Analisis Kesadaran Keamanan Terhadap Ancaman *Phishing*

Nunu Vadila
Program Studi Informatika – Program Sarjana
Universitas Islam Indonesia
Yogyakarta, Indonesia
nunu.vadila@students.uii.ac.id

Ahmad R. Pratama
Jurusan Informatika
Universitas Islam Indonesia
Yogyakarta, Indonesia
ahmad.rafie@uii.ac.id

***Abstract*—Teknologi berkembang maju dengan sangat pesat yangs semakin mempermudah penggunanya untuk melakukan pekerjaan. Namun, perkembangan ini juga memberikan tantangan baru dengan munculnya berbagai kejahatan berbasis siber yang memanfaatkan kelemahan sistem dan kesadaran pengguna informasi. *Phishing* merupakan salah satu bentuk kejahatan siber yang sering dijumpai. Penelitian ini bertujuan untuk melakukan penilaian terhadap tingkat kesadaran masyarakat terhadap ancaman *phishing*. Sebanyak 254 repsonden dengan berbagai latar belakang berbeda ikut berpartisipasi dalam penelitian ini. Analisis dilakukan dengan menggunakan metode ANOVA *(Analysis of Variance)* dengan bahasa pemrograman R, analisis yang berfokus pada aspek demografi jenis kelamin dan kelompok usia tertentu menemukan bahwa masyarakat Indonesia masih belum bisa mengenali ancaman *phishing* yang ada. Hasil dari penelitian ini diharapkan bisa dimanfaatkan untuk menjadi pembelajaran ke depannya sehingga bisa meningkatkan kesadaran terhadap ancaman *phishing*.**

Keywords—phishing, tingkat kesadaran, kejahatan siber

I. PENDAHULUAN

Perkembangan teknologi saat ini telah sangat meningkatkan efesiensi waktu dalam bekerja dan memungkinkan berbagai kegiatan dapat dilakukan dengan lebih cepat. Teknologi sangat membantu manusia dalam berbagai aktivitas. Namun, perkembangan ini menimbulkan tantangan baru dengan munculnya berbagai kejahatan berbasis siber yang berupaya memanfaatkan ketidakmampuan sistem dan kurang sadarnya pengguna sistem informasi.[1]

Phishing merupakan suatu bentuk kejahatan siber yang paling umum. Tindakan ini sangat merugikan dalam hal privasi, hingga bisa menyebabkan kerugian finansial jika informasi pribadi yang didapat disalahgunakan. Selain kerugian finansial phishing juga bisa menyebabkan masalah lain seperti kehilangan data pribadi, dan pencemaran nama baik [1].

Mengingat pentingnya kesadaran akan ancaman *phishing*, peneliti akan melakukan analisis terhadap kesadaran masyarakat pengguna internet Indonesia. Penelitian ini akan melihat dan mengukur tingkat kesadaran masyarakat Indonesia terhadap ancaman *phishing* yang ada di internet. Dalam penelitian ini akan membahas bagaimana kesadaran ancaman *phishing* pada pengguna internet di Indonesia, dan apakah ada perbedaan tingkat kesadaran ancaman *phishing* dengan info demografis berbeda. Selain itu diharapkan menjadi informasi terhadap tingkat kesadaran ancaman *phishing* pada masyarakat Indonesia.

II. KAJIAN PUSTAKA

Dalam menghadapi kejahatan siber, penting bagi setiap pengguna sistem informasi untuk menerapkan strategi keamanan informasi data. Ini dikarenakan jika suatu kejahatan siber sudah terlanjur terjadi maka itu sudah dianggap terlambat dan kerugian besar bisa saja sudah terjadi. Dalam suatu sistem, manusia adalah titik keamanan yang paling lemah dalam hal keamanan informasi. Suatu organisasi bisa memiliki sistem keamanan informasi yang terbaik, namun serangan dan kebocoran data masih berpotensi untuk terjadi dikarenakan keteledoran karyawan yang bekerja di organisasi tersebut [2].

Banyak hal yang perlu dilindungi oleh setiap orang terhadap informasi yang mereka miliki. Hal–hal yang termasuk dalam keamanan informasi adalah kerahasiaan informasi, integritas informasi, dan ketersediaan informasi ketika dibutuhkan. Selain itu, kesadaran keamanan informasi juga mencakup penggunaan program–program yang aman dan perilaku positif yang mengedepankan keamanan. Keduanya penting untuk menciptakan lingkungan keamanan informasi yang efektif [3].

Phishing adalah aktivitas kriminal yang menggunakan teknik rekayasa sosial. Pelaku *phishing* atau yang biasa dikenal dengan *phisher* berusaha untuk mendapatkan informasi pribadi, seperti nama pengguna, kata sandi, dan detail kartu kredit yang dapat digunakan untuk pencurian identitas [4]. Selama Q4 2020 *Anti-Phishing Working Group (APWG)* dalam laporannya, mencatat ada 637.302 situs palsu yang digunakan serta 396.668 subjek *email* yang baru dan unik sebagai sarana *phishing* [5].

Sebuah penelitian dilakukan oleh Button, dkk [1] mencoba mencari tahu mengapa banyak orang yang terjerat penipuan *online*. Pelaku berusaha untuk menipu korban dengan berpura–pura menjadi seseorang yang berasal dari suatu organisasi yang resmi. Cara yang digunakan oleh pelaku adalah dengan mengajak korbannya untuk membuka situs web yang sudah dibuat sebelumnya oleh pelaku. Korban membuka situs tersebut dengan membuka *link* dari *email* yang terlihat berasal dari organisasi yang resmi. *Email* tersebut biasanya berisi informasi palsu bahwa akun korban mengalami masalah dan korban harus memperbaikinya dengan membuka situs tersebut. Teknik ini disebut dengan "*Market Manipulation*".

Berdasarkan penelitian yang dilakukan oleh Rio, & Haris [6] diperoleh kesadaran akan keamanan masih sangat rendah, dibuktikan dengan masih banyaknya mahasiswa yang mengirimkan data pribadi mereka melalui website *e-learning* palsu. Mereka mengirimkan informasi pribadi mereka tanpa ragu seperti *email* dan nama pengguna *e-learning* mereka.

Berdasarkan penelitian yang dilakukan oleh Mukhlis [7] diperoleh kesadaran terhadap kesadaran informasi terlebih lagi tentang kerahasiaan *password* masih terlalu rendah. Narasumber masih kurang menyadari bahwa tindakan mereka bisa membocorkan *password*. Misalnya narasumber menulis kata sandi di kertas membantu mereka mengingat kata sandi, namun bisa saja hal ini membuat seseorang bisa mengetahui

kata sandi tersebut. Kemudian hubungan antar pegawai juga bisa membuat mereka percaya begitu saja sehingga memberikan *password* mereka dengan mudahnya.

Setelah dilakukan berbagai proses kajian pustaka, peneliti mengambil keputusan bahwa penelitian yang membahas dan mengukur tingkat kesadaran masyarakat Indonesia terutama mereka yang menggunakan internet terhadap ancaman *phishing* sangatlah penting.

III. METODE

A. *Pengambilan data*

Data yang digunakan dalam penelitian ini disebarluaskan melalui jejaring sosial seperti Telegram, Facebook, Line, & Instagram yang dibuat dengan bantuan Google Forms. Populasi penelitian ini merupakan pengguna internet di Indonesia, dan sampel yang didapat sebanyak 248 narasumber. Sampel yang didapat masih belum cukup untuk mewakili pemikiran seluruh masyarakat Indonesia. Isi kuesioner yang dibagikan adalah sebagai berikut:

1. Demografi

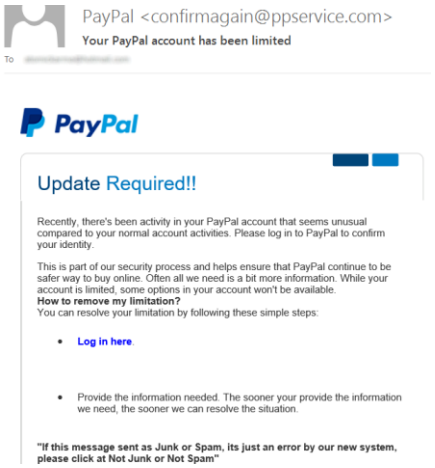
   Pada bagian ini, peneliti mengumpulkan informasi dan ingin mengetahui latar belakang narasumber. Informasi yang dikumpulkan meliputi usia (tahun), tempat tinggal (provinsi), dan latar belakang pendidikan. Informasi ini kemudian akan dianalisis apakah bisa menimbulkan perbedaan jawaban yang signifikan terhadap ancaman *phishing* yang akan diberikan.

2. Eksperimen Survei

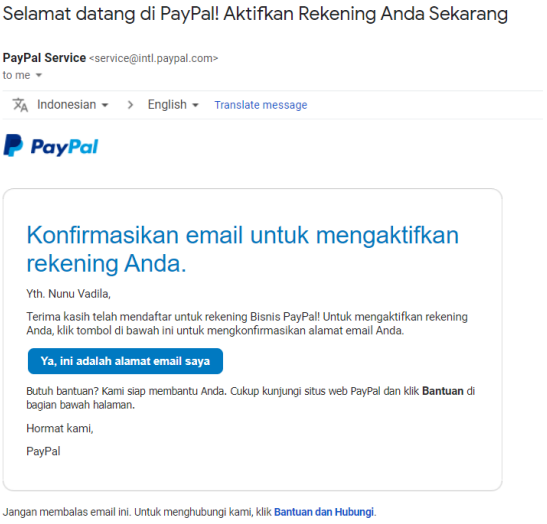
   Pada bagian ini peneliti membuat sebuah eksperimen terhadap survei yang diberikan kepada narasumber. Eksperimen yang dimaksud adalah dengan acak narasumber ada yang diberikan pembelajaran terlebih dahulu tentang adanya *phishing*, dan narasumber lainnya ada yang langsung diberikan soal tentang *phishing* tanpa adanya pembelajaran terlebih dahulu. Selain pemberian edukasi secara acak pada pertanyaan juga dilakukan pengacakan terhadap contoh ancaman *phishing* dan bukan, sehingga bisa mendapatkan hasil yang maksimal.

3. Ancaman *Phishing*

   Di bagian ini, peneliti mencoba mencari tahu apa tanggapan yang akan dilakukan oleh narasumber apabila menjumpai ancaman *phishing*. Untuk memenuhi hal tersebut maka peneliti menyajikan contoh Gambar 1 yang merupakan sebuah ancaman *phishing* dan Gambar 2 bukan ancaman *phishing* yang pernah ada di internet. Dengan contoh gambar tersebut, narasumber diminta untuk memberi tanggapan terhadap ancaman *phishing*. Melalui hasil jawaban yang diberikan oleh narasumber pada bagian ini kita akan mengukur bagaimana tingkat kesadaran mereka terhadap ancaman *phishing*.



Gambar 1. Ancaman *Phishing*



Gambar 2. Bukan Ancaman *Phishing*

Untuk setiap gambar yang diberikan ke narasumber, narasumber diberikan beberapa pilihan seperti yang tercantum dalam Tabel 1 untuk mengetahui pendapat dari narasumber ketika melihat contoh dari ancaman *phishing*.

TABEL 1. PENDAPAT TERHADAP CONTOH ANCAMAN *PHISHING*

No	***Jawaban***
1.	Valid
2.	*Phishing*
3.	Tidak Tahu

B. *Analisis Data*

Data yang sudah dikumpulkan melalui survei didapatkan 254 narasumber. Namun, sebelum dianalisis lebih lanjut, data tersebut melewati tahap *clean up* untuk menghilangkan data duplikat dan data yang tidak bisa dipakai. Setelah proses *clean up*, didapatkan 248 narasumber yang valid dan bisa dipakai.

Proses analisis peneliti lakukan menggunakan metode ANOVA (*Analysis of Variance*). ANOVA (*Analysis of Variance*) adalah metode analisis statistika yang bertujuan untuk mendapatkan nilai perbedaan rata–rata dalam sebuah kelompok atau grup [8]. Pada penelitian ini untuk menerapkan metode ANOVA (*Analysis of Variance*) maka akan memanfaatkan paket dari *library* yang berkaitan dengan ANOVA (*Analysis of Variance*) dan juga *library* yang sudah disediakan oleh bahasa pemrograman R. Pada penelitian ini, peneliti menggunakan model Three-Way ANOVA mengingat nilai AIC (*Akaike Information Criterion*) yang didapatkan lebih kecil dibandingkan dengan model ANOVA lainnya.

IV. HASIL DAN PEMBAHASAN

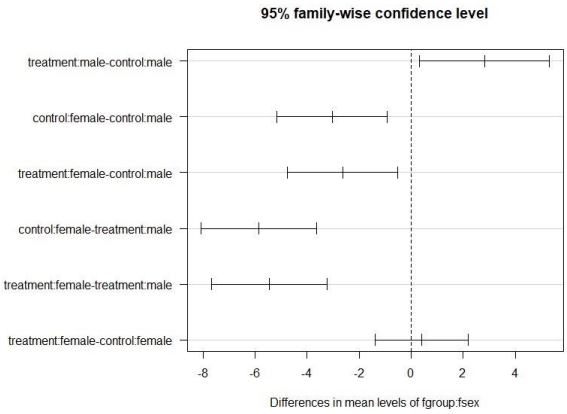
Berdasarkan hasil pengambilan yang dilakukan dengan menggunakan Google Forms, dikumpulkan 248 narasumber yang dikelompokan berdasarkan faktor demografi seperti jenis kelamin, usia, wilayah, dan pendidikan terakhir seperti yang tertera di dalam Tabel 2.

Berdasarkan jawaban responden yang tertera pada Tabel 2 di bawah, sebagian besar sampel yang diperoleh adalah perempuan. Berdasarkan usia, lebih dari dua pertiga narasumber berusia 20-an. Begitu juga dari segi wilayah asalnya, sebagian besar berasal dari provinsi Banten. Dalam hal pendidikan terakhir, lebih dari dua pertiga narasumber tengah menjalani jenjang perguruan tinggi atau telah lulus.

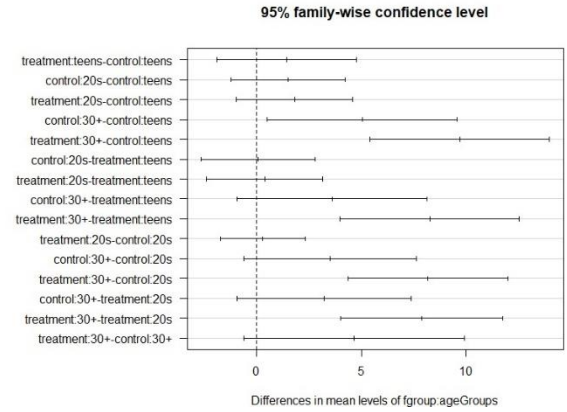
Kemudian, data dibersihkan dari duplikasi data dan permasalahan lain sehingga bisa digunakan dalam analisis dengan metode ANOVA untuk mengetahui nilai perbedaan rata–rata dari sebuah kelompok atau grup.

TABEL 2. TABEL DEMOGRAFI NARASUMBER

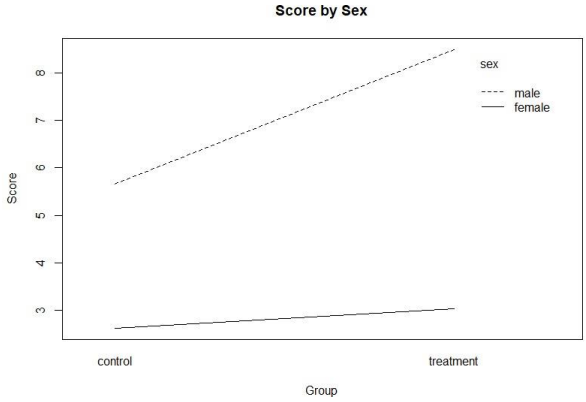
Variabel	*Jumlah*	*Persentase (%)*
Jenis Kelamin		
- Laki–Laki	84	33.87%
- Perempuan	164	66.13%
Usia		
- < 20 Tahun	60	24.20%
- 20-29 Tahun	164	66.13%
- ≥ 30 Tahun	24	9.67%
Asal Daerah Provinsi		
- Banten	163	65.72%
- Jawa Barat	17	6.85%
- Kalimantan Selatan	12	4.84%
- Jawa Tengah	11	4.44%
- Lainnya	45	18.14%
Pendidikan Terakhir		
- SD	5	2%
- SMP	15	6%
- SMA	69	27.9%
- Perguruan Tinggi	159	64.1%



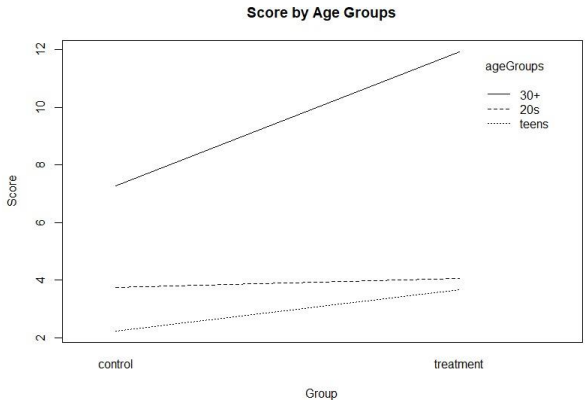
Gambar 3. Visualisi Perbedaan Rata–Rata Tingkat Kepercayaan Berdasarkan Jenis Kelamin



Gambar 4. Visualisi Perbedaan Rata–Rata Tingkat Kepercayaan Berdasarkan Kelompok Usia



Gambar 5. Visualisasi Score Berdasarkan Jenis Kelamin



Gambar 6. Visualisasi Score Berdasarkan Kelompok Usia

Hasil analisis yang didapatkan dari perhitungan secara otomatis dengan menggunakan ANOVA menampilkan hasil perbedaaan rata–rata tingkat kepercayaan berdasarkan jenis kelamin seperti gambaran pada Gambar 3 yang memberikan informasi bahwa narasumber berjenis kelamin laki–laki yang diberikan *treatment* atau pembelajaran tentang *phishing* bisa lebih baik mengenali ancaman *phishing* dibandingkan dengan narasumber berjenis kelamin perempuan yang juga diberikan pembelajaran terlebih dahulu.

Untuk hasil analisis tingkat perbedaan pada kelompok usia seperti gambaran pada Gambar 4 yang memberikan informasi kelompok usia remaja yang lebih dahulu diberikan *treatment* atau pembelajaran tentang *phishing* memberikan hasil yang tidak jauh berbeda, dengan yang belum mendapatkan pembelajaran. Akan tetapi, pada kelompok usia 20 tahun ke atas yang diberi pembelajaran dan tidak sama sekali tidak menunjukan perbedaan yang cukup signifikan. Lalu pada kelompok usia 30 tahun ke atas pembelajaran cukup membantu untuk mengenali ancaman *phishing* dibandingkan dengan yang tidak diberikan pembelajaran.

Untuk hasil berdasarkan jenis kelamin menghasilkan gambaran seperti pada Gambar 5 yang menghasilkan informasi berupa *score* dari hasil analisis data yang peneliti miliki. Hasil analisis terhadap informasi tersebut, yaitu narasumber berjenis kelamin perempuan lebih mengarah belum bisa menyadari tentang adanya ancaman *phishing*. Sedangkan narasumber berjenis kelamin laki–laki sudah sadar dengan adanya ancaman *phishing*.

Untuk hasil berdasarkan kelompok usia menghasilkan gambaran seperti pada Gambar 6 yang memberikan hasil penelitian berupa *score* dari hasil analisis data yang peneliti miliki. Maka terbentuklah hasil analisis, yaitu narasumber remaja atau yang berusia kurang dari 20 tahun masih belum menyadari adanya ancaman *phishing*. Begitu pula dengan kelompok usia 20 tahun ke atas masih belum bisa menyadari adanya ancaman *phishing*. Akan tetapi, pada kelompok usia 30 tahun ke atas narasumber sudah menyadari adanya ancaman *phishing*.

V. KESIMPULAN

Setelah menganalisis dan membahas mengenai kesadaran masyarakat pemakai internet di Indonesia tentang ancaman *phishing*, didapatkan kesimpulan yaitu masyarakat Indonesia secara garis besar masih belum mampu mengenali ancaman *phishing*. Peneliti juga menemukan bahwa faktor demografis yang paling signifikan adalah jenis kelamin. Narasumber yang berjenis kelamin perempuan memiliki tingkat kesadaran yang rendah terhadap ancaman *phishing*. Perlu tindakan lebih lanjut untuk bisa meningkatkan kesadaran terhadap ancaman *phishing* dan dibutuhkan kerjasama dari segala pihak untuk bisa melakukan edukasi terhadap bahaya *phishing*.

Penelitian ini memang masih belum bisa menggambarkan pemikiran setiap warga Indonesia. Peneliti mengharapkan untuk penelitian selanjutnya dengan tema yang sama, bisa menggunakan jumlah narasumber yang lebih banyak dan juga bisa menggunakan metode atau program lain sehingga dapat memberikan hasil yang lebih baik dan lebih akurat.

REFERENSI

[1] I. Radiansyah and Y. Priyadi, “Analisis Ancaman *Phishing* Dalam Layanan Online Banking,” vol. 7, no. 1, 2016.

[2] M. R. Akhyari and A. R. Pratama, “Kesadaran akan Ancaman Serangan Berbasis Backdoor di Kalangan Pengguna Smartphone Android,” *Automata*, vol. 2, no. 1, 2021, [Online]. Available: https://journal.uii.ac.id/AUTOMATA/article/viewFile/17317/10906.

[3] M. S. Alif and A. R. Pratama, “Analisis Kesadaran Keamanan di Kalangan Pengguna E-Wallet di Indonesia,” *Automata*, vol. 2, no. 1, 2021, [Online]. Available: https://journal.uii.ac.id/AUTOMATA/article/view/17279.

[4] N. P. Singh, “Online Frauds in Banks with *Phishing* Journal of Internet Banking and Commerce,” no. August 2007, 2017.

[5] APWG, “*Phishing* Activity Trends Report,” no. February, pp. 1–11, 2021.

[6] R. Wirawan, “Studi Kompetensi dan Kesadaran Pengguna E-Learning Terhadap Keamanan Sistem E-Learning Pada Pendidikan Tinggi,” *ETHOS (Jurnal Penelit. dan Pengabdian)*, vol. 7, no. 1, pp. 9–17, 2019, doi: 10.29313/ethos.v7i1.3850.

[7] M. Amin, “Information Security Awareness Level Measurement Using Multiple Criteria Decision Analysis (Mcda),” *J. Penelit. dan Pengemb. Komun. dan Inform.*, vol. 5, no. 1, p. 122371, 2014.

[8] D. Wahyudi and A. R. A. Djamaris, *Metode Statistik Untuk Ilmu dan Teknologi Pangan*. 2018.