

BAB 3 METODE PENELITIAN

Dalam penelitian ini akan menganalisis tingkat *security awareness* terhadap ancaman *phishing* dari objek mahasiswa Fakultas Teknik dan Teknologi Informasi (FTTI). Penelitian dimulai dengan identifikasi masalah, memetakan proses, mengumpulkan data dan bahan penelitian, melakukan analisis, dan menyimpulkan seberapa tinggi tingkat kesadaran objek terhadap ancaman *phishing*. Untuk detailnya dapat dilihat pada Gambar 3.1.



Gambar 3.1 Alur Proses Penelitian

Adapun bahan, alat, dan jalanya proses penelitian ini dalam melakukan analisis tingkat kesadaran keamanan siber khususnya ancaman *phishing* dari objek mahasiswa FTTI.

3.1 BAHAN DAN ALAT PENELITIAN

Bahan penelitian ini terdiri dari 50 data mahasiswa FTTI Universitas Jenderal Achmad Yani Yogyakarta. Selain itu, peneliti juga memerlukan izin tertulis dari pihak kampus untuk penyebaran *phishing*. Alat yang digunakan dalam penelitian ini adalah komputer (PC) dan smartphone dengan spesifikasi yang cukup untuk menjalankan sistem operasi dan pengembangan perangkat lunak, konektivitas internet, dan kartu perdana. Sistem operasi dan program aplikasi yang digunakan untuk penelitian ini adalah:

Peneliti menggunakan:

1. Sistem Operasi: Windows 8 atau lebih tinggi atau Linux.

2. Google Formulir
3. Google Spreadsheet
4. Aplikasi pesan instan: WhatsApp Business
5. Perangkat lunak IBM SPSS Statistics v.22

Digunakan Responden:

1. Aplikasi pesan instan: WhatsApp
2. Google Form

3.2 JALAN PENELITIAN

Penelitian ini melewati beberapa tahap, termasuk dalam proses pembuatan *phishing*, berikut tahapan dalam penelitian ini:

1. Tahap Identifikasi. Tahap ini terdiri dari mengidentifikasi dan menganalisis:
 - b. Mengidentifikasi masalah yang muncul dan kebutuhan sumber daya.
 - c. Identifikasi objek yang digunakan dalam penelitian.
2. Tahap persiapan pengumpulan data. Beberapa langkah dilakukan pada tahap ini adalah sebagai berikut:
 - a. Mengajukan izin untuk menggunakan data mahasiswa kepada pihak akademik.
 - b. Pengumpulan data objek penelitian.
3. Tahap desain. Pada tahap ini merupakan tahap bagaimana membuat *phishing* dan database pengumpulan data.
4. Tahap pengujian, mengenai bagaimana *phishing* didistribusikan ke objek yang telah ditentukan untuk kemudian dilakukan analisis data yang diperoleh.
5. Pada tahap analisis data, data yang terkumpul dianalisis menggunakan metode MANOVA.
6. Tahap pembuatan laporan merupakan tahap akhir dari penelitian ini. Selain menulis dokumen sebagai laporan penelitian, peneliti juga akan meminta maaf kepada objek penelitian sebagai klarifikasi adanya pesan *phishing* yang disebar.

Di bawah ini adalah rincian tahapan dari analisis tingkat kesadaran keamanan siber terhadap ancaman *phishing* yang ditujukan untuk mahasiswa FTTI.

3.2.1 Studi Literatur

Tahap ini merupakan langkah pertama dalam melakukan identifikasi untuk mengaji dan mempelajari teori-teori yang mendukung penelitian ini. Studi literatur pada penelitian ini dari beberapa artikel, website, jurnal, paper, dan sumber lainnya yang terkait dengan penelitian ini. Semua sumber yang digunakan pada penelitian ini akan dicantumkan pada bagian referensi.

3.2.2 Persiapan Pengujian

Pada tahap persiapan dilakukan pembentukan skenario pengujian *phishing* terhadap 50 mahasiswa. Selain itu, dibentuk juga susunan kuisisioner yang akan disebarkan kepada objek mahasiswa untuk mengetahui apakah terdapat perbedaan yang signifikan dari masing-masing faktor pengaruh terhadap kesadaran keamanan siber objek. Untuk mengukur perbandingan seberapa besar pengaruh tiap faktor terhadap objek maka akan digunakan skala ranting. Dimana nantinya dari jawaban responden akan diubah menjadi *interval* angka dari 3 sampai dengan 1 menyesuaikan terhadap pilihan jawaban yang disediakan, dimana:

- Angka 3 bernilai berpengaruh positif
- Angka 2 bernilai berpengaruh positif
- Angka 1 bernilai berpengaruh negatif

3.2.3 Analisis dan pengujian

Pada tahapan ini dilakukan penyebaran *phishing* terhadap 50 mahasiswa FTTI Universitas Jenderal Achmad Yani dengan beberapa skenario yang disusun pada tahap sebelumnya. Pada tahapan ini dilakukan juga penyebaran kuisisioner setelah dilakukan *phishing test* kepada mahasiswa FTTI secara acak untuk mengetahui seberapa tingkat kesadaran keamanan siber. Metode analisis responden menggunakan metode MANOVA untuk mengetahui perbandingan tiap faktor yang mempengaruhi. Hasil perhitungan MANOVA terhadap analisis model

faktor TTAT berdasarkan data kuisisioner digunakan untuk menarik kesimpulan apakah terdapat faktor yang sangat mempengaruhi tingkat kesadaran keamanan siber bagi mahasiswa FTTH. Dimana H_0 akan diterima jika uji signifikansi menunjukkan sig. <0.05 . Sebelum dilakukan uji ini akan dilakukan uji normalitas distribusi sebagai syarat melakukan uji MANOVA. Analisis MANOVA akan dilakukan menggunakan *software* analisis IBM SPSS Statistics v.22.

3.2.4 Laporan

Laporan merupakan tahap terakhir dari metodologi pada penelitian ini. Pada tahap ini meliputi hasil akhir dari langkah-langkah sebelumnya yaitu identifikasi, persiapan analisis dan pengujian, tahap analisis dan pengujian, dan hasil dari analisis serta pengujiannya.

Perpustakaan
Universitas Jenderal Achmad Yani
Yogyakarta