BAB III
METODE PENELITIAN

3.1 Jenis dan Metode Penelitian

3.1.1 Jenis Penelitian

Penelitian ini dilakukan dengan menggunakan pendekatan deskriptif kuantitatif. Pendekatan kuantitatif melibatkan penggunaan data numerik yang dianalisis secara statistik sehingga dapat menjawab pertanyaan penelitian tertentu yang telah ditulis. Data numerik ini biasanya diperoleh melalui teknik pengukuran yang objektif, seperti survei, kuesioner, atau eksperimen. Pendekatan deskriptif, di sisi lain, bertujuan untuk memberikan sebuah gambaran atau deskripsi yang hasilnya sistematis dan akurat mengenai fenomena yang sedang diteliti. Dalam konteks penelitian ini, pendekatan deskriptif kuantitatif digunakan untuk mengeksplorasi dan menggambarkan kesadaran pengguna WhatsApp terhadap ancaman phishing file APK dengan menggunakan data kuantitatif yang diperoleh dari survei. Pendekatan ini memungkinkan peneliti untuk memahami sejauh mana fenomena phishing ini mempengaruhi pengguna dan untuk mengidentifikasi atau menemukan pola-pola hingga tren yang mungkin ada dalam data yang dikumpulkan (Waruwu, 2023).

3.1.2 Metode Penelitian

Metode penelitian yang digunakan dalam penelitian kuantitatif ini merupakan metode survei. Metode survei adalah salah satu metode penelitian yang umum digunakan dalam penelitian kuantitatif, di mana data dikumpulkan dari sampel yang representatif melalui kuesioner atau wawancara terstruktur. Tujuan utama dari metode survei adalah untuk mengumpulkan informasi tentang variabel-variabel yang relevan dengan penelitian dan untuk menjelaskan hubungan antara variabel-variabel tersebut. Dalam penelitian ini, metode survei akan digunakan untuk mengganbungkan data mengenai tingkat kesadaran dan pemahaman pengguna WhatsApp terhadap praktik phishing file APK. Data yang diperoleh melalui survei ini akan dianalisis secara statistik untuk mengidentifikasi faktor-faktor yang mempengaruhi kesadaran pengguna serta untuk mengevaluasi sejauh mana pengguna mampu mengenali dan menghindari ancaman phishing (Sari, Rachman, Astuti, Afgani, & Siroj, 2023).

3.2 Populasi

Populasi yang diteliti dalam penelitian ini merujuk pada keseluruhan elemen atau individu yang menjadi objek penelitian, dan dari mana sampel akan diambil oleh peneliti. mahasiswa Ilmu Komunikasi Universitas Muhammadiyah Malang Angkatan 2020 menjadi populasi yang akan diteliti. Berdasarkan website di komunikasi.umm.ac.id, mahasiswa dengan program studi Ilmu Komunikasi Universitas Muhammadiyah Malang angkatan 2020 ada sebanyak 604 mahasiswa. Dari 604 mahasiswa tersebut, terpilih melalui pre-survey dan mendapatkan hasil 113 mahasiswa yang memiliki krtiteria sebagai pengguna Whatsapp, mengetahui phishing, dan pernah mendapatkan pesan phishing file APK.

Mahasiswa yang merupakan pengguna aktif media sosial maupun aplikasi berbasis komunikasi pesan instan seperti WhatsApp menjadi asumsi pada pemilihan populasi yang digunakan di penelitian ini. Responden nantinya memiliki potensi untuk mengalami atau menyadari adanya ancaman phishing file APK. Berdasarkan survei awal yang dilakukan, diketahui bahwa sebagian mahasiswa Ilmu Komunikasi Universitas Muhammadiyah Malang Angkatan 2020 pernah menjadi korban atau setidaknya menerima pesan phishing yang menyertakan file APK berbahaya. Oleh karena itu, populasi ini dianggap relevan dan penting untuk diteliti lebih lanjut guna memahami kesadaran mereka terhadap ancaman phishing dan untuk memberikan rekomendasi edukasi atau intervensi yang dapat membantu mencegah serangan serupa di masa depan.

3.3 Sampel

Sampel merupakan bagian dari populasi yang dipilah atau diseleksi untuk dijadikan subjek penelitian dengan tujuan agar dapat mewakili karakteristik dan variasi yang ada dalam populasi tersebut. Subjek penelitian dipilih berdasarkan kriteria yang telah ditentukan dengan maksut dan tujuan agar relevan dengan teknik yang digunakan, yaitu teknik purposive sampling. Kualifikasi atau kriteria yang digunakan untuk menetapkan pada sampel dalam penelitian ini adalah mahasiswa yang sudah familiar dengan penggunaan aplikasi WhatsApp, mengetahui tentang ancaman phishing, dan pernah menerima pesan phishing yang berisi file APK. Pemilihan sampel yang spesifik ini bertujuan untuk memastikan bahwa data yang diperoleh relevan dan dapat digunakan untuk menggambarkan tingkat kesadaran dan pemahaman mahasiswa terhadap praktik phishing file APK.

Menggunakan teknik purposive sampling untuk penelitian ini, sehingga rumus yang digunakan ialah rumus slovin yang dijabarkan sebagai berikut:

$$n = \frac{N}{1 + N\ (e)^2}$$

Keterangan:

n = Total sampel yang akan diteliti

N = Total populasi

d 2 = Presisi

Presisi yang ditetapkan adalah 10%, maka:

$$n = \frac{113}{1 + 113\ (0{,}1)^2}$$

$$n = \frac{113}{2{,}13}$$

$$n = 55$$

Dengan jumlah sampel sebanyak 55 orang, diharapkan hasil dari penelitian ini dapat memberikan deskripsi yang cukup representatif mengenai persepsi dan respons mahasiswa terhadap ancaman phishing di kalangan pengguna WhatsApp.

3.4 Pengumpulan Data

Peneliti menggunakan teknik pengumpulan data yang diterapkan dalam penelitian ini adalah survei berbasis kuesioner. Kuesioner disusun dalam bentuk Google Form dan akan disebarkan secara daring kepada 55 responden yang telah ditetapkan sebagai sampel. Kuesioner yang digunakan dirancang untuk mengukur berbagai aspek kesadaran dan pemahaman pengguna terhadap ancaman phishing, termasuk pengetahuan tentang tanda-tanda phishing, pengalaman menerima pesan phishing, dan tindakan yang diambil ketika menerima pesan mencurigakan.

Kuesioner terdiri dari beberapa bagian yang mencakup pertanyaan demografis (misalnya usia, jenis kelamin, dan tingkat penggunaan WhatsApp), serta pertanyaan khusus yang berfokus pada kesadaran dan pemahaman tentang phishing. Pertanyaan-pertanyaan ini disusun dalam format pilihan ganda dan skala Likert untuk memudahkan responden dalam menjawab dan untuk memudahkan peneliti dalam analisis data. Setiap pertanyaan dalam kuesioner ini dirancang sebagai indikator yang mengukur variabel-variabel yang telah ditentukan dalam penelitian.

Proses penyebaran kuesioner dilakukan secara daring untuk mempermudah akses dan partisipasi responden, mengingat responden adalah mahasiswa yang sering menggunakan perangkat digital. Setelah kuesioner disebarkan, data yang telah terkumpul akan diolah dan juga dianalisis dengan menggunakan metode statistik yang sesuai, guna menarik kesimpulan mengenai tingkat kesadaran dan respons mahasiswa terhadap praktik phishing file APK di WhatsApp.

3.5 Analisis Data

Analisis deskriptif kuantitatif menjadi pilihan peneliti dalam menentukan teknik analisis. Penelitian deskriptif kuantitatif bertujuan guna mengetahui nilai suatu variabel bebas yang terdiri dari paling sedikit satu variabel tanpa melakukan perbandingan atau mencari hubungan korelasi dengan variabel lain (Jayusman & Shavab, 2020).

Teknik anaslisis data deskriptif kuantitatif ini memiliki tahapan yang dimulai dengan mengumpulkan data melalui kuisioner yang disebarkan secara daring menggunakan Google Form. Kuisioner tersebut berisi pertanyaan-pertanyaan dalam bentuk skala penilaian (rating statement) untuk mengukur persepsi responden. Setelah data yang telah disebar terkumpul, maka peneliti dapat melakukan analisis menggunakan teknik statistik deskriptif. Statistik deskriptif diterapkan guna menganalisis dan mendeskripsikan data-data yang telah diperoleh, seperti menghitung frekuensi, persentase, rata-rata, dan deviasi standar, tanpa mengubah sumber asli dari data tersebut.

Penelitian ini akan menggunakan analisis data univariat yang bertujuan guna mendeskripsikan setiap variabel yang akan diukur dalam penelitian. Analisis univariat sendiri bertujuan untuk mendeskripsikan setiap variabel yang diukur dalam penelitian. Analisis univariat akan membantu dalam memahami pola umum yang muncul dalam data terkait

dengan kesadaran responden terhadap praktik phishing file .apk di WhatsApp. Analisis ini memungkinkan peneliti untuk mengidentifikasi distribusi frekuensi dari data, mengukur nilai tengah, serta melihat variasi yang ada dalam satu variabel tertentu, sehingga memberikan gambaran yang jelas mengenai kondisi kesadaran terhadap ancaman phishing di antara responden.

Penelitian ini menggunaka instrumen yang berupa kuesioner dengan skala likert yang telah ditentukan. Skala ini digunakan untuk mengukur sikap hingga perilaku responden terkait ancaman phishing apk di WhatsApp. Score setiap item pertanyaan sebagai berikut:

Jawaban Responden	Score
Sangat Tahu	5
Tahu	4
Cukup Tahu	3
Tidak Tahu	2
Sangat Tidak Tahu	1

Jawaban Responden	Score
Sangat Sering	5
Sering	4
Cukup Sering	3
Tidak Sering	2
Sangat Tidak Sering	1

Jawaban Responden	Score
Sangat Tidak Senang	5
Tidak Senang	4
Cukup Senang	3
Senang	2
Sangat Senang	1

Jawaban Responden	Score
Sangat Intens	5
Intens	4
Cukup Intens	3
Tidak Intens	2
Sangat Tidak Intens	1

Jawaban Responden	Score
Sangat Penting	5
Penting	4
Cukup Penting	3
Tidak Penting	2
Sangat Tidak Penting	1

Penggunaan skala likert dimaksudkan agar nantinya responden mudah memahami dan dengan jelas memahami pertanyaan-pertanyaan dan memberikan respon yang akurat sehingga data lebih konsisten ketika diuji.

3.6 Definisi Konseptual dan Operasional Variabel

3.6.1 Definisi Konseptual

Kesadaran Pengguna WhatsApp terhadap Praktik Phishing File .apk adalah tingkat pemahaman, pengetahuan, dan kewaspadaan yang dimiliki oleh pengguna aplikasi WhatsApp mengenai ancaman keamanan siber yang berupa file APK berbahaya. File APK (*Android Package Kit*) merupakan format file masa kini yang seringkali diaplikasikan untuk mendistribusikan dan memasang perangkat lunak pada sistem operasi Android. Phishing melalui file .apk mengacu pada praktik mengelabui pengguna untuk mengunduh dan menginstal aplikasi berbahaya yang bisa mencuri data pribadi, seperti informasi akun, kata sandi, atau data finansial (Smith, 2018).

3.6.2 Definisi Operasional

Kesadaran Pengguna WhatsApp terhadap Praktik Phishing File .apk dalam penelitian ini diukur berdasarkan beberapa indikator sebagaimana yang dijelaskan Jones (2019) yakni:

1. Pengetahuan

   Tingkat pengetahuan pengguna tentang apa itu phishing, cara kerja file .apk berbahaya, serta risiko yang ditimbulkan oleh file .apk yang mencurigakan.

2. Perilaku Pengguna

   Kewaspadaan dan tindakan pengguna dalam menghadapi potensi ancaman phishing, seperti mengenali tanda-tanda phishing, tidak sembarangan mengunduh file .apk, dan memeriksa sumber file sebelum menginstalnya.

3. Pengalaman

   Pengalaman pribadi pengguna terkait insiden atau percobaan phishing melalui file .apk, termasuk frekuensi dan dampak dari kejadian tersebut.

4. Sikap Pencegahan

   Sikap pengguna dalam mengambil langkah-langkah pencegahan seperti mengaktifkan fitur keamanan di WhatsApp, memperbarui perangkat lunak secara teratur, dan mengikuti informasi terbaru mengenai keamanan siber.