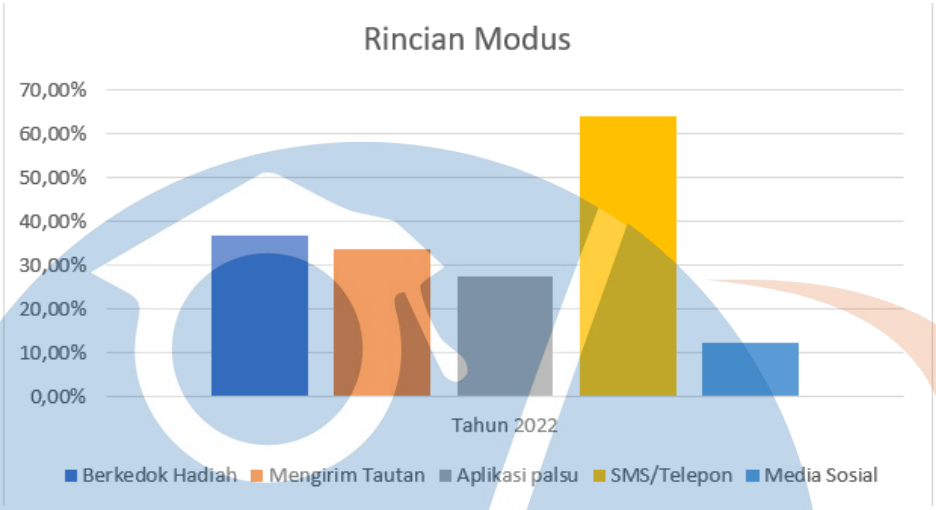
BAB I
PENDAHULUAN

1.1. Latar belakang

Manfaat perkembangan teknologi informasi dan komunikasi (TIK) dirasakan di kalangan masyarakat, khususnya di RT. 001 Dusun Cikole, Desa Ranggon. Teknologi informasi dapat membawa perubahan dalam praktik dan perubahan pemikiran. Hal ini mengubah cara masyarakat berinteraksi, berkomunikasi dan menjalani kehidupan sehari-hari[1]. Masyarakat saat ini sudah benar-benar menjadi budak teknologi[2]. Namun perkembangan tersebut membawa tantangan baru dengan munculnya berbagai kejahatan siber yang dilakukan oleh aktor yang bertujuan untuk mengeksploitasi kelemahan sistem dan kesadaran pengguna sistem informasi[3]. Di dunia nyata seseorang bisa masuk ke rumah orang lain dan mengambil barang berharga dari rumah orang tersebut, sedangkan di dunia maya seseorang bisa mengakses komputer atau jaringan komputer orang lain dan mengambil datanya[4].

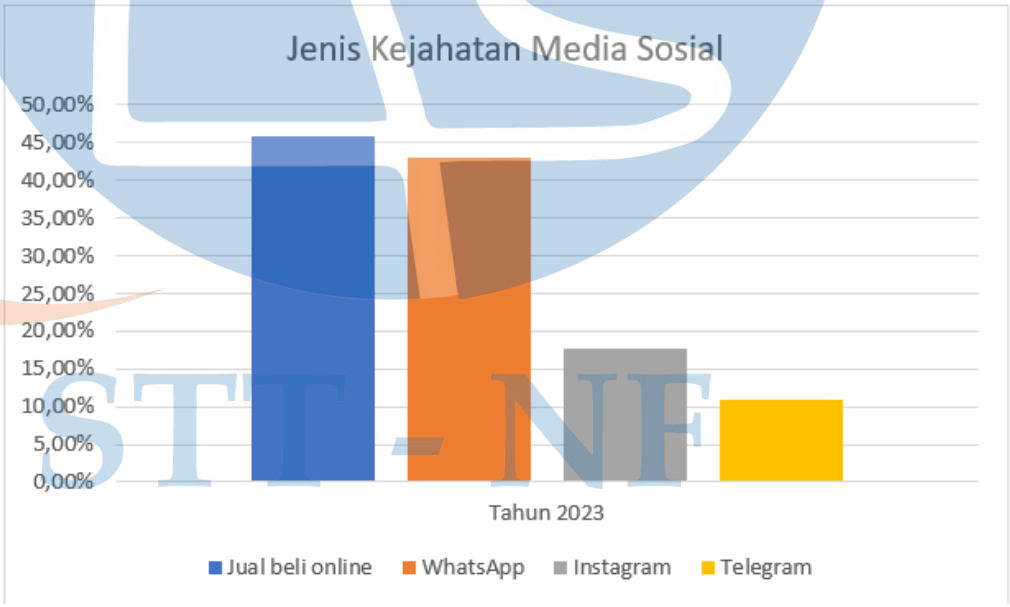
Carding, *hacking*, *phising*, dan penyebaran informasi yang mengganggu adalah contoh kejahatan dunia maya[5]. *Phising* merupakan aktivitas kriminal yang menggunakan teknik rekayasa sosial. *Phisher* (istilah yang digunakan untuk merujuk pada penjahat *phising*) menyamar sebagai organisasi tepercaya dalam komunikasi elektronik dalam upaya mengelabui dan mendapatkan informasi sensitif seperti nama pengguna, kata sandi, dan rincian kartu kredit [3]. Trik yang dilakukan pelaku adalah dengan mengajak korban membuka website atau mengirimkan pesan *WhatsApp* yang telah dibuat sebelumnya oleh pelaku[6].

Berikut data statistik rincian modus terjadinya kejahatan dunia maya pada tahun 2022:



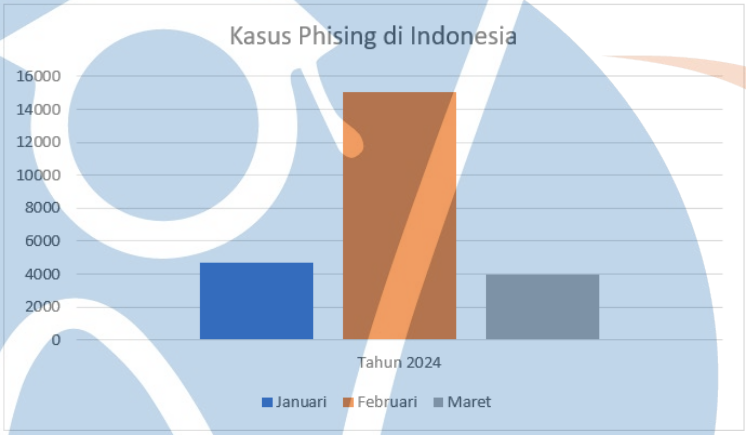
Gambar 1. 1 *Statistik Rincian Modus* [14]

Dari gambar statistik di atas kita dapat melihat, bahwa pada tahun 2022 kasus terbanyak adalah melalui SMS/Telepon. Kemudian berikut statistik jenis kejahatan media sosial. Kemudian statistik jenis kejahatan media social tahun 2023:



Gambar 1. 2 Statistik Jenis Media Sosial [15]

Dapat kita lihat, jumlah kejahatan yang terjadi di jual beli *online* adalah 45.87%, WhatsApp 42.89%, Instagram 17.62%, dan Telegram 10.95%. Kejahatan *cyber* melalui whatsapp berada di posisi kedua. Whatsapp merupakan aplikasi pesan instan yang dibuat oleh Facebook dan merupakan salah satu aplikasi media sosial populer[7]. Berikut statistik terjadinya kasus *phising* di Indonesia 3 bulan terakhir tahun 2024.



Gambar 1. 3 Statistik Kasus *Phising* di Indonesia [16]

Kasus serangan *phising* paling banyak terjadi di bulan Februari dengan jumlah 15.050 kasus. Sementara, jumlah di bulan Januari hanya sekitar 4.665 kasus dan di bulan Maret sebanyak 3.960 kasus.

Alasan mendesak untuk melakukan penelitian di RT. 001 Dusun Cikole, Desa Ranggon, terkait ancaman *phishing* melalui aplikasi *WhatsApp*, adalah karena meningkatnya kasus penipuan siber di wilayah tersebut. Data awal menunjukkan bahwa masyarakat di RT. 001 Dusun Cikole, Desa Ranggon, sering menjadi target serangan *phishing*, namun tingkat kesadaran dan pengetahuan mereka tentang ancaman ini masih rendah. *Phishing* melalui *WhatsApp* telah menyebabkan beberapa insiden kehilangan data pribadi dan kerugian finansial yang signifikan. Oleh karena itu, penting untuk segera melakukan penelitian ini untuk mengidentifikasi sejauh mana masyarakat menyadari ancaman ini, metode umum yang digunakan dalam serangan *phishing*, serta efektivitas pendekatan edukasi dalam meningkatkan kesadaran dan pengetahuan tentang keamanan digital. Penelitian ini terletak pada beberapa aspek utama. Pertama,

penelitian ini akan memberikan pemahaman yang lebih baik tentang tingkat kesadaran masyarakat di RT. 001 Dusun Cikole, Desa Ranggon terhadap ancaman *phising*. Kedua, dengan menggunakan WhatsApp sebagai platform untuk penyebaran informasi dan edukasi, penelitian ini akan mengevaluasi efektivitas media tersebut dalam meningkatkan kesadaran dan pemahaman masyarakat tentang keamanan siber. Ketiga, hasil penelitian ini diharapkan dapat memberikan rekomendasi yang konkret bagi pemerintah daerah, lembaga pendidikan, dan komunitas lokal dalam mengembangkan strategi edukasi yang efektif untuk mencegah serangan *phising* di masa depan.

Perlunya peningkatan kesadaran masyarakat terhadap ancaman *phising* melalui *WhatsApp* sangat penting untuk melindungi pengguna dari serangan *cyber* yang merugikan. Banyak pengguna media sosial yang tidak memikirkan ancaman tersebut. Mereka menganggap ini hanya masalah kecil dan tidak perlu dipermasalahkan[8]. Dengan pemahaman yang lebih baik tentang taktik penipuan yang digunakan dan langkah-langkah pencegahan yang dapat diambil, masyarakat dapat mengurangi resiko menjadi korban serangan *phising* di *WhatsApp*. Oleh karena itu, penelitian ini diharapkan dapat memberikan kontribusi yang signifikan dalam upaya melawan kejahatan *cyber* yang semakin meresahkan ini.

1.2. Rumusan Masalah

1. Bagaimana tingkat kesadaran masyarakat RT. 001 Dusun Cikole, Desa Ranggon tentang ancaman *phising* melalui aplikasi *WhatsApp*?
2. Apakah pendekatan edukasi dapat meningkatkan kesadaran masyarakat RT. 001 Dusun Cikole, Desa Ranggon tentang ancaman *phising* di *WhatsApp*?

1.3. Tujuan

1. Menganalisis Tingkat Kesadaran Masyarakat di RT. 001 Dusun Cikole, Desa Ranggon terhadap Ancaman *Phising* melalui *WhatsApp*. Bertujuan untuk memahami sejauh mana masyarakat di RT. 001 Dusun Cikole, Desa Ranggon menyadari ancaman *phising* yang disebarkan melalui aplikasi *WhatsApp*.

2. Meneliti Efektivitas Pendekatan Edukasi dalam Meningkatkan Kesadaran Masyarakat tentang Ancaman *Phising* di *WhatsApp* di RT. 001 Dusun Cikole, Desa Ranggon.

1.4. Manfaat

1. Manfaat Teoritis

Pengembangan Ilmu Pengetahuan: Penelitian ini akan menambah literatur tentang ancaman *phising* khususnya dalam konteks penggunaan aplikasi *WhatsApp* di Indonesia. Hasil penelitian dapat digunakan sebagai referensi bagi peneliti lain yang tertarik untuk mengeksplorasi lebih lanjut isu keamanan siber dan kesadaran masyarakat terhadap ancaman *phising*.

2. Manfaat Praktis

Masyarakat Umum di RT. 001 Dusun Cikole, Desa Ranggon

i. Peningkatan Kesadaran: Dengan meningkatnya kesadaran masyarakat mengenai ancaman *phising* melalui *WhatsApp*, mereka akan lebih waspada dan mampu mengidentifikasi serta menghindari upaya penipuan siber. Hal ini dapat mengurangi risiko kehilangan data pribadi dan kerugian finansial.

ii. Pengetahuan Keamanan Digital: Program edukasi yang diimplementasikan akan memberikan pengetahuan praktis tentang keamanan digital, sehingga masyarakat dapat mengadopsi praktik keamanan yang lebih baik dalam kehidupan sehari-hari.

Pemerintah Desa Ranggon

i. Strategi Edukasi yang Efektif: Hasil penelitian ini dapat menjadi dasar bagi pemerintah daerah untuk merancang dan mengimplementasikan program-program edukasi yang lebih efektif dalam meningkatkan kesadaran keamanan siber di kalangan warganya.

ii. Kebijakan Keamanan Siber: Temuan penelitian dapat membantu pemerintah daerah dalam merumuskan kebijakan yang lebih baik terkait keamanan siber dan perlindungan data di wilayahnya.

Lembaga Pendidikan

i. Pelatihan dan Workshop: Lembaga pendidikan dapat mengadakan pelatihan dan workshop berdasarkan temuan penelitian untuk meningkatkan literasi digital siswa dan staf pengajar.

Penegak Hukum

i. Pendukung Investigasi: Informasi mengenai metode umum serangan *phising* dan data kesadaran masyarakat dapat membantu penegak hukum dalam melakukan investigasi kasus *phising* lebih efektif dan menyusun strategi pencegahan yang lebih baik.

3. Manfaat bagi Peneliti

Pengalaman Penelitian: Peneliti akan mendapatkan pengalaman berharga dalam melakukan penelitian lapangan, analisis data, dan evaluasi program edukasi, yang semuanya akan meningkatkan keterampilan dan kompetensi dalam bidang penelitian keamanan siber.

1.5. Batasan Masalah

a. Lokasi Penelitian

Penelitian ini dibatasi pada wilayah RT. 001 Dusun Cikole, Desa Ranggon. Data yang dikumpulkan dan dianalisis hanya mencakup masyarakat yang berdomisili di daerah tersebut.

b. Populasi dan Sampel

Penelitian ini hanya mencakup pengguna *WhatsApp* yang berada di RT. 001 Dusun Cikole, Desa Ranggon. Sampel diambil dari berbagai kelompok demografis seperti usia, jenis kelamin, dan pekerjaan untuk mendapatkan gambaran yang representatif. Penduduk yang menjadi fokus penelitian adalah mereka yang berusia 19-50 tahun, berjumlah 98 orang. Berdasarkan perhitungan menggunakan rumus Slovin dengan tingkat kepercayaan 95% dan margin of error 10%, sampel yang diperlukan adalah 50 responden.

c. Platform dan Aplikasi

Fokus utama penelitian ini adalah pada aplikasi *WhatsApp* versi terbaru yang digunakan oleh masyarakat di RT. 001 Dusun Cikole, Desa Ranggon. Penelitian tidak mencakup aplikasi pesan instan lainnya atau versi *WhatsApp* yang usang.

d. Jenis Ancaman *Phising*

Penelitian ini hanya meneliti metode umum serangan *phising* yang terjadi melalui *WhatsApp*. Bentuk ancaman siber lainnya seperti *malware* atau *ransomware* tidak termasuk dalam lingkup penelitian ini.

e. Tools untuk Pengumpulan Data

- Survei: Pengumpulan data dilakukan menggunakan survei *online* yang disebarkan melalui *Google Forms*
- Analisis Kasus: Studi kasus diambil dari insiden *phising* yang dilaporkan di RT. 001 Dusun Cikole, Desa Ranggon.

f. Periode Waktu

Penelitian ini dibatasi pada data yang dikumpulkan selama periode enam bulan, dari Januari 2024 hingga Juni 2024. Data dan insiden di luar periode ini tidak termasuk dalam analisis.

g. Bahasa dan Instrumen

Penelitian ini menggunakan instrumen yang disusun dalam bahasa Indonesia. Semua survei, materi edukasi disajikan dalam bahasa Indonesia untuk memastikan pemahaman yang maksimal oleh responden di RT. 001 Dusun Cikole, Desa Ranggon.

1.6. Sistematika Penulisan

BAB I PENDAHULUAN

1.1 Latar belakang

Dalam bagian ini berisi pengantar tentang perkembangan Teknologi Informasi dan Komunikasi (TIK), dampak positif perkembangan TIK di kalangan masyarakat, perubahan sosial, perubahan praktik dan pemikiran masyarakat. Setelah itu menggambarkan berbagai bentuk kejahatan siber,dan contoh cara phisher beroperasi, seperti mengirimkan pesan *WhatsApp* dengan tautan berbahaya.

1.2. Rumusan Masalah

Penelitian ini berusaha untuk menjawab pertanyaan-pertanyaan berikut:

1. Bagaimana tingkat kesadaran masyarakat RT. 001 Dusun Cikole, Desa Ranggon tentang ancaman *phising* melalui aplikasi WhatsApp?

2. Bagaimana pendekatan edukasi dapat meningkatkan kesadaran masyarakat RT. 001 Dusun Cikole, Desa Ranggon tentang ancaman *phising* di WhatsApp?

1.3 Tujuan

Menganalisis, mengidentifikasi, dan meneliti tingkat kesadaran masyarakat di RT. 001 Dusun Cikole, Desa Ranggon

1.4 Manfaat

Memberikan penjelasan mengenai manfaat penelitian ini, baik itu manfaat teoritis maupun praktis.

1.5 Batasan Masalah

Penelitian ini dibatasi pada wilayah RT. 001 Dusun Cikole, Desa Ranggon, dengan populasi yang mencakup pengguna *WhatsApp*. Fokus utamanya adalah aplikasi *WhatsApp* versi terbaru, dan penelitian hanya meneliti metode umum serangan *phising* melalui platform tersebut.

1.6 Sistematika Penulisan

Dalam bagian ini berisi sistematika penulisan.

BAB II KAJIAN LITERATUR

Kajian literatur dalam penelitian ini mencakup definisi variabel, teori analisis, serta teknologi dan aplikasi yang relevan untuk meningkatkan kesadaran masyarakat di RT.001 Dusun Cikole, Desa Ranggon.

BAB III METODE PENELITIAN

3.1 Tahapan Penelitian

Berisi tahapan tahapan yang akan dilakukan dalam penulisan seperti studi pustaka, tingkat kesadaran masyarakat, dan pendekatan edukasi yang efektif dalam meningkatkan kesadaran akan keamanan digital.

3.2 Jenis Penelitian

Penelitian ini adalah studi deskriptif yang bertujuan untuk menggambarkan tingkat kesadaran masyarakat tentang ancaman *phishing* melalui aplikasi WhatsApp di RT. 001 Dusun Cikole, Desa Ranggon.

3.3 Metode Analisis Data

Data survei akan dianalisis menggunakan metode statistik deskriptif. Analisis ini akan memberikan gambaran yang jelas tentang distribusi dan karakteristik respons dari sampel penelitian.

3.4 Metode Pengujian Data

Pengujian data akan dilakukan melalui beberapa tahap, yaitu *pre-test*, intervensi edukasi, dan *post-test.*

3.5 Proses Edukasi

Proses edukasi dalam penelitian ini melibatkan beberapa tahapan yang dirancang untuk meningkatkan kesadaran masyarakat terhadap ancaman *phishing*. Proses ini dilakukan melalui platform *WhatsApp*, yang merupakan media komunikasi yang banyak digunakan oleh masyarakat di Dusun Cikole, RT 001, Desa Ranggon.

BAB IV IMPLEMENTASI DAN EVALUASI

4.1 Rancangan Penelitian

Rancangan penelitian ini dirancang untuk mengukur efektivitas program edukasi *phishing* yang dilaksanakan melalui platform *WhatsApp*. Penelitian ini dibagi menjadi beberapa tahap, yaitu *pretest*, edukasi, dan *posttest*

4.2 Hasil Implementasi

Bagian ini berisi data hasil kuisioner *pre-test* dan *post-test* yang telah diisi oleh masyarakat Dusun Cikole, RT 001, Desa Ranggon.

4.3 Analisis Hasil

Pre-test dan *post-test* di analisis kemudian diberikan perbandingan mengenai perubahan kesadaran masyarakat Dusun Cikole, RT 001, Desa Ranggon.

BAB V KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dalam bagian ini, akan disajikan kesimpulan mengenai dua aspek utama dari penelitian ini, yaitu tingkat kesadaran masyarakat RT. 001 Dusun Cikole, Desa

Ranggon akan ancaman *phishing*. Kesimpulan pertama menyoroti rendahnya tingkat kesadaran masyarakat sebelum edukasi diberikan, Kesimpulan kedua menjelaskan efektivitas pendekatan edukasi.

5.2 Saran

Dalam bagian ini, disajikan saran untuk penelitian selanjutnya berdasarkan hasil penelitian yang telah dilaksanakan mengenai peningkatan kesadaran masyarakat RT. 001 Dusun Cikole, Desa Ranggon.

DAFTAR PUSTAKA

BAB II
KAJIAN LITERATUR

2.1. Definisi Variabel

2.1.1. Kesadaran Masyarakat tentang *Phising* melalui *WhatsApp*

Merujuk pada pemahaman dan pengetahuan yang dimiliki masyarakat tentang ancaman *phising* yang dapat terjadi melalui aplikasi *WhatsApp*, termasuk pemahaman tentang taktik-taktik penipuan yang umum digunakan[13].

2.1.2. Phising

Merupakan kampanye *email* dan pesan teks yang dimaksudkan untuk membuat korban merasa terancam atau penting. Selanjutnya, hal ini mendorong mereka untuk mengungkapkan data pribadi, mengklik tautan ke situs *web* berbahaya, atau membuka lampiran yang mengandung *malware*. Salah satu contohnya adalah *email* yang dikirimkan kepada pengguna layanan internet yang memberi tahu mereka tentang pelanggaran peraturan yang memerlukan tindakan segera, seperti perubahan kata sandi yang diperlukan. Ini memasukkan tautan ke situs *web* yang tidak sah, yang tampak hampir sama dengan situs *web* yang sah. Ini mendorong pengguna yang tidak berhati-hati untuk memasukkan kata sandi dan kredensial baru mereka saat ini. Setelah mengisi formulir, data dikirim ke penyerang[9].

2.1.3. Aplikasi *WhatsApp*

Merupakan aplikasi berbasis internet yang paling banyak digunakan sebagai media komunikasi. Selain mudah digunakan dan populer, fitur pendukungnya memungkinkan penggunanya untuk berbagi informasi dan berbagai konten[10].

2.1.4. Kesadaran

Kesadaran adalah kesiagaan seseorang terhadap peristiwa-peristiwa di lingkungannya (seperti pemandangan dan suara-suara dari lingkungan sekitarnya) serta peristiwa-peristiwa kognitif yang meliputi memori, pikiran, perasaan, dan sensasi-sensasi fisik (Suparwi, 2020).

2.1.5. Masyarakat

Masyarakat adalah sekumpulan orang yang hidup dalam lingkungan sosial tertentu selama waktu tertentu. Lingkungan sosial ini menghasilkan hubungan sosial di mana orang-orang saling berinteraksi dalam kotak sosial dan memiliki beragam kepentingan yang sama.

2.2. Teori Analisis

2.2.1. Teori Sosial dalam Keamanan *Cyber*

Teori ini akan digunakan untuk memahami faktor-faktor sosial yang mempengaruhi tingkat kesadaran dan perilaku masyarakat terkait dengan praktik keamanan *cyber*, termasuk respons terhadap ancaman *phising* di WhatsApp. Afandi dkk. (2017) meneliti kesadaran dan keamanan pengguna media sosial di Indonesia. Hasil penelitian menunjukkan bahwa persepsi pengguna terhadap ancaman keamanan (persepsi ancaman keamanan) adalah faktor yang memengaruhi perilaku kesadaran dan keamanan (*awareness & security behavior*) pengguna media sosial *Line*[11].

2.2.2. Teori Belajar dan Pendidikan

Teori *Behaviorisme* (B.F. Skinner): Menekankan pentingnya penguatan positif dalam proses belajar. Survei *pretest* dan *posttest* digunakan untuk mengukur efektivitas edukasi sebagai bentuk penguatan. Teori *Behaviorisme* merupakan salah satu pendekatan yang paling berpengaruh dalam psikologi dan pendidikan. Teori ini menekankan bahwa perilaku manusia dapat dijelaskan sebagai respon terhadap stimulus tertentu di lingkungan mereka.

2.2.3. Teori Slovin

Dalam penelitian survei, penentuan ukuran sampel yang tepat adalah salah satu langkah penting untuk memastikan bahwa hasil yang diperoleh dapat dipercaya dan merepresentasikan populasi yang lebih besar. Salah satu metode yang sering digunakan untuk menentukan ukuran sampel adalah dengan menggunakan rumus Slovin. Rumus ini dirancang untuk memberikan perkiraan ukuran sampel yang diperlukan berdasarkan ukuran populasi dan *margin of error* yang diinginkan.

2.2.4. Teknologi dan Aplikasi

1. Metode Survei *Online*: Penelitian ini akan menggunakan survei *online* untuk mengumpulkan data dari responden tentang tingkat kesadaran mereka tentang *phising* di *WhatsApp*, preferensi mereka terkait metode pendekatan edukasi, serta perilaku mereka dalam menghadapi ancaman *phising*.

2. Pendekatan Edukasi *Digital*: Pendekatan ini akan melibatkan penggunaan berbagai platform *online* seperti situs *web*, media sosial, dan aplikasi berbagi video untuk menyampaikan informasi tentang ancaman *phising* dan praktik keamanan cyber kepada masyarakat pengguna WhatsApp secara efektif dan menarik.

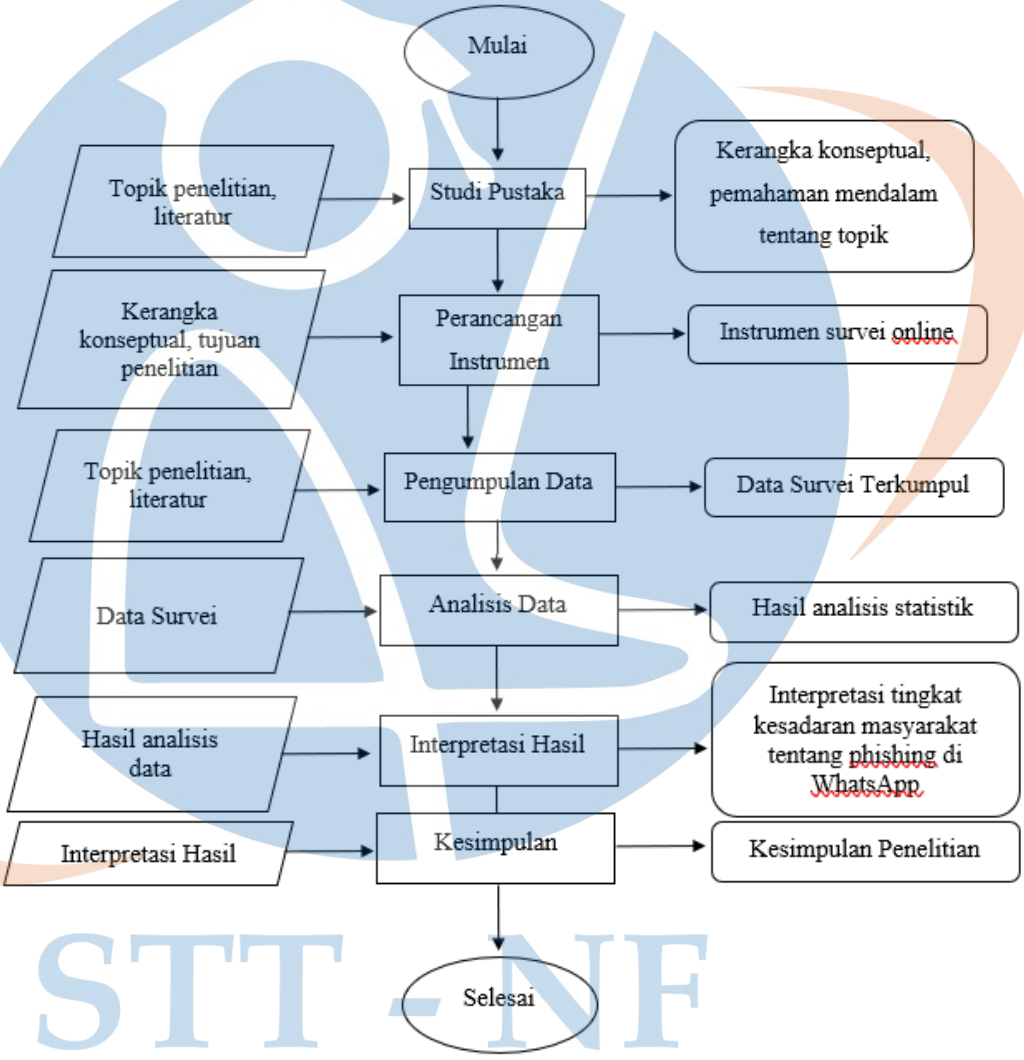
Tabel 2. 1 Penelitian terkait

No	Nama dan Tahun	Judul	Topik	Subjek	Hasil
1	Gustina, Dian, Aisyah, Nurul Syah Putra, Arman, Valentino, VH, Sriyono Prasetyo, Budhi, 2022	Analisis Penyadapan pada Aplikasi *WhatsApp* Menggunakan Sinkronisasi Data	Penyadapan *WhatsApp*	Masyarakat	Pemahaman Terhadap Potensi Penyadapan
2	Firdausiah Ersa, Lutfiah, Aningsih, Gusti, Hidayat, Taufik, Febri Sonni, Alem, 2024	Analisis Jaringan Komunikasi Penipuan Daring Melalui Media Sosial *Whatsapp* Messenger	Penipuan Daring	Masyarakat	Pemahaman Mengenai Penipuan Media Sosial *Whatsapp Messenger*
3	Mia Haryati Wibowo,Nur Fatimah, 2017	Ancaman *Phising* Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime	*Phising* Terhadap Pengguna Sosial Media	Masyarakat	Pemahaman Mengenai *Phising* terhadap Pengguna Sosial Media
4	Nunu Vadila, Ahmad R. Pratama,	Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Indonesia	Cybersecurity Pada Pengguna Media Sosial	Pengguna Media Sosial	Analisis data tingkat kesadaran pada pengguna media sosial

BAB III
METODOLOGI PENELITIAN

3.1. Tahapan Penelitian

Berikut ini merupakan tahapan tahapan yang akan dilakukan dalam penulisan:



Gambar 3. 1 Tahapan Penelitian

3.1.1. Studi Pustaka

Studi pustaka akan dilakukan untuk memahami secara mendalam tentang fenomena *phishing*, tingkat kesadaran masyarakat, dan pendekatan edukasi yang efektif dalam meningkatkan kesadaran akan keamanan digital. Hasil studi pustaka

ini akan menjadi dasar untuk merancang instrumen penelitian dan menentukan kerangka kerja penelitian.

3.1.2. Perancangan Instrumen

Berdasarkan temuan dari studi pustaka, instrumen penelitian akan dirancang untuk mengumpulkan data yang dibutuhkan. Instrumen ini mungkin berupa kuesioner untuk mengukur tingkat pengetahuan dan kesadaran masyarakat terhadap *phishing*, serta faktor-faktor yang memengaruhi perilaku mereka terkait keamanan digital.

3.1.3. Pengumpulan Data

Tahap pengumpulan data akan melibatkan serangkaian kegiatan yang dirancang untuk mendapatkan informasi yang diperlukan dari responden. Langkah-langkah yang akan diambil dalam tahap ini adalah sebagai berikut:

Persiapan Survei: Survei akan disiapkan berdasarkan instrumen penelitian yang telah dirancang sebelumnya. Survei ini akan mencakup pertanyaan yang relevan dengan tujuan penelitian, termasuk pertanyaan tentang pengetahuan tentang *phishing*, pengalaman pribadi dengan serangan *phishing*, dan pendapat tentang keamanan digital.

a. Pengiriman Survei: Survei akan dikirim kepada responden melalui *WhatsApp*. Komunikasi yang jelas akan disampaikan kepada responden mengenai tujuan survei, anonimitas, dan pentingnya partisipasi mereka.

b. Pengumpulan Data Secara *Online*: Untuk responden yang memilih untuk berpartisipasi secara online, data akan dikumpulkan melalui platform survei daring. Hal ini akan memudahkan proses pengumpulan dan pengelolaan data, serta meminimalkan kesalahan input.

c. Pelacakan dan Pengingat: Untuk memastikan tingkat respons yang tinggi, pengingat berkala akan dikirim kepada responden yang belum mengisi survei. Hal ini akan membantu dalam meningkatkan tingkat partisipasi dan keberhasilan pengumpulan data.

d. Pemrosesan Data: Data yang telah terverifikasi akan diproses menggunakan perangkat lunak analisis data yang sesuai. Data mentah akan diubah menjadi bentuk yang dapat dianalisis untuk langkah berikutnya dalam penelitian.

3.1.4. Analisis Data

Data yang terkumpul akan diolah dan dianalisis menggunakan metode statistik (untuk data kuantitatif) dan analisis tematik (untuk data kualitatif) untuk mengidentifikasi pola, hubungan, dan tema utama. Hasil analisis akan diinterpretasikan dan disajikan secara ringkas dalam laporan penelitian. Penelitian kuantitatif adalah kemampuan untuk menggeneralisasi temuan penelitian atau seberapa jauh temuan tersebut dapat diterapkan pada populasi tertentu[13].

3.1.5. Iterpretasi

Hasil analisis data akan diinterpretasikan untuk mengevaluasi tingkat kesadaran masyarakat terhadap *phishing* dan efektivitas pendekatan edukasi yang digunakan melalui *WhatsApp*. Interpretasi data ini akan membantu dalam memahami implikasi temuan penelitian terhadap upaya meningkatkan kesadaran masyarakat akan keamanan digital.

3.1.5. Kesimpulan

Berdasarkan hasil interpretasi data, kesimpulan akan ditarik untuk merangkum temuan utama penelitian ini. Kesimpulan ini akan memberikan gambaran tentang sejauh mana pendekatan edukasi melalui *WhatsApp* efektif dalam meningkatkan kesadaran masyarakat akan ancaman *phishing*.

3.2. Jenis Penelitian

Penelitian ini adalah studi deskriptif yang bertujuan untuk menggambarkan tingkat kesadaran masyarakat tentang ancaman *phishing* melalui aplikasi WhatsApp di RT. 001 Dusun Cikole, Desa Ranggon. Pendekatan deskriptif digunakan untuk memberikan gambaran yang komprehensif tentang fenomena yang diamati, yaitu tingkat kesadaran masyarakat terhadap *phishing* di *WhatsApp*. Dengan pendekatan ini, penelitian akan mengidentifikasi pengetahuan, sikap, dan perilaku masyarakat terkait ancaman *phishing* serta faktor-faktor yang

mempengaruhi kesadaran mereka. Penelitian ini menggunakan pendekatan kuantitatif untuk mengumpulkan dan menganalisis data. Metode kuantitatif dipilih karena memungkinkan pengukuran yang objektif dan statistik dari variabel yang diteliti. Dengan menggunakan instrumen survei, data yang diperoleh dapat dianalisis untuk mengidentifikasi pola dan hubungan yang relevan. Pendekatan kuantitatif sangat cocok untuk penelitian ini karena memerlukan pengukuran perubahan perilaku peserta sebelum dan sesudah edukasi.

3.3. Metode Analisis Data

Data yang dikumpulkan akan dianalisis secara deskriptif.

1. Analisis Deskriptif

Data survei akan dianalisis menggunakan metode statistik deskriptif. Ini akan mencakup perhitungan frekuensi, persentase, untuk variabel yang diukur dalam survei, seperti tingkat pengetahuan tentang *phishing*, sikap terhadap keamanan *cyber*, dan perilaku dalam menghadapi ancaman siber. Analisis ini akan memberikan gambaran yang jelas tentang distribusi dan karakteristik respons dari sampel penelitian.

a. Perhitungan Frekuensi: Menghitung seberapa sering setiap kategori atau nilai dari suatu variabel muncul dalam data survei. Ini akan membantu dalam memahami pola dasar dan tren umum di antara responden.

b. Persentase: Mengkonversi frekuensi menjadi persentase untuk memberikan gambaran yang lebih mudah dipahami tentang proporsi masing-masing kategori atau nilai. Misalnya, persentase responden yang mengetahui tentang *phishing* sebelum dan sesudah edukasi.

3.4. Metode Pengujian Data

Tabel 3. 1 Pertanyaan Survei

NO	PERTANYAAN
1.	Nama
2.	Usia

3.	Jenis Kelamin
4.	Pekerjaan
5.	Apakah Anda pernah mendengar istilah "*phishing*"?
6.	Seberapa baik Anda memahami apa itu *phishing*?
7.	Dari mana Anda pertama kali mendengar tentang *phishing*?
8.	Apakah Anda pernah menerima pesan mencurigakan di *WhatsApp* yang meminta informasi pribadi?
9.	Jika ya, bagaimana Anda merespons pesan tersebut?
10.	Seberapa sering Anda menerima pesan mencurigakan di *WhatsApp*?
11.	Seberapa besar kekhawatiran Anda tentang ancaman *phishing* di *WhatsApp*?
12.	Apakah Anda merasa cukup informasi tentang cara menghindari *phishing* di *WhatsApp*?
13.	Seberapa penting menurut Anda pendidikan tentang *phishing* untuk masyarakat?
14.	Apakah Anda pernah mengikuti program edukasi tentang keamanan siber atau *phishing*?
15.	Jika ya, seberapa efektif program tersebut dalam meningkatkan kesadaran Anda?
16.	Metode edukasi apa yang menurut Anda paling efektif untuk menyampaikan informasi tentang *phishing*?
17.	Apakah Anda lebih suka edukasi tentang phishing dilakukan secara *online* atau *offline*?
18.	Seberapa besar kemungkinan Anda akan mengikuti program edukasi tentang *phishing* jika diadakan di lingkungan Anda?
19.	Apakah Anda telah mengambil langkah-langkah untuk melindungi diri dari *phishing* di *WhatsApp*?
20.	Langkah apa yang telah Anda ambil untuk melindungi diri dari *phishing* di WhatsApp?

1. Pretest

Sebelum pelaksanaan program edukasi, dilakukan *pretest* untuk mengukur tingkat awal kesadaran masyarakat tentang *phishing*. *Pretest* ini mencakup serangkaian pertanyaan yang sama dengan *posttest*, sehingga memungkinkan perbandingan langsung sebelum dan sesudah intervensi edukasi.

2. Intervensi Edukasi

Program edukasi dilaksanakan selama satu minggu, meliputi penyuluhan langsung, penyebaran poster, penyebaran materi edukasi melalui *WhatsApp*, dan penggunaan media sosial untuk meningkatkan kesadaran tentang *phishing*. Materi edukasi disesuaikan dengan karakteristik dan kebutuhan masyarakat setempat, termasuk video pendek, dan panduan praktis.

3. Posttest

Setelah program edukasi selesai, dilakukan *posttest* untuk mengukur perubahan tingkat kesadaran masyarakat. Hasil *pretest* dan *posttest* dibandingkan menggunakan uji berpasangan (*paired t-test*) untuk menentukan apakah ada peningkatan signifikan dalam kesadaran masyarakat setelah mengikuti program edukasi. Analisis ini membantu menilai efektivitas keseluruhan dari program edukasi yang diterapkan.

3.5. Proses Edukasi

Proses edukasi dalam penelitian ini melibatkan beberapa tahapan yang dirancang untuk meningkatkan kesadaran masyarakat terhadap ancaman *phishing*. Proses ini dilakukan melalui platform *WhatsApp*, yang merupakan media komunikasi yang banyak digunakan oleh masyarakat di Dusun Cikole, RT 001, Desa Ranggon.

A. Persiapan Edukasi

1. Materi Edukasi

- Menyusun konten edukasi mengenai *phishing*, termasuk pengertian *phishing*, cara kerja *phishing*, contoh-contoh *phishing*, dan tips untuk menghindari phishing.

- Konten edukasi dibuat dalam bentuk gambar, dan video pendek untuk memudahkan pemahaman.

2. Perangkat Edukasi

- Menggunakan aplikasi *WhatsApp* sebagai *platform* utama untuk distribusi materi edukasi.

- Menyusun jadwal pengiriman materi edukasi selama satu minggu.

3. Kuesioner

- Menyusun kuesioner *pretest* dan *posttest* untuk mengukur tingkat pengetahuan dan kesadaran responden sebelum dan sesudah edukasi.

B. Pelaksanaan Edukasi

1. Pretest

Mengirimkan kuesioner *pretest* melalui *WhatsApp* kepada 50 *responden* untuk mengukur tingkat pengetahuan awal tentang *phishing*.

2. Penyampaian Materi Edukasi

a. Hari ke-1

Pengertian *phishing* dan pentingnya kesadaran terhadap ancaman *phishing*.

(Mengirimkan gambar yang menjelaskan apa itu *phishing* dan mengapa penting untuk menyadarinya).

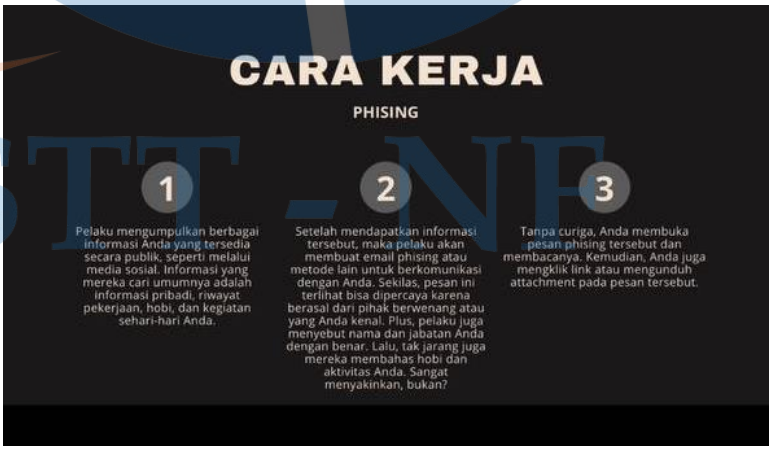
Gambar 3. 2 Materi edukasi hari ke-1

b. Hari ke-2

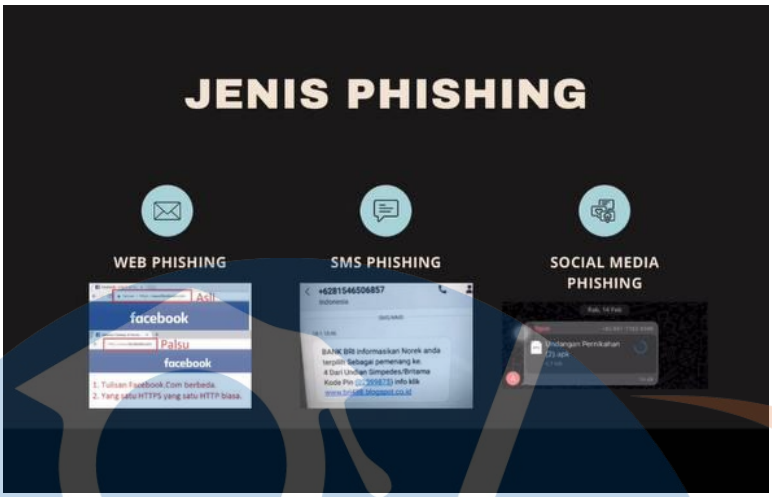
Cara kerja *phishing* dan berbagai jenis *phishing*. (Mengirimkan video pendek slide yang menjelaskan cara kerja *phising* jenis-jenis *phishing*, seperti *web phishing*, SMS *phishing*, dan *phishing* di media sosial).

Gambar 3. 3 Edukasi video pendek

Gambar 3. 4 Edukasi video pendek (1)

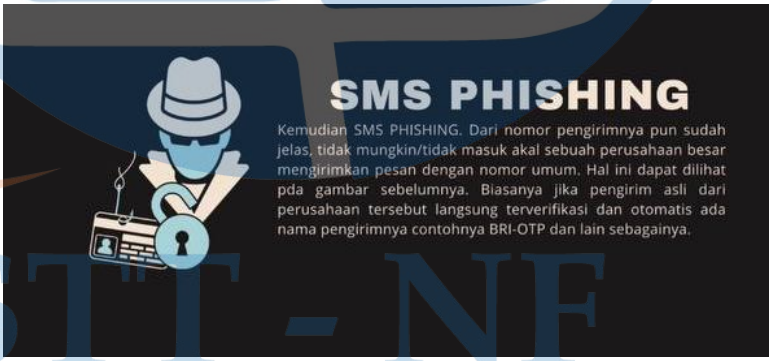


Gambar 3. 5 Edukasi video pendek (2)



Gambar 3. 6 Edukasi video pendek (3)

Gambar 3. 7 Edukasi video pendek (4)



Gambar 3. 8 Edukasi video pendek (5)

Gambar 3. 9 Edukasi video pendek (6)

c. Hari ke-3

Contoh kasus *phishing* yang sedang marak terjadi di Indonesia. (Mengirimkan video berita terkait kasus *phishing* di Indonesia).

Gambar 3. 10 Edukasi video berita kasus *phishing*

a. Hari ke-4

Tips dan langkah-langkah menghindari *phishing*. (Mengirimkan video yang berisi tips untuk mengidentifikasi *phishing* dan langkah-langkah untuk menghindarinya).

Gambar 3. 11 Edukasi video langkah langkah menghindari *phishing*

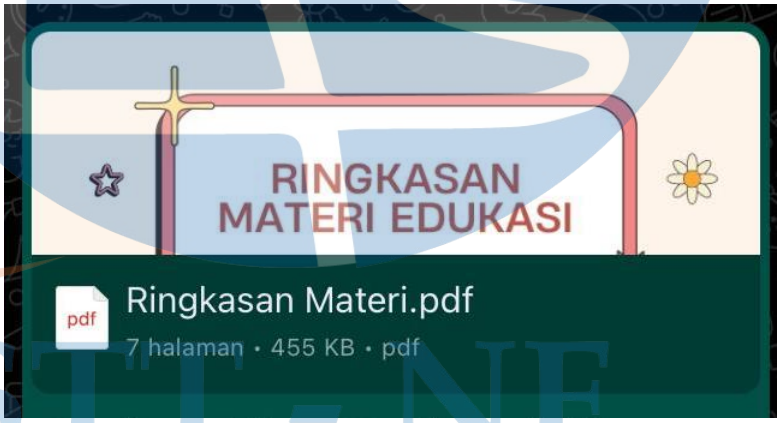
b. Hari ke-5

Dampak dan konsekuensi *phishing*. (Mengirimkan gambar tentang dampak *phishing* yang nyata).

Gambar 3. 12 Dampak *phishing*

c. Hari ke-6

Ringkasan dan penutupan. (Mengirimkan ringkasan materi edukasi selama satu minggu).



Gambar 3. 13 Ringkasan materi edukasi

d. Hari ke-7

Melakukan pengujian. (Mengingatkan responden untuk mengisi kuesioner *posttest*, dan memberikan pengujian tautan *phising).*

Gambar 3. 14 Halaman utama *web*

Gambar 3. 15 Halaman data berhasil disimpan

Hasil Akhir Edukasi:

- Peningkatan pemahaman tentang phishing dan ancamannya pada masyarakat.
- Masyarakat lebih waspada terhadap pesan mencurigakan dan lebih aktif dalam melaporkan insiden *phishing*.
- Peningkatan penggunaan langkah-langkah keamanan digital seperti autentikasi dua faktor dan memperbarui aplikasi secara teratur.

3. Posttest

Mengirimkan kuesioner *posttest* melalui *Google Form* kepada 50 responden untuk mengukur perubahan tingkat kesadaran dan pengetahuan setelah menerima edukasi.

C. Analisis Hasil Edukasi

1. Pengumpulan Data

- Mengumpulkan data dari kuesioner *pretest* dan *posttest*.

- Mencatat tanggapan dan partisipasi responden selama sesi edukasi.

2. Analisis Data

- Menganalisis data *pretest* dan *posttest* untuk mengukur perubahan tingkat pengetahuan dan kesadaran tentang *phishing*.

- Menggunakan metode statistik deskriptif untuk menghitung frekuensi, persentase, dan ukuran pemusatan data.

3. Evaluasi Efektivitas Edukasi

- Mengevaluasi efektivitas edukasi dengan membandingkan hasil *pretest* dan *posttest*. - Membuat laporan hasil analisis dan memberikan rekomendasi untuk peningkatan kesadaran masyarakat terhadap ancaman *phishing* di masa depan.

BAB IV
IMPLEMENTASI DAN EVALUASI

4.1.Rancangan Penelitian

Rancangan penelitian ini dirancang untuk mengukur efektivitas program edukasi *phishing* yang dilaksanakan melalui platform *WhatsApp*. Penelitian ini dibagi menjadi beberapa tahap, yaitu *pretest*, edukasi, dan *posttest*, dengan penjelasan detail sebagai berikut.

4.1.1. Cara Kerja

a. *Pretest*

Tahap ini bertujuan untuk mendapatkan data awal tentang tingkat kesadaran peserta mengenai *phishing*. Kuesioner *pretest* yang dirancang khusus untuk mengukur pengetahuan tentang *phishing* akan dikirimkan melalui *WhatsApp*. Kuesioner ini berisi pertanyaan tentang pengenalan *phishing* dan tanda-tanda *phishing*.

b. Edukasi

Setelah tahap *pretest*, peserta akan menerima materi edukasi mengenai *phishing* selama satu minggu. Materi ini akan disampaikan melalui pesan teks dan gambar yang dikirimkan setiap hari melalui *WhatsApp*. Materi edukasi meliputi definisi *phishing*, berbagai jenis *phishing*, cara mengidentifikasi *phishing*, dan langkah-langkah untuk menghindarinya. Setiap bagian dari materi dirancang untuk mudah dipahami dan menarik bagi peserta.

c. *Posttest*

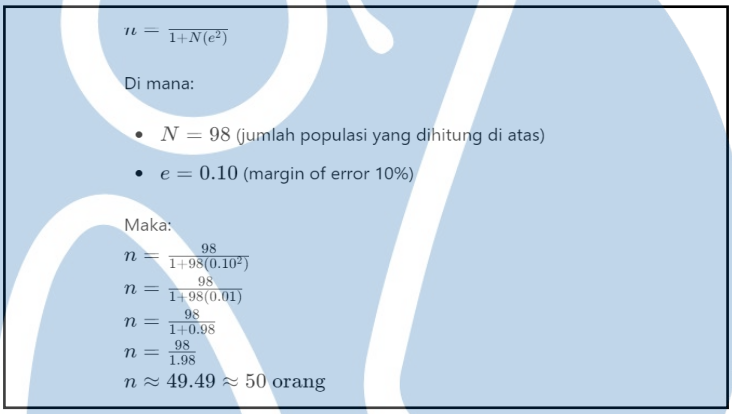
Setelah periode edukasi selesai, peserta akan diminta untuk mengisi kuesioner *posttest* yang sama dengan *pretest*. Ini dilakukan untuk mengevaluasi perubahan tingkat kesadaran peserta tentang *phishing* setelah mereka menerima edukasi.

d. Analisis Data

Data dari *pretest* dan *posttest* akan dianalisis untuk menilai efektivitas program edukasi. Perbandingan hasil *pretest* dan *posttest* akan menunjukkan sejauh mana pengetahuan peserta tentang *phishing* meningkat.

4.1.2. Arsitektur Sistem

Penelitian ini dirancang untuk mengukur efektivitas edukasi tentang ancaman *phishing* melalui platform *WhatsApp*. Lokasi penelitian adalah Dusun Cikole, RT 001, Desa Ranggon, dengan jumlah penduduk sebanyak 227 orang. Penduduk yang menjadi fokus penelitian adalah mereka yang berusia 19-50 tahun, berjumlah 98 orang. Berdasarkan perhitungan menggunakan rumus Slovin dengan tingkat kepercayaan 95% dan margin of error 10%, sampel yang diperlukan adalah 50 responden.



Gambar 4. 1 Rumus Slovin

Berikut adalah arsitektur sistem yang diterapkan dalam penelitian ini.

A. Langkah-Langkah Penelitian

1. Tahap Persiapan

- Menyusun kuesioner *pretest* dan *posttest* untuk mengukur tingkat kesadaran akan ancaman *phishing*.

- Menyusun materi edukasi mengenai *phishing* yang akan dikirimkan melalui *WhatsApp*.

- Menentukan dan merekrut responden dari Dusun Cikole, RT 001, Desa Ranggon yang berusia 19-50 tahun.

2. Tahap Pelaksanaan

- *Pretest*: Mengirimkan kuesioner *pretest* kepada 50 responden melalui *WhatsApp* untuk mengukur pengetahuan awal tentang *phishing*.

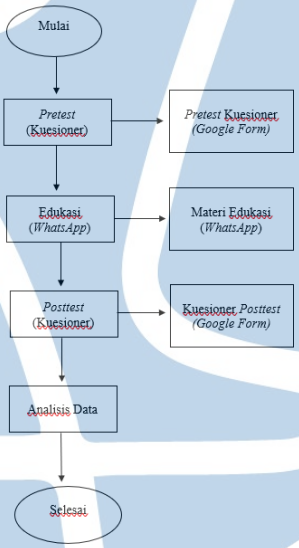
- Edukasi: Mengirimkan materi edukasi tentang *phishing* setiap hari selama satu minggu melalui *WhatsApp* kepada responden.
- *Posttest*: Mengirimkan kuesioner *posttest* kepada responden untuk mengukur perubahan tingkat kesadaran setelah menerima edukasi.

3. Tahap Analisis Data

- Mengumpulkan data hasil *pretest* dan *posttest*.
- Menganalisis data untuk mengukur perubahan tingkat kesadaran peserta mengenai *phishing* setelah menerima edukasi.

B. Diagram Alir Proses Penelitian

Berikut adalah *flowchart* atau diagram alir dari proses penelitian:



Gambar 4. 2 Diagram alir penelitian

C. Komponen Sistem

Platform Komunikasi: *WhatsApp* digunakan sebagai media untuk mengirimkan kuesioner dan materi edukasi.

Instrumen Pengukuran: Kuesioner *pretest* dan *posttest* digunakan untuk mengukur tingkat kesadaran dan pengetahuan responden mengenai *phishing*.

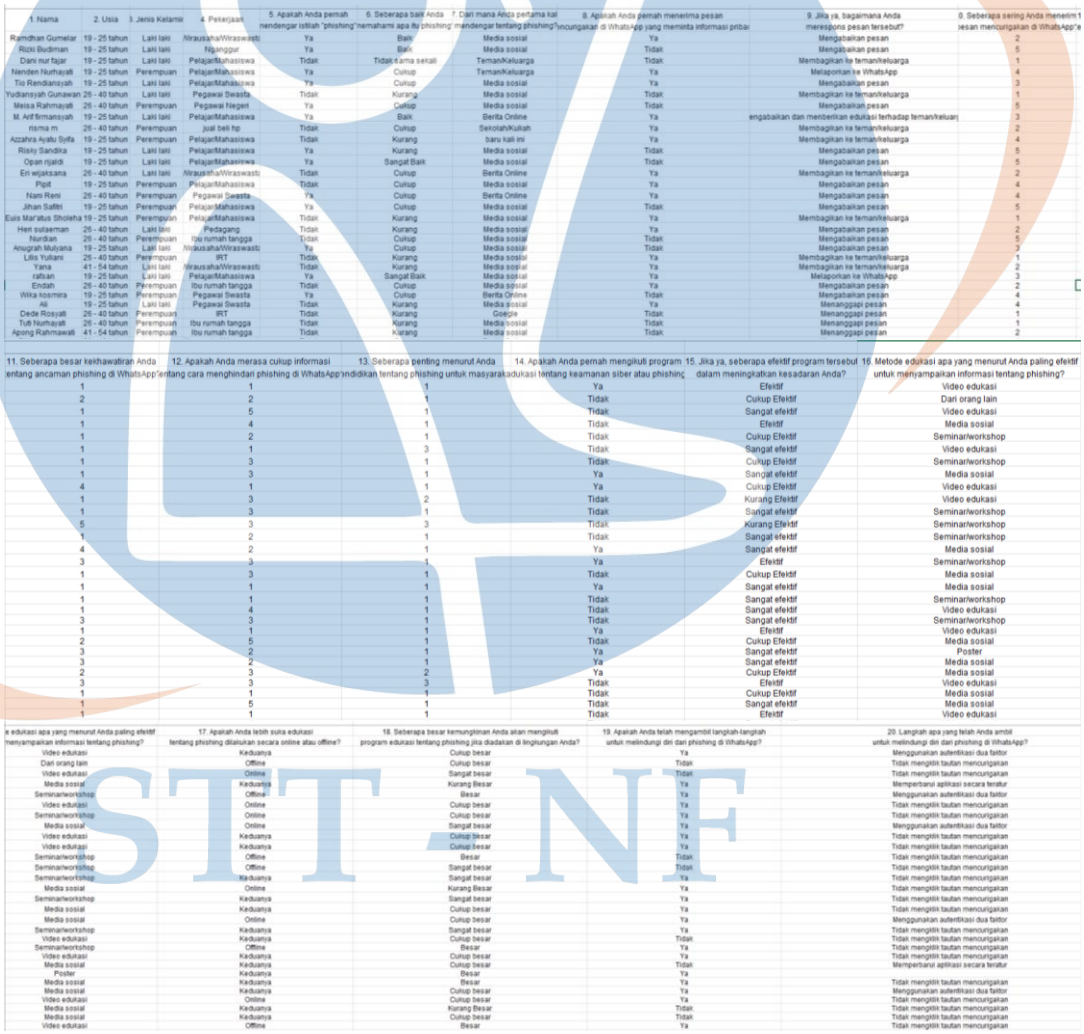
Materi Edukasi: Konten edukasi tentang *phishing* yang dirancang untuk meningkatkan pengetahuan dan kesadaran masyarakat mengenai ancaman *phishing*.

Sistem Pengumpulan Data: Data dari kuesioner *pretest* dan *posttest* dikumpulkan dan dianalisis untuk menentukan perubahan dalam tingkat kesadaran masyarakat setelah menerima edukasi.

4.2. Hasil Implementasi

Berikut ini adalah hasil yang diperoleh dari implementasi program edukasi, dimana didalamnya mencakup 20 pertanyaan.

4.2.1. Hasil *Pretest*

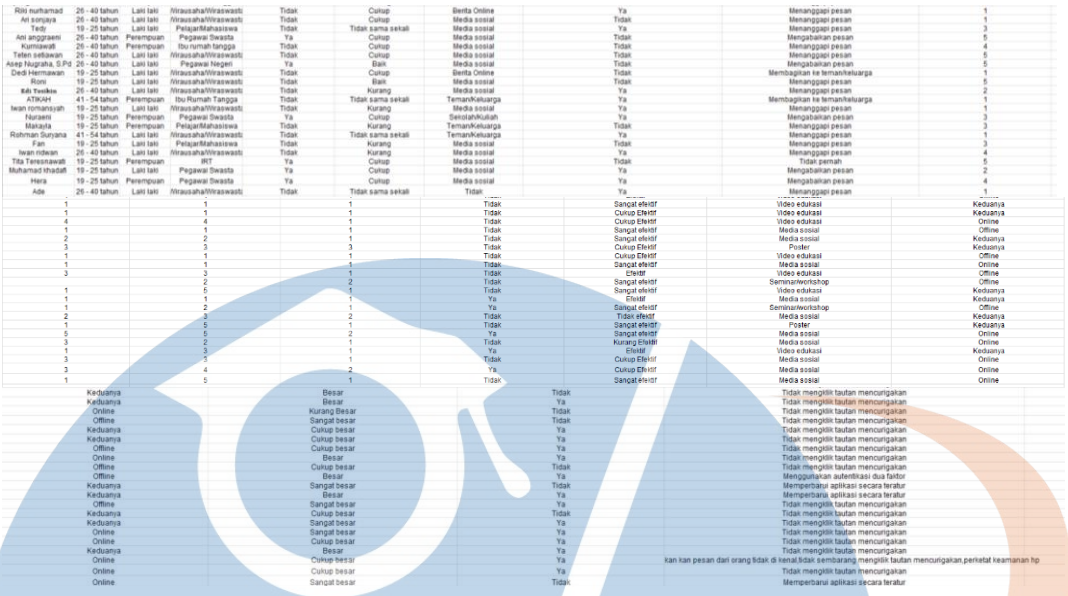


1. Nama	2. Usia	3. Jenis Kelamin	4. Pekerjaan	5. Apakah Anda pernah mendengar istilah "phishing"	6. Seberapa baik Anda memahami apa itu phishing	7. Dari mana Anda pertama kali mendengar tentang phishing?	8. Apakah Anda pernah menerima pesan mencurigakan di WhatsApp yang meminta informasi pribadi	9. Jika ya, bagaimana Anda merespons pesan tersebut?	10. Seberapa sering Anda menerima pesan mencurigakan di WhatsApp?
Ramdhan Gumelar	19 - 25 tahun	Laki laki	Wirausaha/Wiraswasta	Ya	Baik	Media sosial	Ya	Mengabaikan pesan	2
Rizki Budiman	19 - 25 tahun	Laki laki	Nganggur	Ya	Baik	Media sosial	Tidak	Mengabaikan pesan	5
Dani nur fajar	19 - 25 tahun	Laki laki	Pelajar/Mahasiswa	Tidak	Tidak tahu sekali	Teman/Keluarga	Tidak	Membagikan ke teman/keluarga	1
Nenden Nurhayati	19 - 25 tahun	Perempuan	Pelajar/Mahasiswa	Ya	Cukup	Teman/Keluarga	Ya	Melaporkan ke WhatsApp	4
Tio Rendiansyah	19 - 25 tahun	Laki laki	Pelajar/Mahasiswa	Ya	Cukup	Media sosial	Ya	Mengabaikan pesan	3
Yudiansyah Gunawan	26 - 40 tahun	Laki laki	Pegawai Swasta	Tidak	Kurang	Media sosial	Tidak	Membagikan ke teman/keluarga	1
Meisa Rahmayati	26 - 40 tahun	Perempuan	Pegawai Negeri	Ya	Cukup	Media sosial	Tidak	Mengabaikan pesan	5
M. Arif firmansyah	19 - 25 tahun	Laki laki	Pelajar/Mahasiswa	Ya	Baik	Berita Online	Ya	engabaikan dan memberikan edukasi terhadap teman/keluar	3
risma m	26 - 40 tahun	Perempuan	jual beli hp	Tidak	Cukup	Sekolah/Kuliah	Ya	Membagikan ke teman/keluarga	2
Azzahra Ayatu Syifa	19 - 25 tahun	Perempuan	Pelajar/Mahasiswa	Tidak	Kurang	baru kali ini	Ya	Membagikan ke teman/keluarga	4
Risky Sandika	19 - 25 tahun	Laki laki	Pelajar/Mahasiswa	Ya	Kurang	Media sosial	Tidak	Mengabaikan pesan	5
Opan rijaldi	19 - 25 tahun	Laki laki	Pelajar/Mahasiswa	Ya	Sangat Baik	Media sosial	Tidak	Mengabaikan pesan	5
Eri wijaksana	26 - 40 tahun	Laki laki	Wirausaha/Wiraswasta	Tidak	Cukup	Berita Online	Ya	Membagikan ke teman/keluarga	2
Pipit	19 - 25 tahun	Perempuan	Pelajar/Mahasiswa	Tidak	Cukup	Media sosial	Ya	Mengabaikan pesan	4
Nani Reni	26 - 40 tahun	Perempuan	Pegawai Swasta	Ya	Cukup	Berita Online	Ya	Mengabaikan pesan	4
Jihan Safiti	19 - 25 tahun	Perempuan	Pelajar/Mahasiswa	Ya	Cukup	Media sosial	Tidak	Mengabaikan pesan	5
Euis Ma'atus Sholeha	19 - 25 tahun	Perempuan	Pelajar/Mahasiswa	Tidak	Kurang	Media sosial	Ya	Membagikan ke teman/keluarga	1
Heri sulaeman	26 - 40 tahun	Laki laki	Pedagang	Tidak	Kurang	Media sosial	Ya	Mengabaikan pesan	2
Nurdian	26 - 40 tahun	Perempuan	Ibu rumah tangga	Tidak	Cukup	Media sosial	Tidak	Mengabaikan pesan	5
Anugrah Mulyana	19 - 25 tahun	Laki laki	Wirausaha/Wiraswasta	Ya	Cukup	Media sosial	Tidak	Mengabaikan pesan	3
Lilis Yuliani	26 - 40 tahun	Perempuan	IRT	Tidak	Kurang	Media sosial	Ya	Membagikan ke teman/keluarga	1
Yana	41 - 54 tahun	Laki laki	Wirausaha/Wiraswasta	Tidak	Kurang	Media sosial	Ya	Membagikan ke teman/keluarga	2
rafsan	19 - 25 tahun	Laki laki	Pelajar/Mahasiswa	Ya	Sangat Baik	Media sosial	Ya	Melaporkan ke WhatsApp	3
Endah	26 - 40 tahun	Perempuan	Ibu rumah tangga	Tidak	Cukup	Media sosial	Ya	Mengabaikan pesan	2
Wika kosmira	19 - 25 tahun	Perempuan	Pegawai Swasta	Ya	Cukup	Berita Online	Tidak	Mengabaikan pesan	4
Ali	19 - 25 tahun	Laki laki	Pegawai Swasta	Tidak	Kurang	Media sosial	Ya	Menanggapi pesan	4
Dede Rosyati	26 - 40 tahun	Perempuan	IRT	Tidak	Kurang	Goegle	Tidak	Menanggapi pesan	1
Tuti Nurhayati	26 - 40 tahun	Perempuan	Ibu rumah tangga	Tidak	Kurang	Media sosial	Tidak	Menanggapi pesan	1
Apong Rahmawati	41 - 54 tahun	Perempuan	Ibu rumah tangga	Tidak	Kurang	Media sosial	Tidak	Menanggapi pesan	2

11. Seberapa besar kekhawatiran Anda tentang ancaman phishing di WhatsApp?	12. Apakah Anda merasa cukup informasi tentang cara menghindari phishing di WhatsApp?	13. Seberapa penting menurut Anda pendidikan tentang phishing untuk masyarakat?	14. Apakah Anda pernah mengikuti program edukasi tentang keamanan siber atau phishing?	15. Jika ya, seberapa efektif program tersebut dalam meningkatkan kesadaran Anda?	16. Metode edukasi apa yang menurut Anda paling efektif untuk menyampaikan informasi tentang phishing?
1	1	1	Ya	Efektif	Video edukasi
2	2	1	Tidak	Cukup Efektif	Dari orang lain
1	5	1	Tidak	Sangat efektif	Video edukasi
1	4	1	Tidak	Efektif	Media sosial
1	2	1	Tidak	Cukup Efektif	Seminar/workshop
1	1	3	Tidak	Sangat efektif	Video edukasi
1	3	1	Tidak	Cukup Efektif	Seminar/workshop
1	3	1	Ya	Sangat efektif	Media sosial
4	1	1	Ya	Cukup Efektif	Video edukasi
1	3	2	Tidak	Kurang Efektif	Video edukasi
1	3	1	Tidak	Sangat efektif	Seminar/workshop
5	3	3	Tidak	Kurang Efektif	Seminar/workshop
1	2	1	Tidak	Sangat efektif	Seminar/workshop
4	2	1	Ya	Sangat efektif	Media sosial
3	3	1	Ya	Efektif	Seminar/workshop
1	3	1	Tidak	Cukup Efektif	Media sosial
1	1	1	Ya	Sangat efektif	Media sosial
1	1	1	Tidak	Sangat efektif	Seminar/workshop
1	4	1	Tidak	Sangat efektif	Video edukasi
3	3	1	Tidak	Sangat efektif	Seminar/workshop
1	1	1	Ya	Efektif	Video edukasi
2	5	1	Tidak	Cukup Efektif	Media sosial
3	2	1	Ya	Sangat efektif	Poster
3	2	1	Ya	Sangat efektif	Media sosial
2	3	2	Ya	Cukup Efektif	Media sosial
3	3	3	Tidak	Efektif	Video edukasi
1	1	1	Tidak	Cukup Efektif	Media sosial
1	5	1	Tidak	Sangat efektif	Media sosial
1	1	1	Tidak	Efektif	Video edukasi

e edukasi apa yang menurut Anda paling efektif menyampaikan informasi tentang phishing?	17. Apakah Anda lebih suka edukasi tentang phishing dilakukan secara online atau offline?	18. Seberapa besar kemungkinan Anda akan mengikuti program edukasi tentang phishing jika diadakan di lingkungan Anda?	19. Apakah Anda telah mengambil langkah-langkah untuk melindungi diri dari phishing di WhatsApp?	20. Langkah apa yang telah Anda ambil untuk melindungi diri dari phishing di WhatsApp?
Video edukasi	Keduanya	Cukup besar	Ya	Menggunakan autentikasi dua faktor
Dari orang lain	Offline	Cukup besar	Tidak	Tidak mengklik tautan mencurigakan
Video edukasi	Online	Sangat besar	Tidak	Tidak mengklik tautan mencurigakan
Media sosial	Keduanya	Kurang Besar	Ya	Memperbarui aplikasi secara teratur
Seminar/workshop	Offline	Besar	Ya	Menggunakan autentikasi dua faktor
Video edukasi	Online	Cukup besar	Ya	Tidak mengklik tautan mencurigakan
Seminar/workshop	Online	Cukup besar	Ya	Tidak mengklik tautan mencurigakan
Media sosial	Online	Sangat besar	Ya	Menggunakan autentikasi dua faktor
Video edukasi	Keduanya	Cukup besar	Ya	Tidak mengklik tautan mencurigakan
Video edukasi	Keduanya	Cukup besar	Ya	Tidak mengklik tautan mencurigakan
Seminar/workshop	Offline	Besar	Tidak	Tidak mengklik tautan mencurigakan
Seminar/workshop	Offline	Sangat besar	Tidak	Tidak mengklik tautan mencurigakan
Seminar/workshop	Keduanya	Sangat besar	Ya	Tidak mengklik tautan mencurigakan
Media sosial	Online	Kurang Besar	Ya	Tidak mengklik tautan mencurigakan
Seminar/workshop	Keduanya	Sangat besar	Ya	Tidak mengklik tautan mencurigakan
Media sosial	Keduanya	Cukup besar	Ya	Tidak mengklik tautan mencurigakan
Media sosial	Online	Cukup besar	Ya	Menggunakan autentikasi dua faktor
Seminar/workshop	Keduanya	Sangat besar	Ya	Tidak mengklik tautan mencurigakan
Video edukasi	Keduanya	Cukup besar	Tidak	Tidak mengklik tautan mencurigakan
Seminar/workshop	Offline	Besar	Ya	Tidak mengklik tautan mencurigakan
Video edukasi	Keduanya	Cukup besar	Ya	Tidak mengklik tautan mencurigakan
Media sosial	Keduanya	Cukup besar	Tidak	Tidak mengklik tautan mencurigakan
Poster	Keduanya	Besar	Ya	Memperbarui aplikasi secara teratur
Media sosial	Keduanya	Besar	Ya	Tidak mengklik tautan mencurigakan
Media sosial	Keduanya	Cukup besar	Ya	Menggunakan autentikasi dua faktor
Video edukasi	Online	Cukup besar	Ya	Tidak mengklik tautan mencurigakan
Media sosial	Keduanya	Kurang Besar	Tidak	Tidak mengklik tautan mencurigakan
Media sosial	Keduanya	Cukup besar	Tidak	Tidak mengklik tautan mencurigakan
Video edukasi	Offline	Besar	Ya	Tidak mengklik tautan mencurigakan

Gambar 4. 3 Data kuisioner *pretest* responden 1-29



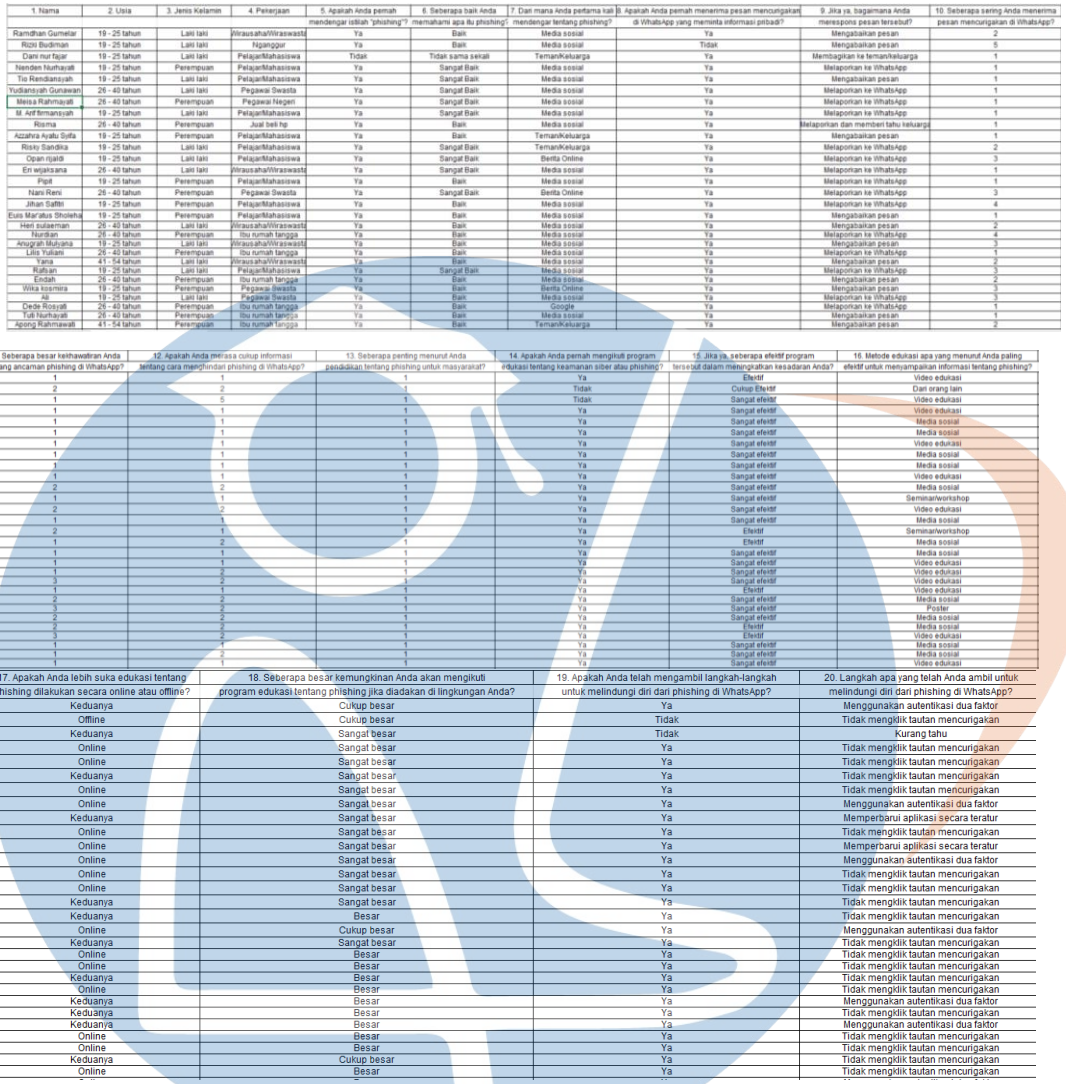
Gambar 4. 4 Data *kuisioner* pretest responden 30-50

$$\text{Persentase} = \left(\frac{\text{Jumlah Responden dengan Kriteria Tertentu}}{\text{Total Jumlah Responden}} \right) \times 100\%$$

Gambar 4. 5 Rumus dasar menghitung persentasi

Dari hasil *pre-test* terhadap 50 responden di Dusun Cikole, Desa Ranggon, ditemukan bahwa 56% responden telah mendengar istilah "*phishing*," sementara 44% belum pernah mendengarnya, menunjukkan sebagian besar memiliki kesadaran awal tentang ancaman ini. Tingkat pengetahuan spesifik tentang *phishing* bervariasi, dengan 12% memiliki pengetahuan dasar, 24% cukup, 14% baik, dan 6% sangat baik. Media sosial menjadi sumber informasi utama (52%), diikuti oleh teman/keluarga (10%), berita online (8%), sekolah/kuliah (4%), dan poster (2%). Sebanyak 48% responden pernah menerima pesan mencurigakan di *WhatsApp* yang meminta informasi pribadi, dan sebagian besar mengabaikan pesan tersebut (66.7%), sementara lainnya membagikannya ke teman/keluarga atau melaporkannya ke *WhatsApp*. Hal ini menunjukkan bahwa hampir setengah dari responden sudah terpapar *phishing* dan mayoritas cukup waspada untuk tidak menanggapi pesan mencurigakan.

4.3.3 Hasil Post-Test

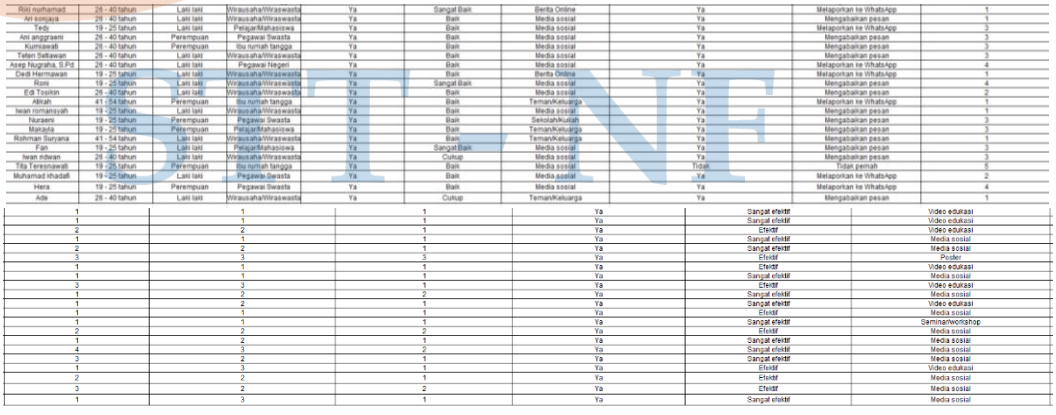


1. Nama	2. Usia	3. Jenis Kelamin	4. Pekerjaan	5. Apakah Anda pernah mendengar istilah "phishing"?	6. Seberapa baik Anda memahami apa itu phishing?	7. Dari mana Anda pertama kali mendengar tentang phishing?	8. Apakah Anda pernah menerima pesan mencurigakan di WhatsApp yang meminta informasi pribadi?	9. Jika ya, bagaimana Anda merespons pesan tersebut?	10. Seberapa sering Anda menerima pesan mencurigakan di WhatsApp?
Ramdhan Gumelar	19 - 25 tahun	Laki laki	Wirausaha/Wiraswasta	Ya	Baik	Media sosial	Ya	Mengabaikan pesan	2
Rizki Budiman	19 - 25 tahun	Laki laki	Nganggur	Ya	Baik	Media sosial	Tidak	Mengabaikan pesan	5
Dani nur fajar	19 - 25 tahun	Laki laki	Pelajar/Mahasiswa	Tidak	Tidak sama sekali	Teman/Keluarga	Ya	Membagikan ke teman/keluarga	1
Nenden Nurhayati	19 - 25 tahun	Perempuan	Pelajar/Mahasiswa	Ya	Sangat Baik	Media sosial	Ya	Melaporkan ke WhatsApp	1
Tio Rendiansyah	19 - 25 tahun	Laki laki	Pelajar/Mahasiswa	Ya	Sangat Baik	Media sosial	Ya	Mengabaikan pesan	1
Yudiansyah Gunawan	26 - 40 tahun	Laki laki	Pegawai Swasta	Ya	Sangat Baik	Media sosial	Ya	Melaporkan ke WhatsApp	1
Meisa Rahmayati	26 - 40 tahun	Perempuan	Pegawai Negeri	Ya	Sangat Baik	Media sosial	Ya	Melaporkan ke WhatsApp	1
M. Arif firmansyah	19 - 25 tahun	Laki laki	Pelajar/Mahasiswa	Ya	Sangat Baik	Media sosial	Ya	Melaporkan ke WhatsApp	1
Rosma	26 - 40 tahun	Perempuan	Jual beli hp	Ya	Baik	Media sosial	Ya	Melaporkan dan memberi tahu keluarga	1
Azzahra Ayalu Syifa	19 - 25 tahun	Perempuan	Pelajar/Mahasiswa	Ya	Baik	Teman/Keluarga	Ya	Mengabaikan pesan	1
Risky Sandika	19 - 25 tahun	Laki laki	Pelajar/Mahasiswa	Ya	Sangat Baik	Teman/Keluarga	Ya	Melaporkan ke WhatsApp	2
Opan rijaldi	19 - 25 tahun	Laki laki	Pelajar/Mahasiswa	Ya	Sangat Baik	Berita Online	Ya	Melaporkan ke WhatsApp	3
Eri wijaksana	26 - 40 tahun	Laki laki	Wirausaha/Wiraswasta	Ya	Sangat Baik	Media sosial	Ya	Melaporkan ke WhatsApp	1
Pipit	19 - 25 tahun	Perempuan	Pelajar/Mahasiswa	Ya	Baik	Media sosial	Ya	Melaporkan ke WhatsApp	1
Nani Reni	26 - 40 tahun	Perempuan	Pegawai Swasta	Ya	Sangat Baik	Berita Online	Ya	Melaporkan ke WhatsApp	3
Jihan Safitri	19 - 25 tahun	Perempuan	Pelajar/Mahasiswa	Ya	Baik	Media sosial	Ya	Melaporkan ke WhatsApp	4
Euis Maratus Sholeha	19 - 25 tahun	Perempuan	Pelajar/Mahasiswa	Ya	Baik	Media sosial	Ya	Mengabaikan pesan	1
Heri sulaeman	26 - 40 tahun	Laki laki	Wirausaha/Wiraswasta	Ya	Baik	Media sosial	Ya	Mengabaikan pesan	2
Nurdian	26 - 40 tahun	Perempuan	Ibu rumah tangga	Ya	Baik	Media sosial	Ya	Melaporkan ke WhatsApp	4
Anugrah Mulyana	19 - 25 tahun	Laki laki	Wirausaha/Wiraswasta	Ya	Baik	Media sosial	Ya	Mengabaikan pesan	3
Lilis Yuliani	26 - 40 tahun	Perempuan	Ibu rumah tangga	Ya	Baik	Media sosial	Ya	Melaporkan ke WhatsApp	1
Yana	41 - 54 tahun	Laki laki	Wirausaha/Wiraswasta	Ya	Baik	Media sosial	Ya	Mengabaikan pesan	2
Rafsan	19 - 25 tahun	Laki laki	Pelajar/Mahasiswa	Ya	Sangat Baik	Media sosial	Ya	Melaporkan ke WhatsApp	3
Endah	26 - 40 tahun	Perempuan	Ibu rumah tangga	Ya	Baik	Media sosial	Ya	Mengabaikan pesan	2
Wika kosmira	19 - 25 tahun	Perempuan	Pegawai Swasta	Ya	Baik	Berita Online	Ya	Mengabaikan pesan	3
Ali	19 - 25 tahun	Laki laki	Pegawai Swasta	Ya	Baik	Media sosial	Ya	Melaporkan ke WhatsApp	3
Dede Rosyati	26 - 40 tahun	Perempuan	Ibu rumah tangga	Ya	Baik	Google	Ya	Melaporkan ke WhatsApp	1
Tuti Nurhayati	26 - 40 tahun	Perempuan	Ibu rumah tangga	Ya	Baik	Media sosial	Ya	Mengabaikan pesan	1
Apong Rahmawati	41 - 54 tahun	Perempuan	Ibu rumah tangga	Ya	Baik	Teman/Keluarga	Ya	Mengabaikan pesan	2

11. Seberapa besar kekhawatiran Anda tentang ancaman phishing di WhatsApp?	12. Apakah Anda merasa cukup informasi tentang cara menghindari phishing di WhatsApp?	13. Seberapa penting menurut Anda pendidikan tentang phishing untuk masyarakat?	14. Apakah Anda pernah mengikuti program edukasi tentang keamanan siber atau phishing?	15. Jika ya, seberapa efektif program tersebut dalam meningkatkan kesadaran Anda?	16. Metode edukasi apa yang menurut Anda paling efektif untuk menyampaikan informasi tentang phishing?
1	1	1	Ya	Efektif	Video edukasi
2	2	1	Tidak	Cukup Efektif	Dari orang lain
1	5	1	Tidak	Sangat efektif	Video edukasi
1	1	1	Ya	Sangat efektif	Video edukasi
1	1	1	Ya	Sangat efektif	Media sosial
1	1	1	Ya	Sangat efektif	Media sosial
1	1	1	Ya	Sangat efektif	Video edukasi
1	1	1	Ya	Sangat efektif	Media sosial
1	1	1	Ya	Sangat efektif	Media sosial
1	1	1	Ya	Sangat efektif	Video edukasi
2	2	1	Ya	Sangat efektif	Media sosial
1	1	1	Ya	Sangat efektif	Seminar/workshop
2	2	1	Ya	Sangat efektif	Video edukasi
1	1	1	Ya	Sangat efektif	Media sosial
2	1	1	Ya	Efektif	Seminar/workshop
1	2	1	Ya	Efektif	Media sosial
1	1	1	Ya	Sangat efektif	Media sosial
1	1	1	Ya	Sangat efektif	Video edukasi
1	2	1	Ya	Sangat efektif	Video edukasi
3	2	1	Ya	Sangat efektif	Video edukasi
1	1	1	Ya	Efektif	Video edukasi
2	2	1	Ya	Sangat efektif	Media sosial
3	2	1	Ya	Sangat efektif	Poster
2	2	1	Ya	Sangat efektif	Media sosial
2	2	1	Ya	Efektif	Media sosial
3	2	1	Ya	Efektif	Video edukasi
1	1	1	Ya	Sangat efektif	Media sosial
1	2	1	Ya	Sangat efektif	Media sosial
1	1	1	Ya	Sangat efektif	Video edukasi

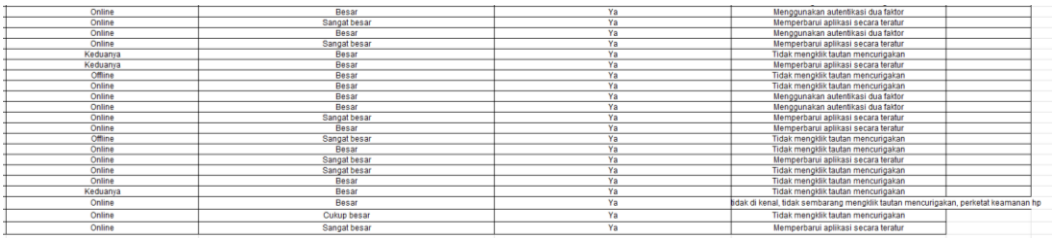
17. Apakah Anda lebih suka edukasi tentang phishing dilakukan secara online atau offline?	18. Seberapa besar kemungkinan Anda akan mengikuti program edukasi tentang phishing jika diadakan di lingkungan Anda?	19. Apakah Anda telah mengambil langkah-langkah untuk melindungi diri dari phishing di WhatsApp?	20. Langkah apa yang telah Anda ambil untuk melindungi diri dari phishing di WhatsApp?
Keduanya	Cukup besar	Ya	Menggunakan autentikasi dua faktor
Offline	Cukup besar	Tidak	Tidak mengklik tautan mencurigakan
Keduanya	Sangat besar	Tidak	Kurang tahu
Online	Sangat besar	Ya	Tidak mengklik tautan mencurigakan
Online	Sangat besar	Ya	Tidak mengklik tautan mencurigakan
Keduanya	Sangat besar	Ya	Tidak mengklik tautan mencurigakan
Online	Sangat besar	Ya	Tidak mengklik tautan mencurigakan
Online	Sangat besar	Ya	Menggunakan autentikasi dua faktor
Keduanya	Sangat besar	Ya	Memperbarui aplikasi secara teratur
Online	Sangat besar	Ya	Tidak mengklik tautan mencurigakan
Online	Sangat besar	Ya	Memperbarui aplikasi secara teratur
Online	Sangat besar	Ya	Menggunakan autentikasi dua faktor
Online	Sangat besar	Ya	Tidak mengklik tautan mencurigakan
Online	Sangat besar	Ya	Tidak mengklik tautan mencurigakan
Keduanya	Sangat besar	Ya	Tidak mengklik tautan mencurigakan
Keduanya	Besar	Ya	Tidak mengklik tautan mencurigakan
Online	Cukup besar	Ya	Menggunakan autentikasi dua faktor
Keduanya	Sangat besar	Ya	Tidak mengklik tautan mencurigakan
Online	Besar	Ya	Tidak mengklik tautan mencurigakan
Online	Besar	Ya	Tidak mengklik tautan mencurigakan
Keduanya	Besar	Ya	Tidak mengklik tautan mencurigakan
Online	Besar	Ya	Tidak mengklik tautan mencurigakan
Keduanya	Besar	Ya	Menggunakan autentikasi dua faktor
Keduanya	Besar	Ya	Tidak mengklik tautan mencurigakan
Keduanya	Besar	Ya	Menggunakan autentikasi dua faktor
Online	Besar	Ya	Tidak mengklik tautan mencurigakan
Online	Besar	Ya	Tidak mengklik tautan mencurigakan
Keduanya	Cukup besar	Ya	Tidak mengklik tautan mencurigakan
Online	Besar	Ya	Tidak mengklik tautan mencurigakan

Gambar 4. 6 Data kuisioner *posttest* responden 1 – 29



Rini nurhamad	26 - 40 tahun	Laki laki	Wirausaha/Wiraswasta	Ya	Sangat Baik	Berita Online	Ya	Melaporkan ke WhatsApp	1
Ari soniaya	26 - 40 tahun	Laki laki	Wirausaha/Wiraswasta	Ya	Baik	Media sosial	Ya	Mengabaikan pesan	1
Tedi	19 - 25 tahun	Laki laki	Pelajar/Mahasiswa	Ya	Baik	Media sosial	Ya	Melaporkan ke WhatsApp	3
Ani anggraeni	26 - 40 tahun	Perempuan	Pegawai Swasta	Ya	Baik	Media sosial	Ya	Mengabaikan pesan	3
Kurniawati	26 - 40 tahun	Perempuan	Ibu rumah tangga	Ya	Baik	Media sosial	Ya	Mengabaikan pesan	3
Teten Setiawan	26 - 40 tahun	Laki laki	Wirausaha/Wiraswasta	Ya	Baik	Media sosial	Ya	Mengabaikan pesan	3
Aseg Nugraha, S.Pd	26 - 40 tahun	Laki laki	Pegawai Negeri	Ya	Baik	Media sosial	Ya	Melaporkan ke WhatsApp	4
Dedi Harmawan	19 - 25 tahun	Laki laki	Wirausaha/Wiraswasta	Ya	Baik	Berita Online	Ya	Melaporkan ke WhatsApp	1
Roni	19 - 25 tahun	Laki laki	Wirausaha/Wiraswasta	Ya	Sangat Baik	Media sosial	Ya	Mengabaikan pesan	4
Edi Toskin	26 - 40 tahun	Laki laki	Wirausaha/Wiraswasta	Ya	Baik	Media sosial	Ya	Mengabaikan pesan	2
Aliah	41 - 54 tahun	Perempuan	Ibu rumah tangga	Ya	Baik	Teman/Keluarga	Ya	Melaporkan ke WhatsApp	1
Iwan romansyah	19 - 25 tahun	Laki laki	Wirausaha/Wiraswasta	Ya	Baik	Media sosial	Ya	Mengabaikan pesan	1
Nuraeni	19 - 25 tahun	Perempuan	Pegawai Swasta	Ya	Baik	Sekolah/Kuliah	Ya	Mengabaikan pesan	3
Maulana	19 - 25 tahun	Perempuan	Pelajar/Mahasiswa	Ya	Baik	Teman/Keluarga	Ya	Mengabaikan pesan	3
Rohman Suryana	41 - 54 tahun	Laki laki	Wirausaha/Wiraswasta	Ya	Baik	Teman/Keluarga	Ya	Mengabaikan pesan	1
Fan	19 - 25 tahun	Laki laki	Pelajar/Mahasiswa	Ya	Sangat Baik	Media sosial	Ya	Mengabaikan pesan	3
Iwan ridwan	26 - 40 tahun	Laki laki	Wirausaha/Wiraswasta	Ya	Cukup	Media sosial	Ya	Mengabaikan pesan	3
Tita Teresnawati	19 - 25 tahun	Perempuan	Ibu rumah tangga	Ya	Baik	Media sosial	Tidak	Tidak pernah	5
Muhamad khadafi	19 - 25 tahun	Laki laki	Pegawai Swasta	Ya	Baik	Media sosial	Ya	Melaporkan ke WhatsApp	2
Hera	19 - 25 tahun	Perempuan	Pegawai Swasta	Ya	Baik	Media sosial	Ya	Melaporkan ke WhatsApp	4
Ade	26 - 40 tahun	Laki laki	Wirausaha/Wiraswasta	Ya	Cukup	Teman/Keluarga	Ya	Mengabaikan pesan	1

1	1	1	Ya	Sangat efektif	Video edukasi
1	1	1	Ya	Sangat efektif	Video edukasi
2	2	1	Ya	Efektif	Video edukasi
1	1	1	Ya	Sangat efektif	Media sosial
2	2	1	Ya	Sangat efektif	Media sosial
3	3	3	Ya	Efektif	Poster
1	1	1	Ya	Efektif	Video edukasi
1	1	1	Ya	Sangat efektif	Media sosial
3	3	1	Ya	Efektif	Video edukasi
1	2	2	Ya	Sangat efektif	Media sosial
1	2	1	Ya	Sangat efektif	Video edukasi
1	1	1	Ya	Efektif	Media sosial
1	1	1	Ya	Sangat efektif	Seminar/workshop
2	2	2	Ya	Efektif	Media sosial
1	2	1	Ya	Sangat efektif	Media sosial
4	3	2	Ya	Sangat efektif	Media sosial
3	2	1	Ya	Sangat efektif	Media sosial
1	3	1	Ya	Efektif	Video edukasi
2	2	1	Ya	Efektif	Media sosial
3	2	2	Ya	Efektif	Media sosial
1	3	1	Ya	Sangat efektif	Media sosial



Online	Besar	Ya	Menggunakan autentikasi dua faktor	
Online	Sangat besar	Ya	Memperbarui aplikasi secara teratur	
Online	Besar	Ya	Menggunakan autentikasi dua faktor	
Online	Sangat besar	Ya	Memperbarui aplikasi secara teratur	
Keduanya	Besar	Ya	Tidak mengklik tautan mencurigakan	
Keduanya	Besar	Ya	Memperbarui aplikasi secara teratur	
Offline	Besar	Ya	Tidak mengklik tautan mencurigakan	
Online	Besar	Ya	Tidak mengklik tautan mencurigakan	
Online	Besar	Ya	Menggunakan autentikasi dua faktor	
Online	Besar	Ya	Menggunakan autentikasi dua faktor	
Online	Sangat besar	Ya	Memperbarui aplikasi secara teratur	
Online	Besar	Ya	Memperbarui aplikasi secara teratur	
Offline	Sangat besar	Ya	Tidak mengklik tautan mencurigakan	
Online	Besar	Ya	Tidak mengklik tautan mencurigakan	
Online	Sangat besar	Ya	Memperbarui aplikasi secara teratur	
Online	Sangat besar	Ya	Tidak mengklik tautan mencurigakan	
Online	Besar	Ya	Tidak mengklik tautan mencurigakan	
Keduanya	Besar	Ya	Tidak mengklik tautan mencurigakan	
Online	Besar	Ya	tidak di kenal, tidak sembarang mengklik tautan mencurigakan, perketat keamanan hp	
Online	Cukup besar	Ya	Tidak mengklik tautan mencurigakan	
Online	Sangat besar	Ya	Memperbarui aplikasi secara teratur	

Gambar 4. 7 Data kuisioner *posttest* responden 30 – 50

4.4. Analisis Hasil

4.4.1. Tingkat pengetahuan tentang *phishing*

Tabel 4. 1 Pengetahuan *phsihing*

Pre-Test	*Post-Test*
Ya: 30 orang (60%)	Ya: 50 orang (100%)
Tidak: 20 orang (40%)	Tidak: 0 orang (0%)

Analisis: Setelah edukasi, semua responden (100%) telah mendengar tentang *phishing*, meningkat dari 60% pada *pre-test.*

4.4.2. Tingkat pemahaman tentang *phishing*

Tabel 4. 2 Tingkat pemahaman phsihing

Pre-Test	*Post-Test*
Sangat Baik: 5 orang (10%)	Sangat Baik: 20 orang (40%)
Baik: 10 orang (20%)	Baik: 20 orang (40%)
Cukup: 5 orang (10%)	Cukup: 5 orang (10%)
Kurang: 10 orang (20%)	Kurang: 5 orang (10%)
Tidak Tahu: 20 orang (40%)	Tidak Tahu: 0 orang (0%)

Analisis: Setelah edukasi, 80% responden memiliki pemahaman yang baik hingga sangat baik, meningkat 30% dari pada *pre-test*. Tidak ada responden yang tidak tahu tentang *phishing* setelah edukasi.

4.4.3. Sumber informasi tentang *phishing*

Tabel 4. 3 Sumber informasi *phsihing*

Pre-Test	*Post-Test*
Media Sosial: 20 orang (40%)	Media Sosial: 25 orang (50%)
Teman/Keluarga: 15 orang (30%)	Teman/Keluarga: 15 orang (30%)
Media Berita: 10 orang (20%)	Media Berita: 5 orang (10%)
Lainnya: 5 orang (10%)	Lainnya: 5 orang (10%)

Media sosial tetap menjadi sumber utama informasi tentang phishing, dengan peningkatan dari 40% pada *pre-test* menjadi 50% pada *post-test*. Sumber informasi lainnya tidak mengalami perubahan signifikan.

4.4.4. Pengalaman menerima pesan mencurigakan

Tabel 4. 4 Pengalaman pesan mencurigakan

Pre-Test	*Post-Test*
Ya: 25 orang (50%)	Ya: 40 orang (80%)
Tidak: 25 orang (50%)	Tidak: 10 orang (20%)

Setelah edukasi, jumlah responden yang pernah menerima pesan mencurigakan meningkat dari 50% menjadi 80%. Ini mungkin menunjukkan bahwa edukasi membantu mereka lebih mengenali pesan mencurigakan.

4.4.5. Respon terhadap pesan mencurigakan

Tabel 4. 5 Respon terhadap pesan mencurigakan

Pre-Test	*Post-Test*
Mengabaikan: 15 orang (30%)	Media Sosial: 25 orang (50%)
Melaporkan ke WhatsApp: 5 orang (10%)	Melaporkan ke WhatsApp: 20 orang (40%)
Membagikan dengan teman/keluarga: 10 orang (20%)	Membagikan dengan teman/keluarga: 15 orang (30%)

Tidak melakukan apa-apa: 20 orang (40%)	Tidak melakukan apa-apa: 5 orang (10%)

Setelah edukasi, ada peningkatan signifikan dalam tindakan melaporkan pesan mencurigakan ke *WhatsApp*, dari 10% pada *pre-test* menjadi 40% pada *post-test*. Jumlah responden yang tidak melakukan apa-apa terhadap pesan mencurigakan menurun dari 40% menjadi 10%.

4.4.6. Pemahaman tentang langkah pencegahan *phishing*

Tabel 4. 6 Pemahaman pencegahan *phishing*

Pre-Test	*Post-Test*
Sangat Baik: 5 orang (10%)	Sangat Baik: 20 orang (40%)
Baik: 10 orang (20%)	Baik: 20 orang (40%)
Cukup: 5 orang (10%)	Cukup: 5 orang (10%)
Kurang: 15 orang (30%)	Kurang: 5 orang (10%)
Tidak Tahu: 15 orang (30%)	Tidak Tahu: 0 orang (0%)

Analisis: Setelah edukasi, 80% responden memiliki pemahaman yang baik hingga sangat baik tentang langkah pencegahan *phishing*, meningkat dari 30% pada *pre-test.* Tidak ada responden yang tidak tahu tentang langkah pencegahan setelah edukasi.

4.4.7. Keyakinan dapat mengenali pesan *phishing*

Tabel 4. 7 Keyakinan mengenali pesan *phishing*

Pre-Test	*Post-Test*
Sangat Yakin: 5 orang (10%)	Sangat Yakin: 20 orang (40%)
Yakin: 10 orang (20%)	Yakin: 20 orang (40%)
Cukup Yakin: 10 orang (20%)	Cukup Yakin: 5 orang (10%)
Kurang Yakin: 10 orang (20%)	Kurang Yakin: 5 orang (10%)
Tidak Yakin: 15 orang (30%)	Tidak Yakin: 0 orang (0%)

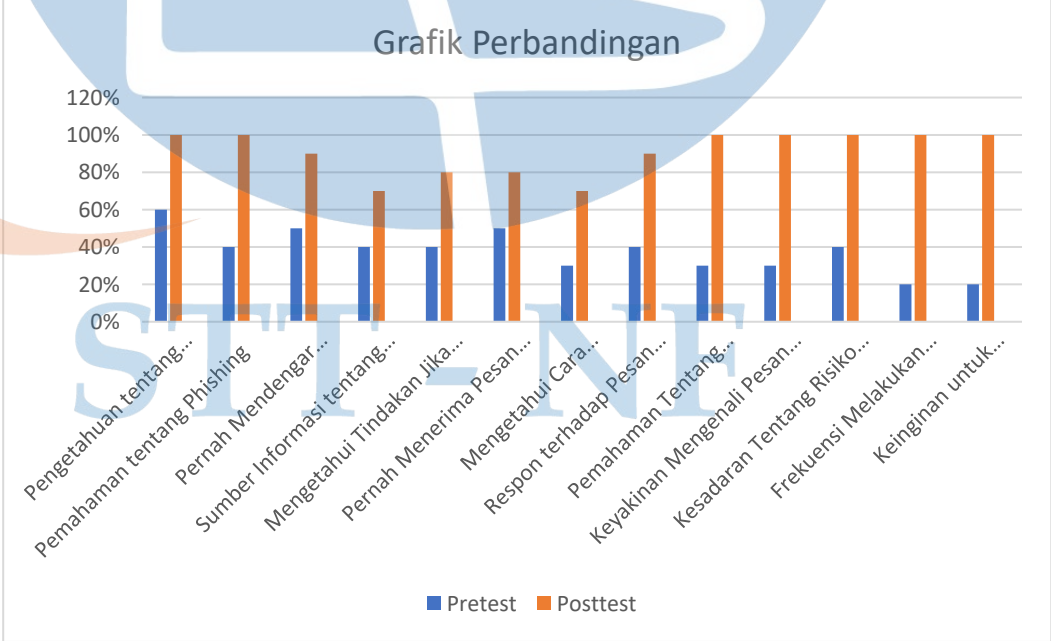
Analisis: Setelah edukasi, 80% responden merasa sangat yakin atau yakin dapat mengenali pesan *phishing*, meningkat 30% dari pada *pre-test*. Tidak ada responden yang merasa tidak yakin setelah edukasi.

4.4.8. Keinginan untuk meningkatkan pengetahuan tentang *phishing*

Tabel 4. 8 Keinginan meningkatkan pengetahuan

Pre-Test	*Post-Test*
Sangat Ingin: 10 orang (20%)	Sangat Ingin: 25 orang (50%)
Ingin: 15 orang (30%)	Ingin: 20 orang (40%)
Cukup Ingin: 10 orang (20%)	Cukup Ingin: 5 orang (10%)
Kurang Ingin: 5 orang (10%)	Kurang Ingin: 0 orang (0%)
Tidak Ingin: 10 orang (20%)	Tidak Ingin: 0 orang (0%)

Analisis: Setelah edukasi, keinginan untuk meningkatkan pengetahuan tentang *phishing* sangat meningkat, dengan 90% responden merasa sangat ingin atau ingin meningkatkan pengetahuan mereka, dibandingkan dengan 50% pada pre-test. Tidak ada responden yang tidak ingin meningkatkan pengetahuan mereka setelah edukasi.



Gambar 4. 8 Grafik Perbandingan

Dari grafik tersebut, terlihat peningkatan yang signifikan dalam semua aspek kesadaran masyarakat tentang *phishing* setelah dilakukan edukasi. Peningkatan terbesar terlihat pada pengetahuan tentang *phishing*, pemahaman tentang *phishing*, dan kesadaran akan risiko membuka link yang tidak dikenal. Sebelumnya, beberapa aspek memiliki kesadaran yang rendah seperti kepercayaan terhadap keamanan *WhatsApp* dan keyakinan dalam mengenali pesan *phishing*, tetapi setelah edukasi, ada peningkatan yang signifikan.

BAB V
KESIMPULAN DAN SARAN

5.1. Kesimpulan

1. Tingkat Kesadaran Masyarakat RT. 001 Dusun Cikole, Desa Ranggon tentang Ancaman *Phishing* melalui Aplikasi *WhatsApp,* Sebelum diberikan edukasi mengenai ancaman *phishing,* tingkat kesadaran masyarakat RT. 001 Dusun Cikole, Desa Ranggon tergolong rendah. Hasil *pre-test* menunjukkan bahwa sebagian besar responden belum memahami secara mendalam tentang *phishing* dan cara mengatasinya. Dari 50 responden, hanya sekitar 50% yang pernah mendengar tentang *phishing* di *WhatsApp,* dan lebih sedikit lagi yang mengetahui tindakan yang harus dilakukan jika menerima pesan *phishing*. Persentase responden yang mengetahui ciri-ciri pesan *phishing,* cara melaporkannya, dan tindakan pencegahan juga berada di bawah 50%.
2. Pendekatan edukasi dalam meningkatkan kesadaran masyarakat RT. 001 Dusun Cikole, Desa Ranggon tentang ancaman *phishing* di *WhatsApp* pendekatan edukasi yang dilakukan melalui serangkaian materi yang disampaikan selama tujuh hari berhasil meningkatkan kesadaran masyarakat secara signifikan. Hasil *post-test* menunjukkan peningkatan yang drastis di berbagai aspek kesadaran tentang *phishing*. Persentase responden yang pernah mendengar tentang *phishing* meningkat menjadi 90%, dan mereka yang mengetahui tindakan yang harus diambil jika menerima pesan *phishing* meningkat menjadi 80%. Pemahaman tentang ciri-ciri pesan *phishing*, cara melaporkan *phishing*, dan tindakan pencegahan juga meningkat.

5.2. Saran

Berdasarkan hasil penelitian yang telah dilaksanakan mengenai peningkatan kesadaran masyarakat RT. 001 Dusun Cikole, Desa Ranggon terhadap ancaman *phishing* melalui *WhatsApp*, berikut beberapa saran untuk penelitian selanjutnya:

1. Perluasan Populasi dan Sampel

Penelitian selanjutnya dapat memperluas cakupan populasi dan sampel ke wilayah yang lebih luas, seperti seluruh Desa Ranggon atau beberapa desa lainnya. Hal ini akan memberikan gambaran yang lebih komprehensif tentang kesadaran masyarakat di berbagai daerah.

2. Pendalaman Materi Edukasi

Materi edukasi bisa diperluas dan diperdalam dengan melibatkan lebih banyak aspek keamanan siber, seperti serangan *malware*, penipuan *online* lainnya, dan cara mengamankan akun digital. Penelitian ini bisa juga mengevaluasi pemahaman masyarakat tentang berbagai ancaman tersebut.

3. Penggunaan Teknologi dalam Edukasi

Menerapkan teknologi seperti aplikasi *mobile* untuk edukasi atau gamifikasi dalam penyampaian materi bisa menjadi fokus penelitian selanjutnya. Evaluasi efektivitas penggunaan teknologi ini dapat memberikan *insight* baru tentang cara meningkatkan kesadaran masyarakat

DAFTAR PUSTAKA

[1] D. A. Rabbani, "Pengaruh Perkembangan Teknologi terhadap Kehidupan dan Interaksi Sosial Masyarakat Indonesia." [Daring]. Tersedia pada: https://www.researchgate.net/publication/375525102

[2] J. Pembangunan, P. : Fondasi, D. Aplikasi, M. Ngafifi, S. Negeri, dan S. Wonosobo, "Kemajuan Teknologi dan Pola Hidup Manusia ... Muhamad Ngafifi 33 KEMAJUAN TEKNOLOGI DAN POLA HIDUP MANUSIA DALAM PERSPEKTIF SOSIAL BUDAYA." [Daring]. Tersedia pada: http://www.tempo.co/read/news/2010/12/23

[3] I. Radiansyah dan Y. Priyadi, "ANALISIS ANCAMAN PHISHING DALAM LAYANAN ONLINE BANKING," *Bulan Januari Tahun*, vol. 7, no. 1, hlm. 1–14, 2016, [Daring]. Tersedia pada: http://ejournal.umm.ac.id/index.php/

[4] R. Syah, "STRATEGI KEPOLISIAN DALAM PENCEGAHAN KEJAHATAN PHISING MELALUI MEDIA SOSIAL DI RUANG SIBER," *Jurnal Impresi Indonesia*, vol. 2, no. 9, hlm. 864–870, Sep 2023, doi: 10.58344/jii.v2i9.3594.

[5] I. Kadek Odie Kharisma Putra, I. Made Adi Darmawan, I. Putu Gede Juliana, K. Kunci, dan C. Crime, "TINDAKAN KEJAHATAN PADA DUNIA DIGITAL DALAM BENTUK PHISING CRIMINAL ACTS IN THE DIGITAL WORLD WITH A FORM OF PHISHING," 2022.

[6] N. Vadila dan A. R. Pratama, "Analisis Kesadaran Keamanan Terhadap Ancaman *Phishing*."

[7] D. Gustina, N. Aisyah, A. Syah Putra, V. Valentino, dan B. Sriyono Prasetyo, "Analisis Penyadapan pada Aplikasi *WhatsApp* Menggunakan Sinkronisasi Data," 2022.

[8] M. H. Wibowo dan N. Fatimah, "ANCAMAN PHISHING TERHADAP PENGGUNA SOSIAL MEDIA DALAM DUNIA CYBER CRIME," 2017.

[9] E. W. Tyas Darmaningrat *dkk.*, "Sosialisasi Bahaya dan Upaya Pencegahan *Social Engineering* untuk Meningkatkan Kesadaran Masyarakat tentang

Keamanan Informasi," *Sewagati*, vol. 6, no. 2, Feb 2022, doi: 10.12962/j26139960.v6i2.92.

[10] F. P. N. Koten, A. Jufriansah, dan H. Hikmatiar, "Analisis Penggunaan Aplikasi Whatsapp sebagai Media Informasi dalam Pembelajaran: *Literature Review*," *Jurnal Ilmu Pendidikan (JIP) STKIP Kusuma Negara*, vol. 14, no. 1, hlm. 72–84, Jul 2022, doi: 10.37640/jip.v14i1.1409.

[11] M. R. Ramadhani dan A. Raf'ie Pratama, "Analisis Kesadaran *Cybersecurity* Pada Pengguna Media Sosial Di Indonesia."

[12] N. Vadila dan A. R. Pratama, "Analisis Kesadaran Keamanan Terhadap Ancaman *Phishing*."

[13] M. Mulyadi, "PENELITIAN KUANTITATIF DAN KUALITATIF SERTA PEMIKIRAN DASAR MENGGABUNGKANNYA," 2011.

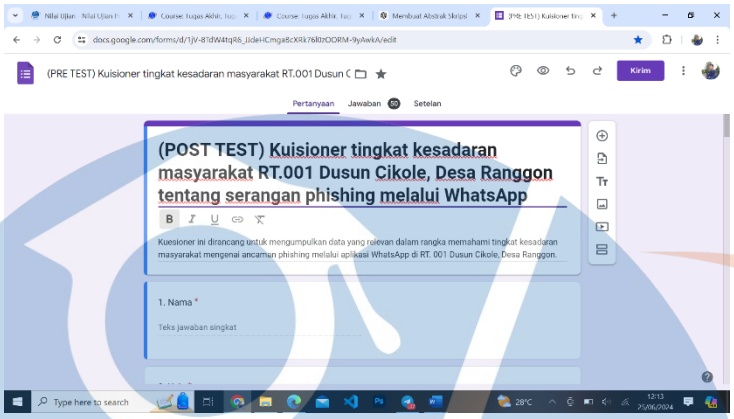
[14] katadata.co.id.(2023, 24 Februari). Kominfo Catatkan 1.730 Kasus Penipuan Online, Kerugian Ratusan Triliun. https://katadata.co.id/digital/teknologi/63f8a599de801/kominfo-catatkan-1730-kasus-penipuan-online-kerugian-ratusan-triliun

[15] detikinet.(2023, 24 November). Statistik Kejahatan Siber di Indonesia Selama 2023. https://inet.detik.com/security/d-7054249/statistik-kejahatan-siber-di-indonesia-selama-2023

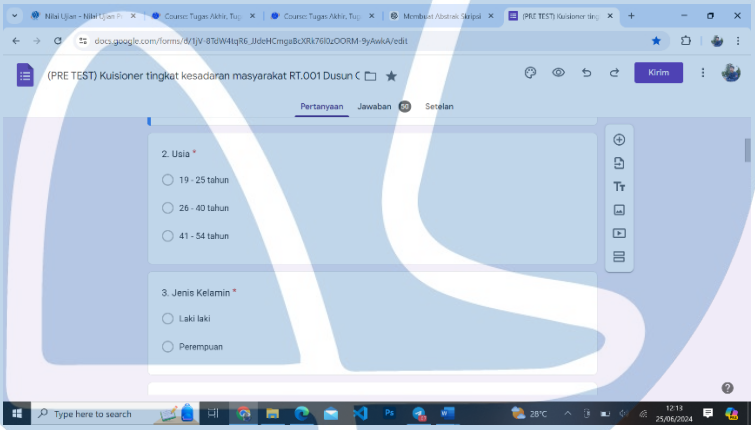
[16] GoodStats.(2023, 9 Mei). Serangan Phishing di Indonesia Terus Meningkat, Ini Datanya. https://goodstats.id/article/serangan-phishing-di-indonesia-terus-meningkat-ini-statistiknya-U8VdY

LAMPIRAN

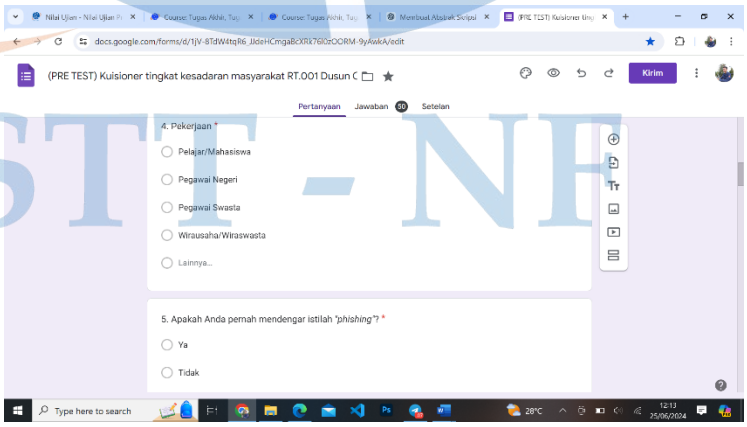
Kuisionet *Pretest dan Posttest*



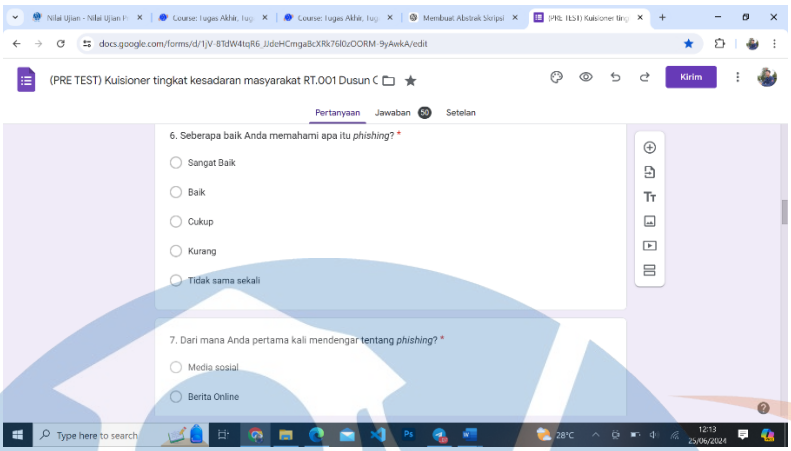
Gambar A. 1



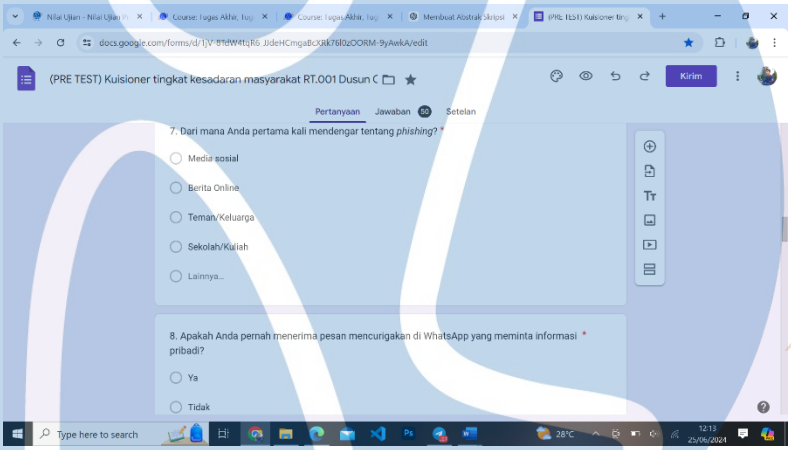
Gambar A. 2



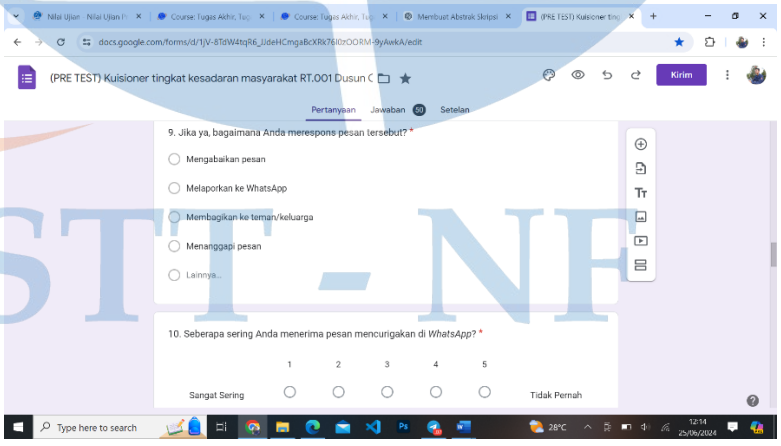
Gambar A. 3



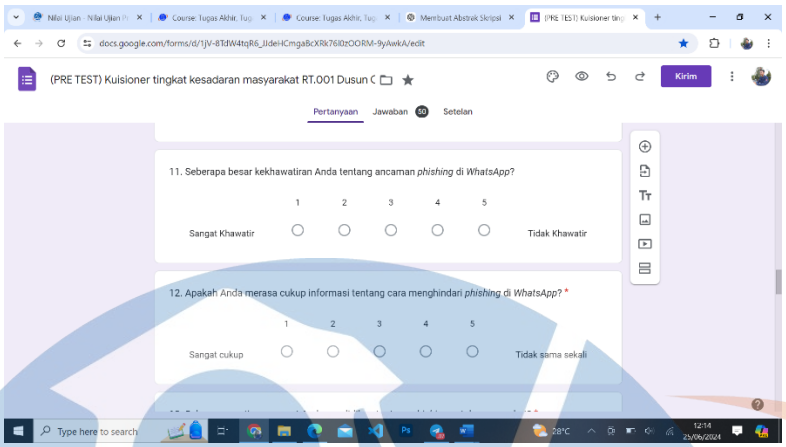
Gambar A. 4



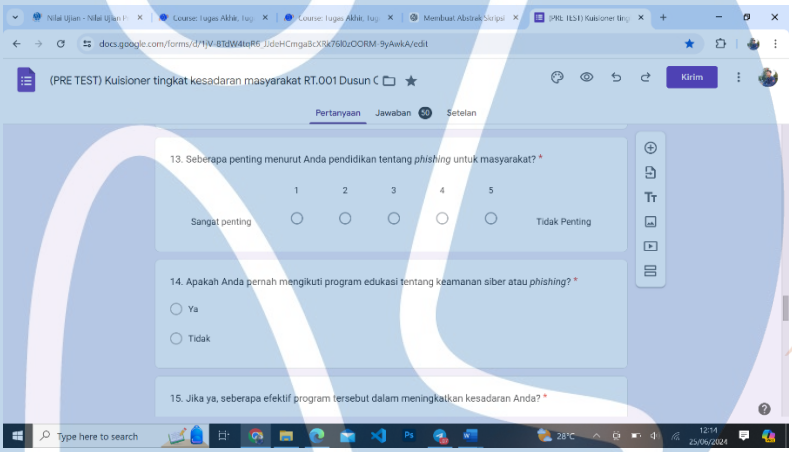
Gambar A. 5



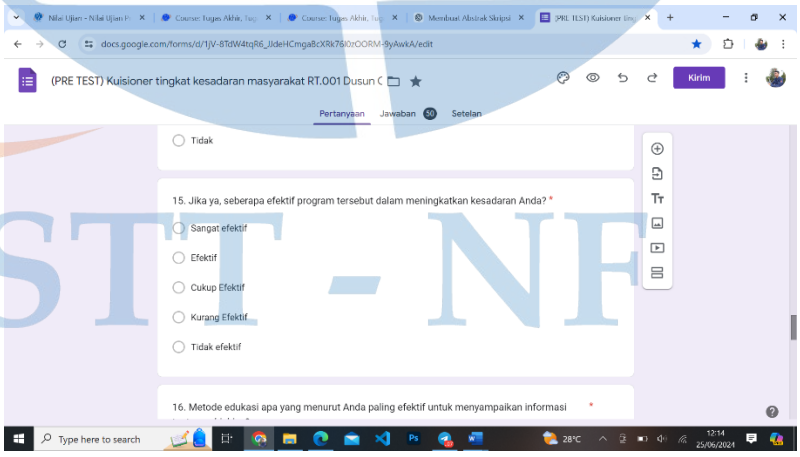
Gambar A. 6



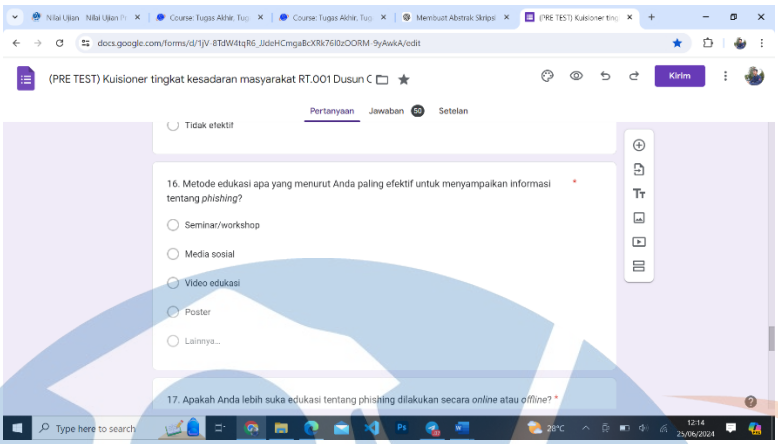
Gambar A. 7



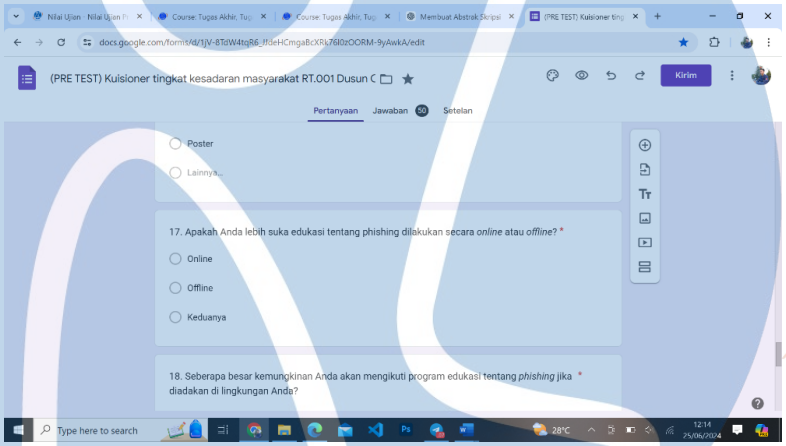
Gambar A. 8



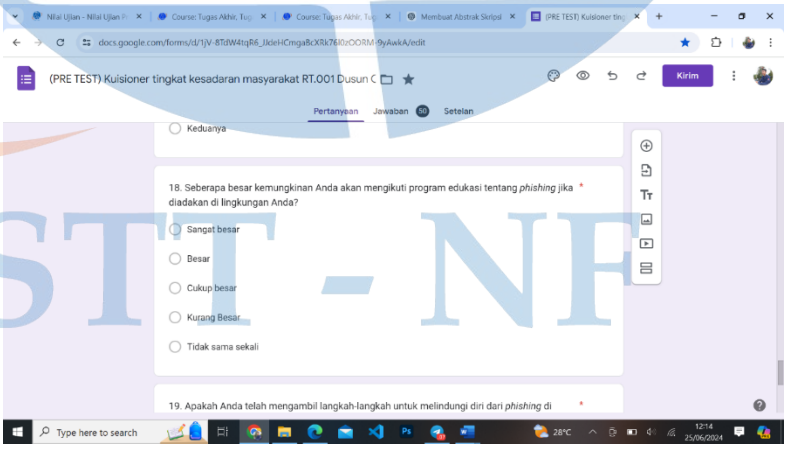
Gambar A. 9



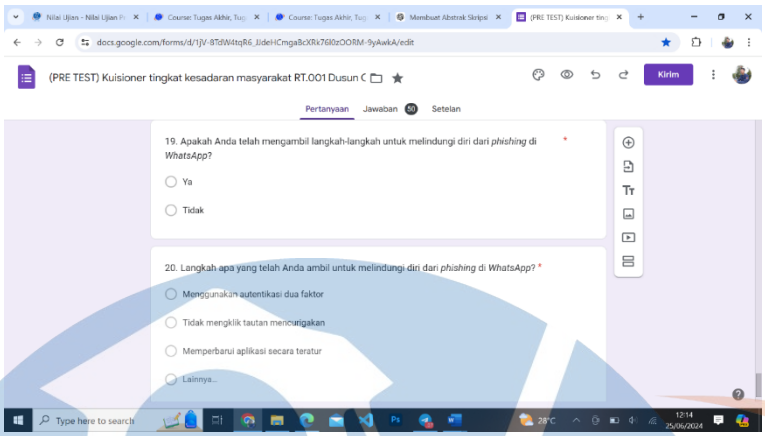
Gambar A. 10



Gambar A. 11



Gambar A. 12



Gambar A. 13