MODUL PENGABDIAN KEPADA MASYARAKAT

PENINGKATAN KESADARAN ANTI-PHISING MELALUI APLIKASI TRUECALLER DI ERA DIGITALISASI PADA KELURAHAN GUNUNG SARI, SURABAYA

Presented by : Kelompok 8 KKN Tematik SDGs

UNIVERSITAS PEMBANAGUNAN NASIONAL "VETERAN" JAWA TIMUR

2025

MODUL PENGABDIAN KEPADA MASYARAKAT

PENINGKATAN KESADARAN ANTI-PHISING MELALUI APLIKASI *TRUECALLER* DI ERA DIGITALISASI PADA KELURAHAN GUNUNG SARI

Oleh:

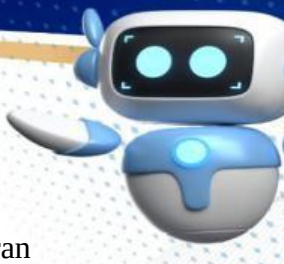
JOKO MIJIARTO, S.Hut, M.Si.

NIP. 199105122024061004

1.	**Farid Pradipta**	**19035010076**
2.	**Helvyyana Wulandari**	**22013010247**
3.	**Yunita Anggraini Setyawati**	**22013010354**
4.	**Diana Zain Wulan Fitriana**	**22071010113**
5.	**Muchammad Basroil Billah**	**22081010260**

KELOMPOK 8 KKN SDGS
UNIVERSITAS PEMBANGUNAN NASIONAL
“VETERAN” JAWA TIMUR
SURABAYA

2025



HALAMAN PENGESAHAN

1. Judul Modul : Peningkatan Kesadaran Anti-Phising Melalui Aplikasi *Truecaller* di Era Digitalisasi pada Kelurahan Gunung Sari
2. Pemanfaatan Iptek : *Truecaller* dan Canva
3. Nama Dosen Pembimbing Lapangan
   a. Nama : Joko Mijiarto, S.Hut. M.Si.
   b. NIP : 199105122024061004
   c. Jabatan Fungsional : Asisten Ahli
   d. Program Studi : Pariwisata
   e. Nomor HP : 082299166098
   f. Alamat e-mail : joko.mijiarto.par@upnjatim.ac.id
   g. Perguruan Tinggi : UPN "Veteran" Jawa Timur
4. Lokasi Kegiatan : Kelurahan Gunung Sari, Kecamatan Dukuh Pakis, Kota Surabaya
5. Anggota
   1. Nama Lengkap : Farid Pradipta
      NPM : 19035010076
      Prodi/Fakultas : Teknik Sipil/FakultasTeknik
   2. Nama Lengkap : Helvyyana Wulandari
      NPM : 22013010247
      Prodi/Fakultas : Akuntansi/Fakultas Ekonomi dan Bisnis
   3. Nama Lengkap : Yunita Anggraini Setyawati
      NPM : 22013010354

Prodi/Fakultas : Akuntansi/Fakultas Ekonomi dan Bisnis

4. Nama Lengkap : Diana Zain Wulan Fitriana
   NPM : 22071010113
   Prodi/Fakultas : Hukum/Fakultas Hukum
5. Nama Lengkap : Muchammad Basroil Billah
   NPM : 22081010260
   Prodi/Fakultas : Informatika/Fakultas Ilmu Komputer

Surabaya, 22 Juli 2025

Menyetujui,

Dosen Pembimbing Lapangan	Ketua Kelompok
Joko Mijiarto, S.Hut., M.Si.	Fitria Rahmatul Laili
NIP. 199105122024061004	NPM. 22042010218

Mengetahui,
Kepala Lembaga Penelitian dan Pengabdian Kepada Masyarakat

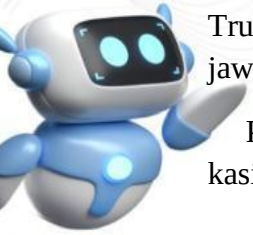
Prof. Dr. Ir. Rossyda Priyadharsini, M.P.
NIP. 19670310 199103 2001

KATA PENGANTAR

Segala puja dan puji syukur kehadirat Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya kepada penulis, sehingga modul dengan judul "Peningkatan Kesadaran Anti-Phising Melalui Truecaller Di Era Digitalisasi pada Kelurahan Gunung Sari" dapat penulis selesaikan dengan baik dan tepat waktu. Tak lupa sholawat serta salam semoga selalu tercurahkan kehadirat junjungan besar kita Rasulullah Muhammad SAW.

Modul ini ditulis dalam rangka memenuhi dan menyelesaikan luaran KKN Tematik SDGs 8 dan 11 sesuai dengan pedoman KKN Tematik SDGs 2025. Dengan pelaksanaan program yang diangkat dalam modul ini menyasar pada warga RW 7 Kelurahan Gunung Sari yang meliputi berbagai kalangan dari remaja hingga orang tua (usia 16–50 tahun).

Program ini dilaksanakan di Balai RW 7 Kelurahan Gunung Sari berupa workshop dengan menggunakan metode ceramah dan pelatihan. Ceramah dan pelatihan dilakukan dalam forum ini memanfaatkan teknologi canva memberikan pemahaman pentingnya waspada digital atau kesadaran anti-phising di era digital saat ini, adanya studi kasus, demo penggunaan aplikasi Truecaller, pencegahan, dan penanganan, sekaligus tanya jawab.



Penulis dengan penuh rasa hormat mengucapkan terima kasih kepada para pihak yang telah memberikan dorongan,

arahan, memotivasi, sekaligus berkontribusi dalam penulisan modul ini. Terutama kepada:

1. Bapak Joko Mijiarto, S.Hut. M.Si., selaku dosen pembimbing lapangan (DPL) KKN Tematik SDGs Kelompok 8 yang telah membantu, memberikan arahan, dorongan dan motivasi;
2. Ibu Siti Salmah A. M.d. selaku Ibu Lurah beserta staf yang sekaligus menjadi mitra kegiatan atas keramah tamahan, keterbukaan dan dukungan pada segala program kerja KKN Tematik SDGs Kelompok 8;
3. Para Warga Kelurahan Gunung Sari Kecamatan Dukuh Pakis Kota Surabaya atas segala keramah tamahan menerima, ikut andil dan mendukung segala program kerja kami sehingga dapat berjalan lancar;
4. Dan para rekan KKN Tematik SDGs Kelompok 8 sekalian yang tidak dapat disebutkan satu-persatu.

Akhir kata, penulis sadar akan segala kekurangan dan ketidaksempurnaan dalam penyusunan modul ini, sehingga saran dan kritik yang membangun sangat penulis harapkan.

Surabaya, 22 Juli 2025

Penulis

DAFTAR ISI

HALAMAN PENGESAHAN ii
KATA PENGANTAR iv
DAFTAR ISI vi
DAFTAR GAMBAR viii
DAFTAR TABEL ix
DAFTAR LAMPIRAN x
1. PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Tujuan 5
1.3 Manfaat 6
1.4 Sasaran 6
1.5 Ruang Lingkup 7
2. PELAKSANAAN KEGIATAN 7
3. HASIL DAN PEMBAHASAN 11
3.1 Pentingnya Edukasi Phising 11
3.1.1 Phising 11
3.1.2 Cara Kerja Phising 12
3.1.3 Strategi Meningkatkan Kesadaran Anti-Phising 14
3.2 Pemanfaatan Truecaller sebagai Alat Verifikasi 18
3.2.1 Truecaller 18
3.2.2 Instalasi dan Penggunaan *Truecaller* 25

3.3 Capaian Kegiatan 35
3.4 Kendala Kegiatan 38
4. PENUTUP 40
4.1 Kesimpulan 40
4.2 Saran 41
5. DAFTAR PUSTAKA 42
6. LAMPIRAN 44

DAFTAR GAMBAR

Gambar 1. Peta Lokasi Kelurahan 10
Gambar 2. Fitur ID Penelepon 20
Gambar 3. Fitur Pemblokir Spam 21
Gambar 4. Fitur Perpesanan 22
Gambar 5. Fitur Pencarian Nomor Cepat 23
Gambar 6. Fitur Tema Gelap 24
Gambar 7. Simbol Play Store dan App Store 25
Gambar 8. Dokumentasi Partisipasi Warga 26
Gambar 9. Warga Registrasi Truecaller 26
Gambar 10. Warga Registrasi Truecaller 27
Gambar 11. Dokumentasi Partisipasi Warga 28
Gambar 12. Verifikasi Nomor 28
Gambar 13. Verifikasi Nomor 29
Gambar 14. Verifikasi Nomor 29
Gambar 15. Verifikasi Nomor 30
Gambar 16. Nomor Terverifikasi 30
Gambar 17. Beranda Aplikasi Truecaller 32
Gambar 18. Halaman Informasi Nomor Aman 33
Gambar 19. Halaman Informasi Nomor Berbahaya 34
Gambar 20. Halaman Informasi Nomor Berbahaya 34
Gambar 21. Pendampingan dan Pengarahan Aplikasi Truecaller 37

DAFTAR TABEL

Tabel 1. Tabel Susunan Kegiatan 8
Tabel 2. Tabel Kendala dan Solusi 39

DAFTAR LAMPIRAN

Lampiran 1. Surat Kesediaan Kerjasama Mitra 44
Lampiran 2. Peta Lokasi Kegiatan 45
Lampiran 3. Dokumentasi Kegiatan 46
Lampiran 4. Slide Materi 47

PENINGKATAN KESADARAN ANTI-PHISING MELALUI APLIKASI *TRUECALLER* DI ERA DIGITALISASI PADA KELURAHAN GUNUNG SARI

[1]Joko Mijiarto, [2]Farid Pradipta, [3]Helvyyana Wulandari, [4]Yunita Anggraini Setyawati, [5]Diana Zain Wulan Fitriana, [6]Muchammad Basroil Billah

e-mail: [1]joko.mijiarto.par@upnjatim.ac.id,
[2]19035010076@student.upnjatim.ac.id,
[3]22013010247@student.upnjatim.ac.id,
[4]22013010354@student.upnjatim.ac.id,
[5]22071010113@student.upnjatim.ac.id,
[6]22081010260@student.upnjatim.ac.id

1. PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi yang pesat membawa perubahan atau dampak besar dalam kehidupan manusia, terutama modernisasi dalam hal akses dan pertukaran informasi di dunia digital. Segala aspek kehidupan masyarakat tentu mengikuti perkembangan zaman sebagaimana menyesuaikan kebutuhan yang kian berkembang. Sehingga didapatkan bahwa dunia digital kini menjadi bagian tak terpisahkan dari aktivitas sehari-hari manusia. Aktivitas yang dimaksud mulai dari komunikasi, transaksi keuangan, hingga konsumsi informasi melalui media sosial dan platform daring lainnya baik dalam bidang ekonomi, sosial budaya, pendidikan, serta dalam segala bidang kehidupan masyarakat (Kelas 4a4 & Iskandar, 2024).

Faktanya perkembangan teknologi digitalisasi mempermudah manusia melakukan aktivitas sehari-hari secara efektif dan efisien baik secara waktu, biaya yang dikeluarkan, dll. Namun kemudahan tersebut tidak dapat menghapuskan kenyataan lain yang dimana dapat membuka celah bagi berbagai bentuk kejahatan siber. Badan Siber dan Sandi Negara (BSSN) menyatakan bahwa serangan siber di Indonesia secara signifikan meningkatkan dari waktu ke waktu. Dikatakan pada tahun 2024, BSSN telah mencatat lebih dari 1,2 miliar anomali trafik yang berpotensi sebagai ancaman siber. Serangan siber tersebut meliputi phising, ransomware, sampai dengan peretasan. Salah satu kejahatan cyber yang marak dikalangan warga dalam kehidupan sehari-hari adalah phising (Kelas 4a4 & Iskandar, 2024). Oleh sebab, dalam pemanfaatan internet ini tidak sedikit orang menggunakannya internet secara tidak benar dan tidak sehat untuk mencari keuntungan pribadi yang disisi lain dapat merugikan orang lain (Dm et al., 2022).

Phising dari kata Fishing yang artinya memancing merupakan salah satu bentuk pemanfaatan internet yang tidak baik yakni teknik penipuan yang dilakukan dengan cara memancing orang lain untuk memberikan informasi atau data penting yang bersifat pribadi untuk tujuan kejahatan. Phising ini merupakan upaya penipuan dalam kategori kejahatan siber yang dilakukan oleh pihak tidak bertanggung jawab dengan cara menyamar seolah sumber terpercaya (terlihat sah) seperti melalui email, SMS, atau replika web untuk mendapatkan informasi/ data sensitif seperti kata sandi, pin, nomor kartu kredit, dan data pribadi sensitif lainnya (Cut Mutia & Rayyan

Firdaus, 2024). Semakin berkembangnya zaman modus phising ini juga ikut berkembang dan semakin canggih sehingga sulit dideteksi, seringkali menyamar melalui email, pesan instan, tautan mencurigakan, atau bahkan situs web palsu yang terlihat seperti aslinya sekaligus beragam bentuk lainnya.

Minimnya literasi dan kurangnya kewaspadaan digital serta kebiasaan menyebarkan atau menerima informasi secara mentah tanpa verifikasi terlebih dahulu menjadi faktor utama yang mempermudah pelaku phising melancarkan aksinya. Nyatanya warga tidak terkecuali warga Kelurahan Gunung Sari terkhusus pada masyarakat RW 7 Kelurahan Gunung Sari, Kecamatan Dukuh Pakis, Kota Surabaya ini sangat rentan menjadi korban karena kurangnya literasi digital serta ketidaktahuan terhadap modus-modus penipuan yang kian beragam, canggih dan semakin meyakinkan. Banyak korban yang tertipu dengan pesan palsu mengatasnamakan instansi resmi, tautan mencurigakan, hingga panggilan telepon dari nomor tidak dikenal. Aktivitas phising ini tidak hanya menimbulkan kerugian materil dalam hal finansial bagi individu, namun dapat pula merugikan secara immateril dengan merusak harkat martabat dan nama baik akibat penyalahgunaan. Oleh sebab itu, penting bagi setiap individu terutama warga RW 7 Kelurahan Gunung Sari untuk meningkatkan literasi digital, khususnya dalam hal verifikasi data dan informasi sebelum mempercayainya hingga mengambil tindakan atau menyebarkannya kembali. Warga masyarakat perlu membudayakan sikap kritis terhadap setiap informasi yang diterima dan memahami cara mengenali ciri-

ciri upaya phising, seperti adanya permintaan data pribadi yang tidak wajar, kesalahan penulisan, atau dapat membedakan antara domain situs asli dengan domain situs yang mencurigakan.

Salah satu kasus phising yang pernah terjadi di Indonesia tepatnya di Jakarta Selatan yakni adanya SMS phising melalui sinyal BTS palsu dengan modus mengendarai mobil yang telah dipasang alat BTS palsu. BTS palsu berfungsi mengirimkan SMS yang berisi link palsu yang menyamar seolah-olah dikirim oleh pihak perbankan. Korban sebanyak 259 mendapatkan SMS phising dengan total 12 yang sudah terjerat melakukan transaksi hingga mengalami kerugian total Rp 437 Juta. Kasus ini terjadi selama 2 kali, kali pertama pelaku lolos dan mendapatkan keuntungan serta pada kali kedua pelaku baru ditangkap. Kedua kali tersebut dengan modus yang sama disebutkan oleh Bareskrim Polri dan Polda Metro Jaya bahwa pelaku memanfaatkan pengiriman SMS ke alat komunikasi atau ponsel yang ada di sekitarnya. Ponsel yang mendapatkan pesan, kata dia, akan menerima sebuah SMS berisi pesan dengan iming-iming tertentu dan tautan yang sangat mirip dengan tautan resmi kemudian ketika tautan tersebut di klik, pemilik ponsel akan diarahkan mengisi data pribadi, seperti OTP dan CVV (Portal Antara *News*). Bermula dari sanalah data-data tersebut diatas sudah didapat oleh pelaku sehingga bisa digunakan oleh yang bersangkutan untuk melakukan aksi kejahatan yang merugikan bagi target.

Oleh karena itu, penulis merasa penting memberikan pemahaman waspada dan bahaya digital sebagai upaya peningkatan kesadaran dan pengetahuan masyarakat

pentingnya keamanan digital agar tidak mudah tertipu yang sekaligus menjadi langkah preventif untuk pengambilan langkah dikemudian hari. Sekaligus diharapkan memberikan *impact* yang bermakna dengan adanya kemampuan melakukan verifikasi dasar seperti mengecek nomor mencurigakan melalui aplikasi pengidentifikasi seperti *Truecaller*. Aplikasi *Truecaller* sendiri merupakan aplikasi yang berfungsi dapat mencari identitas dari nomor telepon dan pemblokir nomor spam yang bisa didownload di Play Store maupun App Store. Dengan adanya modul ini besar harapan terhadap masyarakat akan dapat lebih mewaspadai dalam segala aktivitas digital terutama Warga RW 7 Kelurahan Gunung Sari dapat menjadi pengguna internet yang lebih bijak, waspada, serta dapat melindungi dirinya dari kejahatan siber dengan memiliki kemampuan identifikasi dasar memanfaatkan aplikasi pengidentifikasi seperti *Truecaller*.

1.2 Tujuan

Tujuan pembuatan modul ini adalah sebagai berikut:

1. Memberikan pemahaman dasar kepada masyarakat mengenai apa itu phising, berbagai cara kerja/modus phising (penipuan online) yang sering terjadi, dan penanganan.
2. Meningkatkan kesadaran masyarakat terhadap pentingnya verifikasi informasi sebelum memberikan data pribadi atau melakukan tindakan tertentu.
3. Mengajarkan cara-cara sederhana dalam mendeteksi penipuan digital, termasuk pengecekan nomor mencurigakan menggunakan *Truecaller*.

4. Mendorong masyarakat untuk menjadi lebih waspada dan bijak dalam penggunaan teknologi digital.

1.3 Manfaat

Manfaat pembuatan modul ini sendiri dapat menjadi referensi menambah ilmu atau pedoman bagi pembaca terutama sasaran program yakni para warga RW 7 Kelurahan Gunung Sari, meningkatkan kesadaran mereka dalam hal mewaspadai era digitalisasi dalam konteks media digital dan penggunaan teknologi digital dengan bijak selama transaksi atau kegiatan digital seperti:

1. Pemahaman dasar kepada masyarakat mengenai apa itu phising, berbagai cara kerja/modus phising (penipuan online) yang sering terjadi, pencegahan dan penanganan;
2. Pentingnya verifikasi informasi sebelum memberikan data pribadi atau melakukan tindakan tertentu;
3. Cara-cara sederhana dalam mendeteksi penipuan digital, termasuk pengecekan nomor mencurigakan menggunakan *Truecaller*.

1.4 Sasaran

Modul ini dibuat untuk menambah pengetahuan dan menjadi pedoman untuk pembaca terutama masyarakat umum yang rentan menjadi sasaran oknum tidak bertanggung jawab. Khususnya pelaksanaan program ini menyasar pada warga RW 7 Kelurahan Gunung Sari meliputi berbagai kalangan dari remaja hingga orang tua (usia 16–50 tahun) yang memiliki berbagai jenis pekerjaan seperti para UMKM daerah sana agar lebih aware terhadap bahaya teknologi digital sehingga dapat

memberikan perkembangan positif dan perlindungan diri dalam kegiatan masyarakat sehari-hari.

1.5 Ruang Lingkup

Modul dengan judul "Peningkatan Kesadaran Anti-phising Melalui Truecaller di Era Digitalisasi pada Kelurahan Gunung Sari" ini ditulis agar dapat memberikan gambaran pada masyarakat pentingnya waspada dan perlindungan data diri pribadi pada era digital saat ini, memahami konsep dasar phising hingga cara kerja phising, bahaya phising, konsep Truecaller sekaligus instalasi dan penggunaan Truecaller sebagai alat dasar pengidentifikasi dan alat bantu pemblokir aktivitas phising. Modul ini hanya mencakup cara verifikasi dasar untuk melindungi data diri pribadi, sehingga tidak mencakup hal-hal lain diluar konsep dasar dan verifikasi dasar terutama fitur yang tidak dimiliki oleh aplikasi *Truecaller*. Hal ini oleh karena, aplikasi hanya mampu melindungi pribadi dari gangguan atau ancaman phising secara dasar namun belum mampu untuk mendeteksi lokasi pelaku phising hingga identitas asli pelaku atau pengidentifikasian secara mendalam.

2. PELAKSANAAN KEGIATAN

Kegiatan atau program kerja pengabdian kepada masyarakat dengan mengusung tema "Waspada Digital" yang dipersembahkan oleh Kelompok KKN SDGs Universitas Pembangunan Nasional "Veteran" Jawa Timur ini dilaksanakan di Balai RW 7 Kelurahan Gunung Sari Kecamatan Dukuh Pakis, pada hari Sabtu, 19 Juli 2025, pukul 08.15–11.00 WIB. Kegiatan ini merupakan kegiatan pemberdayaan masyarakat menciptakan masyarakat anti-

phising dengan mengusung bentuk pembelajaran secara teori dikombinasi adanya pelatihan dalam praktiknya agar masyarakat mampu mengidentifikasi upaya-upaya phising serta bagaimana cara menghadapinya agar lebih bijaksana dalam pemanfaatan digital.

Kegiatan ini menggunakan metode pelaksanaan kombinasi antara sosialisasi/penyuluhan, forum diskusi interaktif disertai tanya jawab, praktik dan pendampingan langsung dalam upaya anti-phising. Kegiatan ini memberikan 2 pemateri langsung, materi disampaikan oleh mahasiswa Informatika Universitas Pembangunan Nasional "Veteran" Jawa Timur yakni Muchammad Basroil Billah dan Bryan Alexander Sihaloho. Dengan susunan acara sebagai berikut.

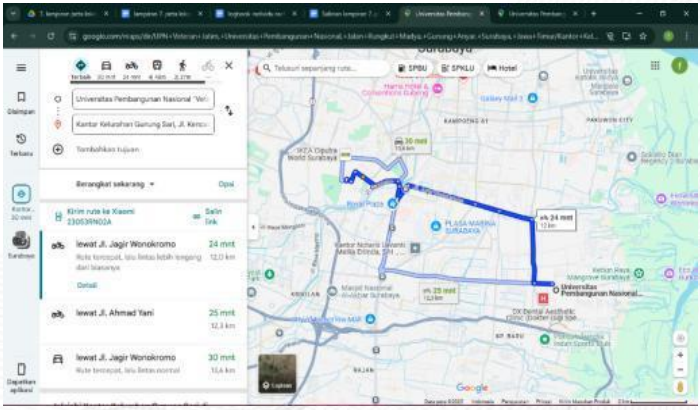
Tabel 1. Tabel Susunan Kegiatan

No	Waktu (WIB)	Kegiatan
1	08.15–08.40	Kedatangan & Persiapan Panitia di Balai Desa
2	08.40 – 08.45	Briefing Singkat Panitia & Penataan Tempat
3	08.45 – 09.00	Registrasi & Penyambutan Peserta

4	09.00 – 09.05	Pembukaan oleh MC
5	09.05 – 09.08	Menyanyikan Lagu Indonesia Raya
6	09.08– 09.10	Sambutan
7	09.10 – 09.40	Pemaparan Materi
8	09.40 – 10.00	Sesi Tanya Jawab Berhadiah
9	10.00– 10.40	Pelatihan dan Pendampingan Penggunaan Aplikasi, Penutupan & Ucapan Terima Kasih
10	10.40 – 10.55	Dokumentasi Foto Bersama
11	10.55 – 11.00	Evaluasi

Kegiatan ini menyasar kepada warga RW 7 Kelurahan Gunung Sari dari berbagai kalangan baik remaja hingga

orang tua (usia 16–50 tahun) yang sekaligus beberapa diantaranya merupakan para pelaku UMKM. Lokasi pelaksanaan di Balai RW 7 Kelurahan Gunung Sari Kecamatan Dukuh Pakis yang terlampir pada peta kelurahan di bawah ini:



Gambar 1. Peta Lokasi Kelurahan
(Sumber: Google Maps)

3. HASIL DAN PEMBAHASAN

3.1 Pentingnya Edukasi Phising

3.1.1 Phising

Definisi phising menurut Saputra et. al (2020) berasal dari kata dalam bahasa Inggris *fishing* yang berarti memancing, sesuai dengan maknanya, aktivitas ini bertujuan untuk "memancing" korban agar secara tidak sadar memberikan informasi pribadi mereka. Secara lebih spesifik, phising merupakan salah satu bentuk kejahatan siber (cyber crime) yang dilakukan melalui penipuan. Teknik ini biasanya digunakan untuk memperoleh data sensitif seperti nama pengguna (*username*), kata sandi (*password*), serta informasi kartu kredit, dengan cara menyamar sebagai pihak yang seolah-olah resmi dan terpercaya.

Serangan phising umumnya terjadi melalui komunikasi elektronik, seperti email atau pesan singkat (SMS), dan sangat sering menyasar pengguna layanan *online banking*. Hal ini karena layanan tersebut mengharuskan pengguna memasukkan data login, yang jika dimasukkan ke dalam halaman palsu (*fake login form*), maka data tersebut dapat dicuri oleh pelaku kejahatan. Selain perbankan, serangan ini juga menyasar pengguna internet secara umum, terutama melalui situs web dan media sosial yang terhubung dengan jaringan internet.

Pelaku phising dikenal dengan istilah *phiser*. Berbeda dengan *hacker*, yang pada awal kemunculannya justru dipandang positif karena merujuk pada individu yang ahli di bidang komputer dan mampu menciptakan program yang

lebih unggul dari rancangan sebelumnya. Sementara itu, *phiser* sejak awal sudah dikaitkan dengan makna negatif.

3.1.2 Cara Kerja Phising

Phising dari kata “fishing” yang berarti “memancing”, teknik ini biasanya dilakukan dengan cara mengirimkan pesan palsu yang menyamar seakan-akan bersumber dari pihak yang asli dan terverifikasi. Phising ini bekerja dengan berbagai cara kerja sesuai dengan jenis-jenisnya, namun tentunya aktivitas ini memuat unsur penipuan yakni mengelabui korban sehingga korban dengan sukarela mau memberikan data pribadinya.

Cara kerja phising secara umum pelaku melakukan pemalsuan identitas pribadi mengatasnamakan pihak resmi seperti bank, setelah itu pelaku mengirimkan pemberitahuan baik melalui SMS atau aplikasi yang memiliki fitur perpesanan lain terutama *WhatsApp*. Media seperti *WhatsApp* ini sering menjadi media praktik phising, pelaku mengirimkan tautan yang dapat berupa link, pdf, aplikasi serta bentuk-bentuk lain yang berisi malware berupa virus. Nantinya hal ini digunakan oleh pelaku tersebut dengan tujuan mendapat dan mengumpulkan data pribadi korban atau menyadap (membaca) ponsel korban dari jarak jauh. Apabila calon korban membuka tautan link, pdf, aplikasi tersebut biasanya akan diarahkan untuk mengisi data pribadi yang rawan penyalahgunaan seperti tanggal pengakhiran kartu, nomor ATM, kode otp, pin atau nomor id, (CVV) card konfirmasi nilai, (CVC) cek kartu kode atau kata sandi aplikasi (Cut Mutia & Rayyan Firdaus, 2024).

Dimasukkannya data pribadi secara lengkap dan akurat, hal ini akan disalahgunakan oleh pelaku dan biasanya terjadi pemindahan aset dari penguasaan oleh korban menjadi penguasaan milik pelaku. Berikut beberapa cara kerja phising sesuai dengan bentuk phising yang dilakukan, antara lain (Cut Mutia & Rayyan Firdaus, 2024):

1. Email Phising: biasanya dilakukan dengan adanya kiriman email palsu yang seolah-olah bersumber dari pihak asli yang terverifikasi, nantinya di dalam email didapati adanya tautan link yang mengandung list kelengkapan data pribadi
2. *Spear* Phising: biasanya menargetkan baik individu maupun organisasi dengan pengiriman pesan yang lebih personalisasi, pada konteksnya memiliki informasi target lebih detail sehingga terlihat meyakinkan dan terpercaya
3. *Malware* Phising: cara kerja jenis phising ini yakni dengan memanfaatkan *malware* atau virus untuk menyadap atau membaca data informasi calon korban dari jarak jauh
4. SMS Phising: phising sejenis ini biasanya dilakukan dengan memanfaatkan fitur SMS yakni mengirimkan pesan melalui media dengan fitur perpesanan sebagai media hubung pengiriman link situs palsu
5. Clone Phising: dengan memanfaatkan teknologi, phising ini mereplikasi sebuah situs web seolah web tiruan tersebut merupakan situs asli dengan tampilan yang sama dengan yang asli, pengguna yang tidak

mengetahui perbedaan situs web yang asli dengan yang palsu akan dengan mudah tertipu memasukkan informasi dan melakukan login di web tiruan/palsu sehingga nantinya informasi/data data tersebut dapat disalahgunakan

6. *Voice* Phising: *voice* phising ini bekerja dengan cara adanya panggilan telepon atau melalui rekaman suara palsu dalam hal ini mengandung pemanfaatan kerentanan berupa ketidaktahuan, kekhawatiran, perasaan dan ketergantungan calon korban dalam rangka mendapatkan informasi calon korban dengan tujuan utama menguntungkan diri pelaku

3.1.3 Strategi Meningkatkan Kesadaran Anti-Phising

1. Edukasi Melalui Sosialisasi dan Pelatihan

Edukasi menjadi fondasi utama dalam membangun kesadaran masyarakat terhadap ancaman phising. Penting untuk mengadakan kegiatan sosialisasi dan pelatihan secara rutin di berbagai kesempatan yang mudah diakses oleh warga Kelurahan Gunung Sari. Misalnya, seminar, workshop, atau pelatihan yang dikemas secara interaktif dan menarik agar peserta bisa memahami dengan baik apa itu phising, bagaimana modus-modusnya bekerja, serta dampak negatif yang dapat ditimbulkan bagi korban. Selain itu, penyebaran materi edukasi dalam bentuk leaflet, poster, ataupun video-video pendek dari media sosial juga harus dilakukan secara kontinu untuk mengingatkan masyarakat secara visual dan audio. Pemilihan bahasa yang mudah dimengerti serta penggunaan contoh kasus nyata yang dekat

dengan kehidupan sehari-hari akan membuat edukasi ini lebih relevan dan mudah diterima. Tidak kalah penting adalah melibatkan tokoh masyarakat, seperti ketua RT/RW, tokoh agama, dan figur yang disegani dalam komunitas. Kehadiran mereka dalam kegiatan sosialisasi akan menambah kredibilitas dan meningkatkan tingkat partisipasi masyarakat dalam memahami serta menerapkan langkah-langkah anti-phising.

2. Pemanfaatan Teknologi: Truecaller

Penggunaan teknologi modern adalah salah satu cara efektif untuk menangkal serangan phising, khususnya yang dilakukan melalui telepon dan SMS. Aplikasi Truecaller, misalnya, bisa menjadi alat utama dalam mendeteksi panggilan atau pesan yang berpotensi berbahaya. Melalui aplikasi ini, masyarakat dapat mengenali nomor-nomor tidak dikenal yang dicurigai sebagai spam atau penipu dan memblokirnya secara langsung. Truecaller juga menyediakan fitur pelaporan nomor, sehingga jika warga menerima panggilan phising, mereka bisa melaporkannya sehingga nomor tersebut dapat ditandai dan diblokir secara lebih luas. Untuk memastikan bahwa masyarakat faham dan mampu menggunakan aplikasi ini secara maksimal, perlu diselenggarakan pelatihan khusus yang membahas cara instalasi, pengaturan, serta pemanfaatan fitur-fitur keamanan dalam Truecaller. Dalam pelatihan tersebut juga harus dijelaskan bagaimana aplikasi ini dapat membantu menjaga data pribadi pengguna agar tidak mudah diketahui oleh pihak tak bertanggung jawab, sehingga memberikan rasa aman lebih dalam menjalani aktivitas digital.

3. Peningkatan Literasi Digital

Kesadaran masyarakat juga harus didukung dengan peningkatan literasi digital yang baik dan benar. Literasi digital bukan hanya tentang kemampuan menggunakan perangkat teknologi, tetapi juga mencakup pengetahuan tentang bagaimana mengamankan informasi pribadi, cara membuat kata sandi yang kuat dan sulit ditebak, serta bagaimana mengenali situs web atau tautan yang mencurigakan di internet. Melalui pelatihan yang mengandung simulasi kasus phising, masyarakat dapat belajar langsung bagaimana merespons jika mereka menerima email, pesan, atau telepon yang mencurigakan. Simulasi ini penting untuk memberi gambaran nyata atas ancaman yang bisa terjadi sehingga warga tidak hanya memahami teori tetapi juga mampu bertindak secara bijak saat menghadapi situasi tersebut. Perlu juga diberikan tips praktis seperti selalu melakukan verifikasi informasi dengan sumber resmi sebelum menanggapi pesan yang meminta data pribadi atau melakukan transfer uang. Secara konsisten, kebiasaan ini akan membangun pola pikir kritis yang dapat melindungi masyarakat dari penipuan digital.

4. Kolaborasi dengan Lembaga Terkait

Peningkatan kesadaran anti-phising bukan hanya tanggung jawab individu atau pemerintahan kelurahan saja, melainkan juga membutuhkan kolaborasi yang erat dengan berbagai lembaga terkait. Kepolisian dapat turun tangan untuk memberikan penyuluhan dan proses penindakan terhadap pelaku phising yang meresahkan. Dinas

komunikasi dan informatika dapat menyediakan materi edukasi serta dukungan teknis dalam pelaksanaan kampanye literasi digital. Operator telekomunikasi juga penting untuk diajak bekerjasama dalam memblokir nomor-nomor yang sudah terbukti melakukan spam dan penipuan. Selain itu, pembentukan tim relawan digital di tingkat kelurahan yang terdiri dari warga yang paham teknologi bisa menjadi perpanjangan tangan pemerintah dalam mendampingi dan membantu masyarakat mengatasi ancaman phising. Relawan ini juga bisa menjadi penghubung yang cepat dalam melaporkan kasus-kasus phising ke instansi berwenang serta menjadi pusat informasi anti-phising di tengah komunitas.

5. Penguatan Sistem Pelaporan

Agar masyarakat merasa didukung dan kasus phising segera tertangani, perlu dibangun sistem pelaporan yang efektif dan mudah diakses. Saluran pelaporan harus bisa diakses secara online, misalnya melalui aplikasi atau website resmi, dan secara offline, seperti melalui posko pengaduan di kantor kelurahan atau posko layanan masyarakat. Prosedur pelaporan harus dibuat sesederhana mungkin agar semua lapisan masyarakat dapat dengan mudah melaporkan jika mengalami atau mengetahui upaya phising. Informasi tentang keberadaan dan cara penggunaan saluran pelaporan ini juga harus disebarluaskan melalui berbagai media. Dengan demikian, data dari laporan masyarakat dapat menjadi salah satu sumber utama bagi penegak hukum dan instansi terkait dalam memantau dan menindak pelaku phising secara cepat dan tepat.

6. Kampanye Berkelanjutan

Kesadaran terhadap phising perlu terus ditingkatkan melalui kampanye yang dilakukan secara berkelanjutan. Kampanye ini dapat dilakukan di berbagai platform, mulai dari media sosial yang banyak digunakan masyarakat, grup WhatsApp warga, radio komunitas, hingga papan pengumuman yang mudah dijangkau oleh seluruh warga kelurahan. Informasi yang diangkat dalam kampanye harus variatif namun tetap fokus pada edukasi anti-phising, seperti cara mengenali ciri panggilan dan pesan phising, serta manfaat menggunakan aplikasi keamanan seperti Truecaller. Untuk meningkatkan daya tarik dan motivasi masyarakat, dapat juga diselenggarakan lomba atau kuis yang berhubungan dengan pengetahuan literasi digital dan anti-phising dengan hadiah menarik. Bentuk kegiatan ini dapat mempromosikan interaksi positif dan mendorong masyarakat tidak hanya menjadi penerima informasi, tetapi juga aktif ikut serta dalam membangun komunitas digital yang aman.

3.2 Pemanfaatan Truecaller sebagai Alat Verifikasi

3.2.1 Truecaller

Truecaller adalah sebuah perusahaan teknologi yang berasal dari Swedia, didirikan pada tahun 2009 di kota Stockholm oleh dua tokoh muda, Nami Zarringhalam dan Alan Mamedi. Pada awalnya, aplikasi ini tercipta saat kedua pendirinya masih menjalani kehidupan sebagai mahasiswa. Mereka memiliki keinginan untuk menghadirkan solusi

digital yang bisa membantu banyak orang dalam mengidentifikasi panggilan masuk dari nomor yang tidak dikenal, sesuatu yang kala itu masih menjadi tantangan besar bagi banyak pengguna telepon seluler. Dari ide inilah, Truecaller mulai dikembangkan sebagai jawaban atas kebutuhan masyarakat akan keamanan dan kenyamanan berkomunikasi.

Seiring berjalannya waktu, Truecaller mengalami pertumbuhan pesat dan mendapat sambutan hangat di berbagai negara. Saat ini, aplikasi ini telah digunakan dan sangat disukai oleh lebih dari 450 juta pengguna aktif setiap bulan di seluruh penjuru dunia. Kepopuleran aplikasi ini tidak lepas dari kemampuannya sebagai solusi terbaik untuk mengenali identitas penelepon dan secara efektif memblokir panggilan serta pesan spam yang sering mengganggu. Dengan fitur-fitur canggih yang terus dikembangkan, Truecaller kini telah menjadi aplikasi andalan banyak orang untuk melindungi diri dari panggilan yang tidak diinginkan, memperkuat privasi, dan memberikan pengalaman komunikasi yang lebih aman serta nyaman bagi penggunanya. Berdasarkan web resmi Truecaller, fitur-fitur yang terdapat dalam Truecaller antara lain terdiri dari sebagai berikut :

1. ID Penelepon

Fitur ID Penelepon memungkinkan Anda untuk mengenali nomor yang tidak dikenal, nomor spam, atau bahkan nomor dari perusahaan sebelum Anda memutuskan untuk mengangkat telepon tersebut. Dengan teknologi

canggih yang dimiliki, Anda dapat melihat identitas asli dari setiap panggilan yang masuk, tidak terbatas oleh wilayah geografis, baik itu nomor telepon rumah, kantor, ponsel pribadi, maupun nomor prabayar sekalipun. Truecaller sebagai aplikasi ID Penelepon dapat mengenali dan mengidentifikasi semua jenis nomor, baik yang berasal dari dalam negeri maupun dari luar negeri. Dengan adanya fitur ini, Anda tidak perlu merasa cemas atau panik ketika menerima panggilan dari nomor yang belum dikenal. Sistem akan secara otomatis menampilkan informasi penting seperti nama pemilik nomor, lokasi mereka berada, serta apakah nomor tersebut terdeteksi sebagai spam atau bukan. Dengan begitu, Anda bisa mengambil keputusan yang lebih tepat dan aman dalam menjawab panggilan yang masuk, sekaligus menghindari gangguan dari telepon yang tidak diinginkan secara efektif.

Gambar 2. Fitur ID Penelepon
(*Sumber: https://www.truecaller.com/id-id*)

2. Pemblokir Spam

Truecaller menyediakan fitur blokir nomor dan blokir otomatis untuk telemarketer serta panggilan robot yang mengganggu, sehingga pengguna dapat terhindar dari panggilan tidak diinginkan dengan lebih mudah dan efektif. Fitur ini bekerja bersama komunitas pengguna global yang aktif melaporkan nomor spam secara real-time, memastikan perlindungan yang terus diperbarui bagi seluruh pengguna di seluruh dunia. Dengan Truecaller, memblokir panggilan spam menjadi sangat praktis karena aplikasi ini secara otomatis mengidentifikasi dan menyaring berbagai jenis panggilan yang berpotensi mengganggu, seperti panggilan dari robot, telemarketer, penipu, pelaku scam, dan pengganggu lainnya. Aplikasi ini berjalan secara terus-menerus di latar belakang perangkat Android Anda, memantau semua SMS dan panggilan masuk. Saat ada nomor yang terdeteksi sebagai spam berdasarkan data komunitas dan algoritma kecerdasan buatan, panggilan tersebut langsung dikenali dan dapat diblokir tanpa harus melakukan pemblokiran manual satu per satu.

Gambar 3. Fitur Pemblokir Spam
(*Sumber: https://www.truecaller.com/id-id*)

3. Perpesanan

Truecaller menghadirkan fitur perpesanan lengkap yang memungkinkan Anda untuk mengelola semua komunikasi tanpa perlu beralih ke aplikasi lain. Dengan Truecaller sebagai aplikasi SMS utama, Anda tidak hanya bisa mengirim dan menerima pesan teks biasa, tetapi juga melakukan chat menggunakan data internet, sehingga dapat menghindari biaya pengiriman SMS tradisional. Aplikasi ini dilengkapi dengan kemampuan untuk mengidentifikasi pesan spam secara otomatis, sehingga pesan tidak penting atau berbahaya dapat difilter dan tidak mengganggu kotak masuk utama Anda. SMS dan chat yang Anda terima akan dikelompokkan dalam kategori yang jelas seperti Pribadi, Penting, Bisnis, dan Spam, sehingga Anda lebih mudah memantau pesan yang benar-benar membutuhkan perhatian. Selain itu, Truecaller memungkinkan Anda untuk menjadwalkan pengiriman pesan mendatang, memberikan fleksibilitas dalam mengatur komunikasi Anda.

Gambar 4. Fitur Perpesanan
(*Sumber: https://www.truecaller.com/id-id*)

4. Pencarian Nomor Cepat

Pencarian Nomor Cepat adalah fitur praktis yang dirancang untuk menghemat waktu Anda dengan memungkinkan pencarian informasi nomor telepon secara langsung tanpa harus membuka aplikasi Truecaller secara penuh. Dengan fitur ini, Anda dapat dengan mudah mengetahui identitas pemilik nomor telepon dalam waktu singkat hanya melalui fungsi pencarian yang c

epat dan efisien. Misalnya, ketika Anda mendapatkan nomor telepon yang belum dikenal dari pesan, panggilan masuk, atau sumber lain, Anda cukup mengetikkan atau menyalin nomor tersebut ke dalam fitur Pencarian Nomor Cepat. Dalam waktu sekejap, aplikasi akan menampilkan nama dan informasi terkait pemilik nomor tersebut, sehingga Anda bisa memutuskan apakah nomor tersebut layak dihubungi atau perlu diwaspadai sebagai spam atau penipuan.

Gambar 5. Fitur Pencarian Nomor Cepat
(*Sumber: https://www.truecaller.com/id-id*)

5. Tema Gelap

Truecaller menyediakan opsi untuk memilih tema terang atau tema gelap yang dapat diterapkan secara menyeluruh di semua layar aplikasi. Dengan fitur ini, pengguna memiliki kebebasan menyesuaikan tampilan aplikasi sesuai preferensi atau kondisi pencahayaan sekitar, sehingga kenyamanan visual dapat terjaga saat menggunakan Truecaller, baik dalam suasana terang maupun gelap. Tema gelap juga membantu mengurangi kelelahan mata terutama saat menggunakan aplikasi dalam kondisi cahaya rendah atau di malam hari, sekaligus dapat memperpanjang daya tahan baterai pada handphone.

Gambar 6. Fitur Tema Gelap
(*Sumber: https://www.truecaller.com/id-id*)

3.2.2 Instalasi dan Penggunaan *Truecaller*

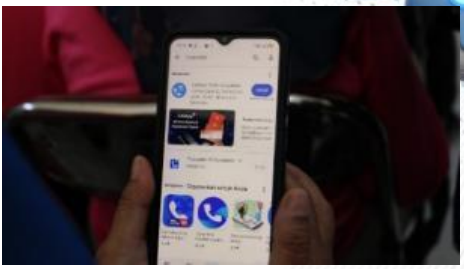
Fungsi utama aplikasi *truecaller* adalah untuk mengidentifikasi nomor telepon yang tidak dikenal serta memblokir panggilan spam. Dalam kegiatan ini, aplikasi tersebut diperkenalkan kepada masyarakat sebagai langkah preventif terhadap modus penipuan digital yang marak terjadi melalui sambungan telepon. Para warga diajarkan mulai dari instalasi hingga penggunaan aplikasi truecaller, yakni sebagai berikut :

1. Unduh Aplikasi Truecaller

Gambar 7. Simbol Play Store dan App Store (*Sumber:Google*)

Aplikasi Truecaller telah tersedia dan dapat diunduh secara legal serta gratis melalui *Google Play Store* (bagi pengguna Android) atau *App Store* (bagi pengguna iOS).

Pada tahap ini para warga sangat antusias untuk ikut men-download aplikasi Truecaller seperti pada gambar berikut.



Gambar 8. Dokumentasi Partisipasi Warga
(*Sumber: Dokumentasi Pribadi*)

2. Registrasi dan Perizinan Akses

Setelah terinstall, buka aplikasi klik mulai dan izinkan segala akses yang dibutuhkan. Kemudian pengguna akan ditampilkan sebagai berikut.

Gambar 9. Warga Registrasi Truecaller
(*Sumber: Dokumentasi Pribadi*)

Pilih akun google yang digunakan.

Gambar 10. Warga Registrasi Truecaller
(*Sumber: Dokumentasi Pribadi*)

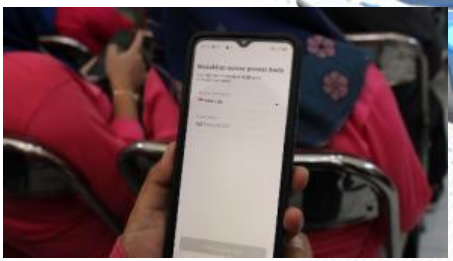
Klik lanjutkan sebagai "..."

Setelah berhasil masuk, kemudian izinkan akses pada "telepon" agar dapat registrasi dengan nomor telepon sebagai berikut.

3. Verifikasi Nomor

Setelah registrasi dengan akun google pengguna akan diarahkan pada halaman verifikasi nomor. Gunakan nomor telepon yang aktif, agar mendapatkan kode OTP. Setelah berhasil registrasi, tahap selanjutnya adalah perizinan semua akses yang diminta yaitu pada kontak, Log Panggilan, dan SMS dengan meng-klik "Izinkan". Hal ini tentu diperlukan jika ingin mengidentifikasi panggilan tidak dikenal yang masuk.

Biasanya aplikasi akan mengarahkan pengguna untuk melakukan verifikasi melalui akun *WhatsApp*. Tahap ini pengguna dapat memasukkan nomor *WhatsApp* pengguna dan tekan verifikasi nomor saya.

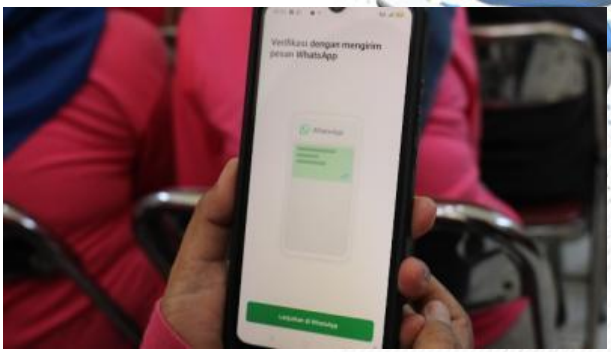


Gambar 11. Dokumentasi Partisipasi Warga
(*Sumber: Dokumentasi Pribadi*)

Setelah itu pengguna akan diarahkan ke halaman ini. Ketik ya jika nomor telepon sudah benar, dan edit jika terdapat kesalahan agar tidak terkendala pada saat verifikasi.

Gambar 12. Verifikasi Nomor
(*Sumber: Aplikasi Truecaller*)

Klik lanjutkan di *WhatsApp*.



Gambar 13. Verifikasi Nomor
(*Sumber: Dokumentasi Pribadi*)

Selanjutnya pengguna akan otomatis diarahkan ke *WhatsApp* dan ada pesan otomatis di papan pesan yang tinggal pengguna klik kirim.

Gambar 14. Verifikasi Nomor
(*Sumber: Dokumentasi Pribadi*)

Kemudian klik link biru untuk verifikasi, setelahnya akan dialihkan langsung ke aplikasi *Truecaller*.

Gambar 15. Verifikasi Nomor
(*Sumber: Dokumentasi Pribadi*)

Setelahnya dialihkan secra otomatis ke aplikasi *Truecaller* dan muncul laman berikut ini.

Gambar 16. Nomor Terverifikasi
(*Sumber: Aplikasi Truecaller*)

Dengan demikian Truecaller siap untuk digunakan.

4. Fungsi-Fungsi Utama Truecaller

Truecaller memiliki fitur-fitur dengan berbagai fungsi, yang mana telah dijelaskan pada bab sebelumnya. Diantaranya adalah sebagai berikut:

- Identifikasi nama/ID pemilik nomor tidak dikenal yang melakukan panggilan masuk.
- Blokir nomor-nomor yang telah dilaporkan sebagai spam oleh komunitas pengguna.
- Pencarian nomor telepon tertentu untuk mengetahui identitas pemiliknya.

5. Simulasi penggunaan

Selanjutnya, warga diajak mencoba secara langsung fitur-fitur utama *Truecaller* seperti yang telah disebutkan diatas, khususnya untuk mengenali dan menghindari panggilan mencurigakan.

Apabila kita mendapatkan telepon dari nomor tidak dikenal pengguna dapat mengecek nomor tersebut menggunakan fitur cari nomor pada aplikasi *Truecaller*.

Penggunaan Fitur Utama Aplikasi: Cari, Verifikasi Nomor dan Blokir

Setelah *Truecaller* siap digunakan pengguna akan disuguhkan halaman beranda aplikasi, apabila kita mendapatkan telepon dari nomor tidak dikenal pengguna dapat mengecek nomor tersebut menggunakan fitur cari nomor pada aplikasi *Truecaller*.

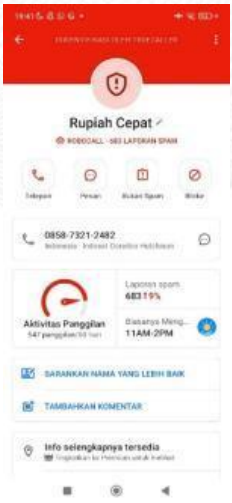
Gambar 17. Beranda Aplikasi Truecaller
(*Sumber: Aplikasi Truecaller*)

Apabila stelah mencari nomor, muncul id atau identitas normal yang pengguna kenal maka terverifikasi nomor tersebut aman. Contohnya pada gambar berikut ini.anan

Gambar 18. Halaman Informasi Nomor Aman
(*Sumber: Aplikasi Truecaller*)

Apabila setelah dicari nomor tersebut muncul halaman informasi id tidak normal atau bertanda seperti spam, penipu dan semacamnya. Contohnya seperti dibawah ini terverifikasi bahwa nomor tersebut berbahaya dan pengguna dapat memanfaatkan fitur blokir dihalaman tersebut agar nomor tersebut tidak menggangu dan menghindari adanya spam telepon.

Gambar 19. Halaman Informasi Nomor Berbahaya
(*Sumber: Aplikasi Truecaller*)



Gambar 20. Halaman Informasi Nomor Berbahaya
(Sumber: Aplikasi Truecaller)

ID penelpon dapat muncul otomatis tanpa perlu dicari melalui aplikasi apabila penelpon tidak dikenal tersebut melakukan aksi menelpon berulang-kali (spam). Jika hanya sekali ID penelpon tidak dapat muncul secara otomatis melainkan harus dicari secara manual melalui fitur cari nomor di aplikasi *Truecaller*.

3.3 Capaian Kegiatan

Pelaksanaan program kerja KKN dengan tema waspada digital ini diselenggarakan di Balai RW 7 Kelurahan Gunung Sari Kecamatan Dukuh Pakis Kota Surabaya. Dihadiri oleh Bu Siti Salmah, A.Md., selaku Ibu Lurah Kelurahan Gunung Sari beserta jajarannya (perwakilan), Bapak Muhammad Arif RW 7 Kelurahan Gunung Sari, Bu Erny selaku bendahara KSH dan Bu Nugraeni selaku koordinator KSH Kelurahan Gunung Sari sekaligus para peserta yaitu ibu-ibu KSH sejumlah 24 yang di mana beberapa diantaranya juga merupakan pemilik UMKM.

Edukasi phising ini sangat penting, oleh karena phising secara definisi merupakan salah satu ancaman digital yang mengandung unsur penipuan dengan menyebabkan kerugian dan mengancam keamanan data diri pribadi sehingga dapat dengan mudah disalahgunakan. Penyalahgunaan akibat phising ini tidak hanya merugikan secara materiil namun juga dapat merugikan secara immateriil yaitu terkait harkat martabat serta nama baik individu.

Pentingnya edukasi waspada digital yang terfokus pada ancaman phising ini oleh karena ancaman phising sering ditemukan dalam kehidupan sehari-hari. Banyak kasus ancaman digital yang telah terjadi dalam berbagai jenis dan yang paling sering ditemui adalah phising. Sebab itu upaya membangun pemahaman konsep dasar phising dan memiliki kemampuan deteksi awal untuk melindungi data diri pribadi, edukasi serta pelatihan anti-phising ini merupakan langkah yang penting dalam upaya preventif menuju pemberdayaan terhadap Warga RW 7 Kelurahan Gunung Sari terutama warga golongan UMKM yang rentan menjadi calon korban.

Program kerja waspada digital ini mengandung pemahaman secara konseptual sekaligus dpelatihan/praktek langsung dilapangan dalam upaya penyelesaian masalah yang ada terkait dengan perlindungan data diri pribadi. Dalam proses diarahkan partisipan untuk mengisi daftar hadir, kemudian pembukaan dan sambutan, pemaparan materi dilakukan tanya jawab dengan warga memberikan kesempatan kepada warga untuk bertanya berdasar pengalaman pribadi maupun seputar pemahaman materi. Didapat bahwa Warga Kelurahan Gunung Sari tepatnya RW 7 aktif menggunakan smartphone (khususnya para UMKM menjadi salah satu kelompok yang rawan), namun belum banyak yang mengetahui dan memahami ancaman kejahatan digital (siber) yang mengancam keamanan kehidupan mereka serta banyaknya warga yang menjadi target penipuan melalui media sosial seperti *WhatsApp* dan aplikasi yang memiliki fitur serupa lainnya akibat ketidaktahuan atau kurangnya informasi yang didapat karena minimnya literasi.

Antusiasme Warga RW 7 dalam pelaksanaan program ini sangat tinggi. Terlihat pada saat demo/pelatihan penggunaan aplikasi, banyak warga yang tertarik secara sukarela mendownload aplikasi dan meminta bantuan pengarahan kepada para mahasiswa yang sedang bertugas. Hampir seluruh peserta ikut dalam demo instalasi dan penggunaan aplikasi. Masyarakat sangat terkesan dan merasa terbantu saat mencoba aplikasi. Mendapati bahwa kegunaannya sangat bermanfaat di sisi lain dapat digunakan untuk memblokir nomor tidak dikenal yang dicurigai sebagai pelaku kejahatan digital seperti phising, sehingga pelaku tidak dapat menghubungi kembali dengan nomor yang sama.

Gambar 21. Pendampingan dan Pengarahan Aplikasi Truecaller
(*Sumber: Dokumentasi Pribadi)*

Berdasarkan gambar diatas didapati antusiasme tinggi warga pada sesi dilakukan pendampingan dan pengarahan aplikasi *Truecaller* sebagai aplikasi pendeteksi dasar adanya nomor tidak dikenal dan dicurigai. Mahasiswa secara berganti dan berkeliling membantu warga yang kesulitan atau dalam kata lain adalah mahasiswa hadir mendampingi warga yang

membutuhkan bantuan dalam pengaplikasian. Masyarakat sangat ramah dan terbuka pada arahan para mahasiswa, sehingga acara dapat berjalan lancar serta tujuan program ini terpenuhi. Dengan tercapainya ketertarikan masyarakat mendownload dan mempraktekkan aplikasi ini didapat bahwa masyarakat telah sadar dan memahami bahaya phising, konsep phising mulai dari definisi, jenis-jenis dan ciri khas, serta cara kerja phising sehingga masyarakat jadi lebih waspada melalui upaya pencegahan dengan memanfaatkan *Truecaller*.

Besar harapan kami para mahasiswa Kelompok 8 KKN Tematik SDGs UPN "Veteran" Jawa Timur dengan telah terlaksananya program kerja ini memberikan kenangan yang berkesan dan berharga kepada para partisipan yang hadir. Memberikan bekal bermakna kepada para peserta terkait pengetahuan pentingnya melindungi data diri pribadi, konsep phising, cara kerja, dan antisipasi dengan memanfaatkan aplikasi *Truecaller.* Dengan harapan lain partisipan dapat sekaligus menyebarkan info yang didapat kepada sanak keluarga maupun saudaranya sehingga langkah kecil ini menjadi berarti dan dapat berdampak lebih luas untuk keamanan tiap-tiap individu.

3.4 Kendala Kegiatan

Antusiasme warga RW 7 dalam mengikuti sosialisasi "Pencegahan Penipuan Online" di balai RW 7 sangatlah tinggi terutama pada saat sesi demo aplikasi truecaller yang menunjukkan bahwa warga sadar terhadap pentingnya waspada digital. Namun, dalam pelaksanaan kegiatan ini terdapat beberapa kendala yang perlu diperhatikan, antara lain sebagai berikut.

Tabel 2. Tabel Kendala dan Solusi

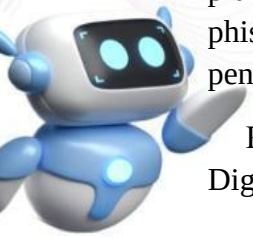
No.	Kendala	Solusi
1.	Beberapa peserta mengalami kendala teknis karena perangkat yang mereka gunakan tidak mendukung aplikasi truecaller dikarenakan versi Android atau iOS yang sudah usang sehingga Truecaller tidak dapat diunduh.	Aplikasi Truecaller memerlukan sistem operasi Android atau iOS dengan versi yang lebih baru. Untuk mengatasinya yaitu melakukan pembaruan perangkat ke versi yang lebih baru.
2.	Rendahnya literasi digital dan kesadaran keamanan	Sebagian warga kurang memahami konsep keamanan digital dan cara mengenali penipuan online sehingga rentan menjadi korban. Untuk mengatasinya, materi dalam powerpoint telah dirancang secara rinci mulai dari pengenalan apa itu phising, bagaimana phising bekerja, bagaimana cara membedakan link atau aplikasi yang termasuk phising atau bukan, dsb.
3.	Keterbatasan akses dan kecepatan internet	Tidak semua warga memiliki akses internet yang stabil atau cepat. Untuk mengatasinya, yaitu dengan memfasilitasi akses Wi-Fi di lokasi sosialisasi agar peserta bisa langsung mencoba aplikasi dengan koneksi yang memadai.
4.	Keterbatasan tempat yang menghambat jumlah peserta lebih banyak	Untuk mengatasinya yaitu dengan membagikan materi powerpoint kepada warga sehingga warga tetap mendapatkan informasi penting meskipun tidak hadir dalam kegiatan sosialisasi tersebut.

4. PENUTUP

4.1 Kesimpulan

Atas dasar program yang telah dilakukan diperoleh kesimpulan bahwa penting bagi tiap-tiap individu untuk dibekali pemahaman konsep dasar phising, cara kerja phising, dan pemanfaatan teknologi secara waspada namun tetap bijak. Program ini merupakan langkah preventif yang dapat diberikan oleh kami Kelompok 8 KKN SDGs. Diharapkan program dengan tema "Waspadai Digital" pada RW 7 Kelurahan Gunung Sari Kecamatan Dukuh Pakis ini terutama pada kelompok UMKM yang turut hadir memberikan *impact* nyata untuk kedepannya.

Didapat bahwa Warga Kelurahan Gunung Sari tepatnya RW 7 aktif menggunakan smartphone (khususnya para UMKM menjadi salah satu kelompok yang rawan), namun belum banyak yang mengetahui dan memahami ancaman kejahatan digital (siber) yang mengancam keamanan kehidupan mereka serta banyaknya warga yang menjadi target penipuan melalui media sosial seperti *WhatsApp* dan aplikasi yang memiliki fitur serupa lainnya akibat ketidaktahuan atau kurangnya informasi yang didapat karena minimnya literasi. Atas kendala tersebut, oleh sebab itu penulis berinisiatif mengadakan sosialisasi tidak hanya ilmu tapi juga meliputi praktik pengaplikasian aplikasi *Truecaller*, pengenalan phising, jenis dan ciri khas, cara kerja, pencegahan dan penanganan.



Pelaksanaan program kerja dengan tema "Waspadai Digital" yang memfokuskan pada phising ini mendapat

antusiasme yang tinggi oleh warga. Tidak sedikit warga menyatakan bahwa pernah mengalami hal yang sama sehingga mereka tertarik mendownload aplikasi *Truecaller* dan memanfaatkannya sebagai langkah pencegahan.

Pemberian pemahaman konsep dasar phising sekaligus pelatihan penggunaan aplikasi *Truecaller* ini pada Warga RW 7 Kelurahan Gunung Sari baik kelompok UMKM diharapkan dapat memiliki bekal yang cukup untuk melindungi dirinya beserta keluarganya secara mandiri. Hal ini menjadi solusi yang tepat atas segala kendala atau permasalahan yang dihadapi oleh warga. Didapati bahwa warga RW 7 sangat puas dengan program ini dan tingkat kesadaran anti-phising mereka meningkat oleh karena tidak sedikit dari mereka yang secara sukarela mendownload dan mencoba aplikasi ini.

4.2 Saran

Program kerja pengabdian ini berjalan cukup lancar walau terkendala oleh terbatasnya sumber daya yang ada sehingga hanya dapat mengundang sebagian warga Kelurahan Gunung Sari. Meski begitu, dengan telah diberinya pengetahuan phising ini alangkah baiknya para partisipan dapat membagikan ilmu yang diperoleh sehingga dapat memberikan dampak yang lebih luas. Tujuannya untuk saling menjaga dan memberdayakan warga Kelurahan Gunung Sari akan pentingnya sadar bahaya digital sehingga dapat lebih waspada dan berhati-hati dalam menggunakannya.

5. DAFTAR PUSTAKA

Jurnal

Cut Mutia, & Rayyan Firdaus. (2024). Analisis Penipuan Digital Teknik Phising Terhadap Layanan Mobile Banking. *Jurnal Transformasi Bisnis Digital*, *1*(4), 05–10. https://doi.org/10.61132/jutrabidi.v1i4.191

Dm, M. Y., Addermi, & Lim, J. (2022). Kejahatan Phising dalam Dunia Cyber Crime dan Sistem Hukum di Indonesia. *Jurnal Pendidikan Dan Konseling*, *4*(5), 8018–8023.

Gulo, A. S., Lasmadi, S., & Nawawi, K. (2021). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal of Criminal Law*, *1*(2), 68–81. https://doi.org/10.22437/pampas.v1i2.9574

Kelas 4a4, & Iskandar, O. (2024). Analisis Kejahatan Online Phising Pada Masyarakat. *Leuser : Jurnal Hukum Nusantara*, *1*(2), 32–36. https://journal.myrepublikcorp.com/index.php/leuser/article/view/85/75

Gulo, A. S., Lasmadi, S., & Nawawi, K. (2020). Cyber crime dalam bentuk phising berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. PAMPAS: Journal of Criminal Law, 1(2), 35–46. https://repository.unja.ac.id/18131/1/9574-Article%20Text-28027-1-10-20201010.pdf

Skripsi

Hanifah, L. (2023). Pengaturan tindak pidana cyber crime dalam bentuk cyber phising menurut hukum pidana Indonesia (Skripsi Sarjana, Universitas Islam Sultan Agung). Universitas Islam Sultan Agung Repository. https://repository.unissula.ac.id/30148/2/30301900202_fullpdf.pdf

Parlagutan, D., Ramadhani, S., Putri, E., Oktaviani, O., Khalisia, K. P., Husnul, L., & Khairiyyah. (2023). Penegakan hukum terhadap tindak pidana phising ditinjau berdasarkan hukum yang berlaku di Indonesia. Universitas Pembangunan Nasional Veteran Jakarta. https://www.researchgate.net/publication/375922453_Penegakan_Hukum_Terhadap_Tindak_Pidana_Phising_Ditinjau_Berdasarkan_Hukum_yang_Berlaku_di_Indonesia

Benyamin, B. (2024). Analisis yuridis tindak pidana cyber crime phising dalam ketentuan hukum positif Indonesia (Skripsi Sarjana, Universitas Hasanuddin). Universitas Hasanuddin Repository. https://repository.unhas.ac.id/id/eprint/33696/2/B011171585_skripsi_01-04-2024%201-2.pdf

Website

Truecaller, diakses pada 21 Juli 2025, dari https://www.truecaller.com/id-id

6. LAMPIRAN

Lampiran 1. Surat Kesediaan Kerjasama Mitra

PEMERINTAH KOTA SURABAYA
KECAMATAN DUKUH PAKIS
KELURAHAN GUNUNG SARI
Jalan Kencana Sari Timur No. 101 Surabaya 60224
Telepon (031) 5617694
Laman surabaya.go.id, Pos-el: kel_gunungsari@surabaya.go.id

SURAT KETERANGAN
NOMOR 000 /577/436.9.5.3/2025

Yang bertandatangan di bawah ini :

a. Nama : SITI SALMAH A.Md
b. Jabatan : Lurah Gunung Sari

Dengan ini menerangkan bahwa :

a. Nama/(NIP/NIK) : Fitria Rahmatul Laili / 22042010218
b. Pangkat/Golongan : Ketua Kelompok KKNT MBKM
c. Umur : 22 Tahun
d. Kebangsaan : Indonesia
e. Pekerjaan : Mahasiswa Jurusan Administasi Bisnis, Fakultas Ilmu Sosial, Budaya dan Ilmu Politik Universitas Pembangunan Nasional Veteran Jawa Timur
f. alamat : Wonokromo SS Baru 6/11B, Surabaya

Maksud : Dengan ini menyatakan bersedia untuk bekerjasama dalam pelaksanaan Kegiatan Kuliah Kerja Nyata Tematik Merdeka Belajar Kampus (KKNT MBKM) Tahun 2025 dari Universitas Pembangunan Nasional Veteran Jawa Timur dengan Judul program **"Pemberdayaan UMKM Inklusif dan Berkelanjutan Melalui Digitalisasi dan Inovasi Produk di Kelurahan Gunung Sari"**

Bersama ini pula kami menyatakan dengan sebenarnya bahwa di antara Pimpinan Mitra dan Ketua Kelompok KKNT MBKM tidak terdapat ikatan kekeluargaan dan ikatan usaha dalam wujud apapun.

Demikian Surat Keterangan ini dibuat untuk dipergunakan seperlunya.

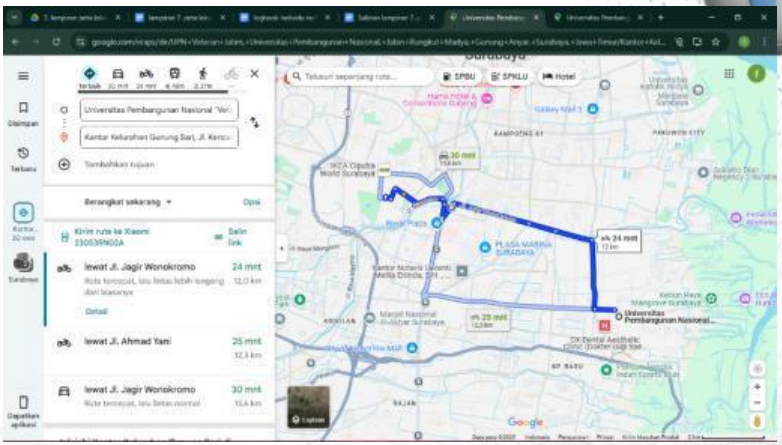
Surabaya, 26 Juli 2025

Surat ini Ditandatangani Elektronik Oleh :
a.n. CAMAT
LURAH,

SITI SALMAH A.Md
Penata / III/c
NIP. 197908211998092001

Tembusan:
Yth. 1. Camat Dukuh Pakis

Lampiran 2. Peta Lokasi Kegiatan



Gambar Peta Lokasi Kegiatan di Kelurahan Gunungsari, Kecamatan Dukuh Pakis, Kota Surabaya berjarak 12 km dari UPN "Veteran" Jawa Timur

Lampiran 3. Dokumentasi Kegiatan

Lampiran 4. Slide Materi

Manakah?

https://www.tokopedia.com/ncoshop/keycaps-blank-xda-1u-mechanical-keyboard-hitam-fcbd7

1. Website Asli Memakai HTTPS
2. Tidak Ada Salah Kata
3. Belakang url jelas tidak angka dan huruf acak

http://www.tok0pedia.coms/unknownshop/keycaps/a908af+aaa0ihAsdgsas8243sad24!

Manakah?

Manakah email yang bukan Phishing ?

halobca@bca.co.id

VS

bcacustomerservice@gmail.com

Manakah?

Manakah email yang bukan Phishing ?

halobca@bca.co.id ✓

bcacustomerservice@gmail.com ✗

Voice Phising

Voice Phishing

- Anak Kecelakaan
- Pihak Bank
- Pihak Berwenang
- Investasi / Hadiah
- DLL

SMS PHISING

SMS Phishing pada kode OTP (One-Time Password)

APK PHISING

Malware Phishing pada surat undangan digital berbentuk apk (aplikasi)

APK PHISING

Manakah Aplikasi Yang aman dan bukan Phishing ?

VS

Manakah?

Dua-duanya merupakan aplikasi phishing

Gimana Cara Membedakan Aplikasi Phishing?

Sumber terpercaya :

Play Store

APP Store

Penanganan Phising

01 Jangan Panik

02 Cari Informasi/validasi

03 Hapus Aplikasi Virus

04 Ganti Semua Password/pin

05 Lapor Pihak Berwajib

Truecaller

Mencari Identitas Nomor Telepon Melalui Aplikasi

Kita dapat mencari identitas dari nomor telepon menggunakan bantuan aplikasi seperti Truecaller.

"Bisa di Download melalaui Play Store".

TRUECALLER

Terima Kasih