BAB 1
PENDAHULUAN

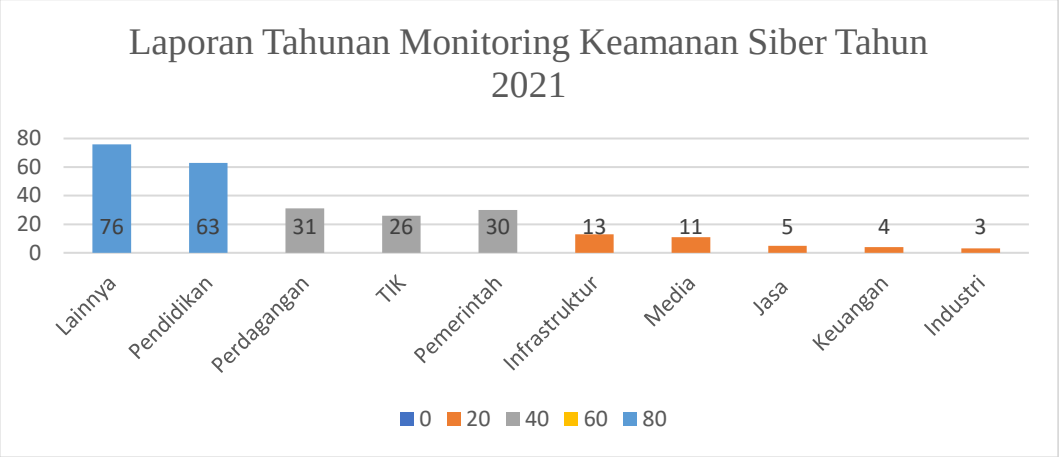
1.1. Latar Belakang

Perkembangan teknologi yang pesat dapat menimbulkan masalah, diantaranya kejahatan internet, *cybercrime* sebagai salah satu media yang digunakan untuk pencurian data oleh individu, organisasi dan pemerintah. *Cybercrime* melibatkan berbagai jenis aktivitas yang melanggar hukum, seperti melakukan akses yang tidak sah ke dalam sistem jaringan komputer tanpa izin, mengirimkan data dan informasi secara ilegal melalui internet menggunakan *malware*, serta mencuri nomor kartu kredit orang lain untuk digunakan dalam transaksi komersial di dunia maya (Mushlihudin & Nofiyan, 2020).

Jenis kejahatan yang sering terjadi adalah *phishing*. *Phishing* merupakan salah satu metode *cybercrime* yang mengiringi perkembangan teknologi digital. Kejahatan digital ini berupa pencurian informasi dan data pribadi melalui *email*, panggilan telepon, pesan teks, dan tautan yang meniru lembaga tertentu. Tantangan di era digital semakin bertambah salah satunya dengan serangan manipulatif ini. *Phishing* adalah jenis pelanggaran data yang telah ada sejak tahun 1990-an. Sampai hari ini, *phishing* tetap menjadi salah satu teknik serangan siber yang paling merusak. Apalagi dengan perkembangan teknologi dan metode eksekusi yang semakin canggih (Mushlihudin & Nofiyan, 2020).

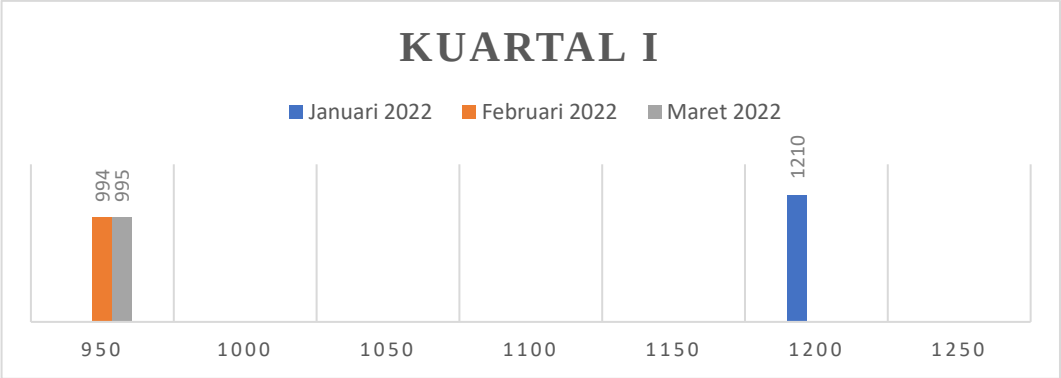
Berdasarkan Laporan Tahunan Monitoring Keamanan Siber pada tahun 2021 (Direktorat Operasi Keamanan Siber, 2021), terdapat 262 *website* terdampak *phishing* di Indonesia. *Website* tersebut terdiri dari 10 sektor, antara lain sektor Lainnya, Pendidikan, Perdagangan, TIK, Pemerintah, Infrastruktur, Media, Jasa, Keuangan, dan Industri. Pada sektor Lainnya menjadi jumlah aktivitas *phishing* dengan jumlah sebanyak 76 hit. Kemudian diurutan kedua pada sektor Pendidikan dan diikuti sektor Perdagangan yang terdampak *phishing* terbanyak dengan jumlah 63 hit untuk sektor Pendidikan dan 31 hit untuk sektor Perdagangan. *Web phishing*

dan *email phishing* menjadi jenis *phishing* yang digunakan. Berikut data berdasarkan grafik yang dapat dilihat pada Gambar 1.1.



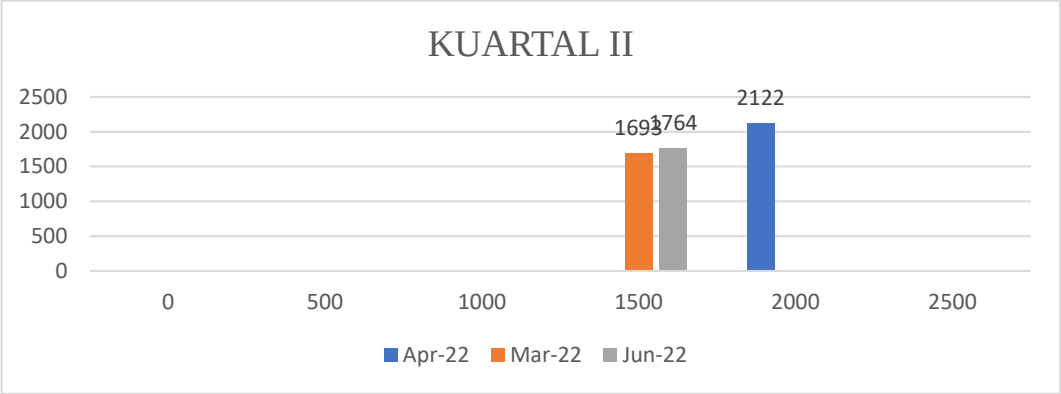
Gambar 1.1. Laporan *Monitoring* Keamanan Siber Tahun 2021
(Direktorat Operasi Keamanan Siber, 2021)

Berdasarkan data pada tahun 2022 di kuartal I, Indonesia Anti-*Phishing* Data Exchange (IDADX) mencatat total sebanyak 3.169 laporan *phishing* di Indonesia (Indonesia Anti-Phishing Data Exchange, 2022). Jumlah tersebut lebih rendah daripada kuartal IV pada tahun 2021 yang mencatat total sebanyak 5.325 laporan *phishing*. Jumlah laporan *phishing* pada tiga bulan pertama tahun 2022 mengalami catatan peningkatan dibandingkan pada tiga bulan pertama pada tahun 2021 yang hanya menerima sebanyak 536 laporan *phishing*. Pada bulan januari 2021 merupakan kasus *phishing* terbanyak dengan total 1.210 laporan *phishing*. Kemudian pada bulan Februari dan Maret menjadi 994 laporan dan 965 laporan secara berurutan. Berikut data berdasarkan grafik yang dapat dilihat pada Gambar 1.2.



Gambar 1.2. Laporan *Phishing* Kuartal I Tahun 2022
(Indonesia Anti-Phishing Data Exchange, 2022)

Berdasarkan data laporan *phishing* yang disampaikan kepada Indonesia Anti-*Phishing* Data Exchange (IDADX) pada kuartal II 2022 mendapatkan sebanyak total 5.579 laporan (Indonesia Anti-Phishing Data Exchange, 2022). Dari angka tersebut meningkat 2.410 laporan *phishing* jika dibandingkan dengan kuartal I 2022 yaitu sebanyak 3.169 laporan *phishing*. Jika dilihat berdasarkan bulannya, pada bulan April 2022 terdapat sebanyak 2.122 laporan *phishing*, lalu pada bulan Mei 2022 terdapat sebanyak 1.693 laporan, kemudian pada bulan Juni 2022 terdapat sebanyak 1.764 laporan *phishing.* Berikut data berdasarkan grafik yang dapat dilihat pada Gambar 1.3.



Gambar 1.3. Laporan *Phishing* Kuartal II Tahun 2022
(Indonesia Anti-Phishing Data Exchange, 2022)

Beberapa penelitian tentang *phishing* pernah dilakukan sebelumnya oleh Rio Wirawan, S.Kom, MMSI dan Haris Nizhomul Haq, S.Kom., M.Sc, pada tahun

2019 dengan menggunakan metode eksperimental yang dimana objek dari penelitian tersebut adalah pengguna *E-Learning* di UPN "Veteran" Jakarta khususnya Fakultas Ilmu Komputer. Hasil akhir dari penelitian ini adalah untuk mengetahui tingkat kesadaran pengguna terhadap keamanan sistem *E-Learning*.

Berdasarkan data di atas, dengan maraknya kasus *phishing* di Indonesia, maka penulis akan mencoba untuk melakukan eksperimen untuk menguji tingkat kesadaran dan pengetahuan terkait *phishing* pada sektor Pendidikan yaitu mahasiswa Universitas Pembangunan Nasional "Veteran" Jakarta. Kurangnya tingkat kesadaran mahasiswa terhadap kasus *phishing* akan menyebabkan kerugian bagi diri mereka sendiri, dikarenakan pelaku kejahatan *phishing (phiser)* akan memanipulasi *link* atau *URL* untuk mendapatkan informasi penting atau data pribadi dari korban yang terkena *phishing* tersebut.

Pada penelitian ini, penulis akan mencoba untuk membuat dua metode yaitu metode eksperimental dan kuesioner. Pada metode eksperimental, penulis akan membuat *web cloning website* SIAKAD UPNVJ. Dengan *web cloning* tersebut, penulis akan menyebarkan *link phishing* melalui *email dummy* yang mengatasnamakan UPN "Veteran" Jakarta. Melalui *email* tersebut, *link phishing* akan disebarkan ke beberapa *email* mahasiswa Angkatan 2020, 2021, dan 2022 di UPN "Veteran" Jakarta. Data mahasiswa akan masuk ke *database* yang mana pada penelitian ini penulis menggunakan *firebase realtime database.* Dari data tersebut akan memuat jumlah data mahasiswa yang terkena *phishing*, kemudian tingkat kesadaran mahasiswa akan dilihat berdasarkan persentase mahasiswa yang terkena *phishing* dan yang tidak terkena *phishing*. Pada metode kuesioner akan dihitung menggunakan analisis deskriptif dengan batasan nilai yang sudah ditentukan.

1.2. Rumusan Masalah

Adapun rumusan masalah yang akan didapatkan berdasarkan latar belakang diatas adalah sebagai berikut:

1. Bagaimana mengetahui tingkat kesadaran mahasiswa UPN "Veteran" Jakarta terhadap *mail phishing*?

2. Bagaimana mengetahui rata – rata tingkat pengetahuan mahasiswa UPN "Veteran" Jakarta terhadap *mail phishing*?

1.3. Tujuan Penelitian

Dalam pelaksanaan penelitian ini, penulis mengidentifikasi beberapa tujuan, di antaranya sebagai berikut:

1. Untuk memberi pengetahuan mengenai *phishing* untuk kalangan mahasiswa UPN "Veteran" Jakarta.
2. Untuk memberi masukan kepada UPT TIK UPN "Veteran" Jakarta untuk mengevaluasi berdasarkan sampel yang digunakan pada penelitian ini.

1.4. Manfaat Penelitian

Hasil penelitian diharapkan dapat memberikan manfaat dan kontribusi bagi pihak-pihak terkait, yaitu:

1. Sebagai bahan edukasi kesadaran dan pengetahuan bagi mahasiswa UPN "Veteran" Jakarta dalam melindungi diri dari ancaman kejahatan elektronik yaitu *mail phishing*.
2. Sebagai bahan kajian atau literatur bagi penelitian lainnya untuk mengembangkan penelitian mengenai kesadaran dan pengetahuan bahaya *mail phishing* pada kalangan mahasiswa UPN "Veteran" Jakarta atau penelitian terkait.

1.5. Ruang Lingkup

Berikut ini adalah beberapa ruang lingkup dalam penelitian ini, diantaranya sebagai berikut:

1. Penelitian ini hanya dilakukan di UPN "Veteran" Jakarta
2. Penyebaran *link phishing* hanya disebar ke *email* mahasiswa angkatan tahun masuk 2020,2021, dan 2022 di UPN "Veteran" Jakarta.
3. Survei disebarkan secara daring.
4. Target mahasiswa sebanyak 1.500 *email* dengan disebarkan secara *random.*

1.6. Luaran yang Diharapkan

Penelitian ini diharapkan dapat menghasilkan luaran berupa hasil kajian tingkat kesadaran dan pengetahuan data mahasiswa terhadap *mail phishing* agar dapat menjadikan bahan evaluasi terkait pemahaman mahasiswa mengenai bahaya *mail phishing*.

1.7. Sistematika Penulisan

Dalam penyusunan penulisan ini, penulis menggunakan sistematika penulisan yang cukup jelas sehingga pembaca dapat dengan mudah membaca, memahami, dan mempelajarinya. Sistematika penulisannya adalah sebagai berikut:

BAB I: PENDAHULUAN

Bab ini menguraikan secara singkat mengenai latar belakang masalah, rumusan masalah, tujuan penelitian, ruang lingkup penelitian, manfaat penelitian, luaran penelitian, serta sistematika penulisan.

BAB II: TINJAUAN PUSTAKA

Bab ini berisi tentang teori-teori yang akan digunakan sebagai acuan/pedoman dalam menyusun laporan tugas akhir tentang kegiatan yang dilakukan oleh penulis

BAB III: METODOLOGI PENELITIAN

Bab ini berisi langah-langkah penelitian dari metode perancangan sistem yang dirancang oleh penulis dalam penyusunan laporan tugas akhir dari tahapan pembuatan hingga tahapan penyususnan laporan tugas akhir.

BAB IV: PEMBAHASAN

Bab ini berisikan analisis dan evaluasi berdasarkan hasil penelitian yang sudah dilakukan terkait judul penelitian oleh peneliti.

BAB V: PENUTUP

Bab ini berisikan hasil penelitian yang telah disimpulkan serta pemberian saran terkait objek penelitian