

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi merupakan fenomena yang mendorong berbagai aspek kehidupan seperti pendidikan, ekonomi, politik, kebudayaan dan seni (Saniah *et al.*, 2024, hlm.995). Dalam aspek pendidikan penggunaan teknologi sudah menjadi bagian yang sangat penting bagi kehidupan mahasiswa. Pemanfaatan teknologi ini terus meningkat khususnya pada masa pandemi COVID-19, yang mana semua jenjang pendidikan bertransformasi melakukan pembelajaran secara daring atau *online* (Aransyah *et al.*, 2023, hlm.308). Penggunaan teknologi dimanfaatkan oleh mahasiswa terutama dalam mengakses informasi (Elindasari *et al.*, 2024, hlm.61). Kemudahan yang didapatkan melalui pemanfaatan teknologi ini dapat meningkatkan efisiensi serta efektivitas kegiatan pembelajaran dalam dunia akademik.

Terlepas dari kemudahan yang didapatkan, terdapat tantangan yang harus dihadapi yaitu berupa ancaman siber yang kini semakin berkembang pesat (Nabillah, Satriawan & Saputra, 2025, hlm.137). Ancaman siber adalah serangan yang berpotensi membahayakan dan mengakibatkan kerugian yang dapat merusak kerahasiaan, integritas, dan ketersediaan pada sistem informasi (Haryanto & Sutra, 2023, hlm.60). Adanya ancaman siber menunjukkan bahwa semakin berkembangnya teknologi maka semakin berkembang pula ancaman yang terjadi pada dunia lingkungan digital (Haryanto & Sutra, 2023, hlm.61). Oleh karena itu, hal ini harus menjadi fokus utama pengguna dalam pemanfaatan teknologi untuk lebih waspada terhadap masuknya berbagai potensi risiko yang ada.

Ancaman siber semakin meningkat seiring dengan berkembangnya teknologi informasi. Ancaman siber terbentuk menjadi berbagai metode yang semakin kompleks. Rizki (2022, hlm.57) menjelaskan bentuk ancaman siber yang sering terjadi dalam suatu negara yaitu serangan dalam *website* lembaga negara atau pemerintah seperti *phishing*, *malware*, dan *Advanced Persistent Threats* (APT). Target utama dari ancaman siber ini tidak hanya sistem yang digunakan tetapi juga manusia yang menjalankan sistem tersebut. Pengguna yang minim akan pengetahuan mengenai ancaman siber menjadi target yang mudah diperdaya oleh pelaku kejahatan siber.

Phishing merupakan bentuk penipuan yang dilakukan oleh pelaku kejahatan dengan tujuan untuk mendapatkan informasi pribadi korban yang bersifat rahasia dengan cara berpura-pura menjadi entitas terpercaya (Oktaviana & Rinaldi, 2025, hlm.655). Beberapa cara kerja *phishing* yaitu menyamar menjadi entitas terpercaya, mengirim pesan yang mendesak, mengirim pesan yang mengandung tautan palsu, dan menyalahgunakan informasi untuk melakukan kejahatan (Sulistyo *et al.*, 2024, hlm.386-387). Tidak hanya kehilangan data pribadi, risiko yang muncul akibat adanya serangan *phishing* ini yaitu mengalami kerugian finansial dan efek psikologi pada korban (Zalukhu *et al.*, 2026, hlm.1-2).

Bentuk *phishing* merupakan jenis ancaman yang sering terjadi dalam dunia pendidikan. Hal ini diungkapkan oleh Pusdatin (2025) yang mengatakan bahwa meskipun jauh dari dunia *e-commerce* dan perbankan, sektor pendidikan merupakan salah satu target serangan yang cukup sering. Hal ini dikarenakan sekolah memiliki data-data sensitif seperti rekap nilai, data pribadi siswa, dan dokumen internal yang dimiliki oleh sekolah. Adapun, Nuranisa, Hidayasari dan Ristra (2026, hlm.2297) sektor pendidikan menjadi target utama dari ancaman siber akibat dari lemahnya sistem keamanan informasi dan rendahnya kesadaran pengguna.

Sebagai pengguna terbanyak yang memanfaatkan teknologi, mahasiswa menjadi kelompok yang paling rentan akan terserang ancaman siber dalam bentuk *phishing*. Hal ini diungkapkan oleh Alfathi (2025) melalui laporan *Southeast Asia Freedom of Expression Network* (SAFE-net) yang menunjukkan 7 kelompok yang paling banyak mendapatkan serangan digital 2024 yaitu mahasiswa atau pelajar yang menempati posisi pertama dengan 83 kasus. Kurangnya literasi dalam menggunakan sosial media, kurangnya kesadaran akan keamanan siber, kurangnya pemahaman tentang cara melindungi dalam dunia maya, dan perilaku *oversharing* merupakan alasan utama peningkatan siber terjadi (Ananta, Ambodo & Tohawi, 2024, hlm.119).

Salah satu contoh kasus ancaman siber dalam bentuk *phishing* yang dapat ditemui di lingkungan pelajar dalam bentuk pesan seperti berikut.



Gambar 1 Screenshot Pesan Telegram

Sumber : Telegram 2024

Berdasarkan gambar 1 dapat dilihat bahwa pada tanggal 14 November 2024, terjadi kasus yang menargetkan salah satu mahasiswa Universitas YARSI. Pengirim mengirimkan pesan berupa tautan berbahaya yang dapat berpotensi terdapat virus yang dapat mencuri data pribadi. Dapat dilihat bahwa korban mencurigai aktivitas pesan tersebut sehingga korban memastikan kembali isi pesan tersebut.

Kesadaran akan pentingnya keamanan informasi merupakan salah satu hal yang wajib dimiliki oleh mahasiswa dalam menghadapi ancaman *phishing*. Memiliki tingkat kesadaran yang tinggi terhadap keamanan informasi dapat membantu seseorang menghindari risiko akan terjadinya ancaman siber. Sehingga diperlukannya kesadaran dan pemahaman yang baik terhadap keamanan informasi ini terhadap mahasiswa sehingga dapat melindungi diri dari berbagai ancaman siber tersebut.

Dalam Al-Qur'an, *phishing* termasuk kedalam tindak kejahatan yang dapat menipu banyak orang (Azzahra & Musthofa, 2024, hlm.2). Hal ini terdapat pada firman Allah ﷻ dalam (QS. Al-Baqarah [2]:188):

وَلَا تَأْكُلُوا أَمْوَالَكُمْ بَيْنَكُمْ بِالْبَاطِلِ وَتُدْلُوا بِهَا إِلَى الْحُكَّامِ لِتَأْكُلُوا فَرِيقًا مِّنْ أَمْوَالِ النَّاسِ بِالْإِثْمِ وَأَنتُمْ تَعْلَمُونَ

Terjemah Kemenag 2019

"Janganlah kamu makan harta di antara kamu dengan jalan yang batil dan (janganlah) kamu membawa (urusan) harta itu kepada para hakim dengan maksud agar kamu dapat memakan sebagian harta orang lain itu dengan jalan dosa, padahal kamu mengetahui." (QS. Al-Baqarah [2]:188)

Ayat tersebut berisikan larangan untuk melakukan peniruan terhadap suatu sistem lembaga, pencurian data dan penyalahgunaan data, serta memanipulasi sistem keuangan yang dapat merugikan pihak lain (Ahmad & Hamdi, 2025, hlm.388).

Penelitian serupa telah dilakukan oleh Nuranisa, Hidayasari dan Ristra (2026). Penelitian ini berfokus pada perilaku nyata pengguna melalui simulasi serangan *phishing*. Hasil penelitian ini menunjukkan bahwa tingkat kewaspadaan mahasiswa terhadap keamanan informasi masih tergolong rendah. Namun, penelitian ini belum mengkaji mengenai mengapa mahasiswa rentan dan apa yang menghambat mahasiswa dalam melakukan penerapan langkah keamanan informasi.

Berdasarkan kasus tersebut pentingnya memiliki kesadaran akan ancaman siber khususnya ancaman *phishing*. Memiliki kesadaran akan pentingnya ancaman siber sangat berpengaruh untuk melindungi keamanan informasi yang dimiliki sehingga dapat mencegah terjadinya kejahatan siber di lingkungan pendidikan. Oleh karena itu, berdasarkan penjelasan permasalahan di atas maka peneliti tertarik untuk melakukan penelitian dengan judul “Analisis Tingkat Kesadaran Keamanan Informasi Mahasiswa Universitas YARSI mengenai Ancaman *Phishing*”. Hasil penelitian ini diharapkan dapat meminimalisir terjadinya ancaman *phishing* di sektor pendidikan.

1.2 Perumusan Masalah

Hingga saat ini, data mengenai tingkat kesadaran mahasiswa YARSI mengenai ancaman *phishing* belum diketahui secara pasti. Padahal kesadaran mengenai ancaman *phishing* sangat diperlukan baik mahasiswa maupun universitas untuk menghindari kebocoran data pribadi hingga dokumen internal yang bersifat rahasia. Tanpa adanya pendataan mengenai tingkat kesadaran mahasiswa, universitas tidak dapat merancang program edukasi yang tepat sasaran. Oleh karena itu, diperlukan penelitian mengenai analisis tingkat kesadaran keamanan informasi mahasiswa Universitas YARSI mengenai ancaman *phishing*.

Berdasarkan latar belakang di atas, maka dapat disimpulkan rumusan masalah dalam penelitian sebagai berikut:

1. Bagaimana tingkat kesadaran keamanan informasi mahasiswa Universitas YARSI mengenai ancaman *phishing*?
2. Bagaimana pandangan Islam terhadap kesadaran keamanan informasi mengenai ancaman *phishing*?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka tujuan dari penelitian ini sebagai berikut:

1. Mengukur tingkat kesadaran keamanan informasi mahasiswa Universitas YARSI mengenai ancaman *phishing*.
2. Menganalisis pandangan Islam terhadap kesadaran keamanan informasi mengenai ancaman *phishing*.

1.4 Manfaat Penelitian

Berdasarkan tujuan penelitian, maka diharapkan penelitian ini dapat memberikan manfaat sebagai berikut:

1. Manfaat secara teoritis

Penelitian ini diharapkan dapat meningkatkan pemahaman dan kesadaran mahasiswa mengenai ancaman *phishing*. Selain itu, penelitian ini juga diharapkan dapat menjadi bahan rujukan oleh penelitian lainnya yang sedang mendalami topik terkait.

2. Manfaat secara praktis

- a. Penelitian ini diharapkan dapat memberikan pengetahuan kepada mahasiswa mengenai ancaman *phishing* yang dapat mengancam keamanan informasi.
- b. Memberikan gambaran ke perguruan tinggi untuk memberikan edukasi kepada mahasiswa terkait keamanan informasi guna mencegah terjadinya ancaman *phishing* di sektor pendidikan.

1.5 Batasan Penelitian

Agar penelitian ini dapat terfokus dan spesifik, maka peneliti memberikan batasan penelitian yaitu penelitian ini menggunakan metode kuantitatif dengan pendekatan deskriptif serta teknik pengumpulan data melalui survei menggunakan kuesioner. Selain itu, populasi yang digunakan dalam penelitian ini merupakan mahasiswa aktif S1 Universitas YARSI.