

BAB 1

PENDAHULUAN

1.1 LATAR BELAKANG

Perkembangan teknologi informasi terjadi begitu pesat sehingga membawa banyak dampak yang signifikan (Fahlevi, Saparudin, Mamunah, Irma, & Ekhsan, 2019). Salah satunya pada teknologi perbankan atau keuangan, menjadi layanan yang banyak dipilih oleh sebagian besar masyarakat untuk melakukan segala transaksi keuangan digital. Menurut data Bank Indonesia (BI), sejak 2019 telah dimulai pertumbuhan transaksi digital di Indonesia secara besar-besaran (Sautlan, 2021). Didukung dengan adanya pandemi, hal tersebut menjadi terus meningkat dan tren di kalangan masyarakat.

Layanan keuangan digital, dapat memudahkan, mempercepat, dan aman, sehingga membuat tingginya kebutuhan dalam bertransaksi menggunakan layanan tersebut. Maka, pengelola atau pemilik dari layanan keuangan digital harus melakukan peningkatan layanannya, terutama di bidang keamanan *cyber security* (Dianta & Zusrony, 2019). Sejak 2017 sampai 2020, ada 16.845 metode kejahatan dunia maya. Yang paling umum terjadi adalah di industri perbankan atau keuangan, yaitu *defacing* (penggantian atau modifikasi laman layanan digital), *phishing* (mengelabui pengguna layanan digital), *hacking* (peretasan layanan digital), *skimming* (penyalinan informasi data dari pengguna layanan digital), *social engineering* (rekayasa sosial ke pengguna layanan digital), dan *BEC (business email compromise)* (CNBC Indonesia, 2021). Telah ditunjukkan dari laporan tindak kejahatan *cyber crime* yang dikirim ke Direktorat Tindak Pidana Siber (Ditipidsiber) Polri bahwa *social engineering* (rekayasa sosial) merupakan tindak kejahatan yang paling umum terjadi sepanjang tahun 2020. Hal tersebut terjadi karena korban kurang waspada. Sehingga dengan mudahnya memberikan berbagai data pribadinya, seperti PIN atau *password*, atau bahkan kode rahasia, sehingga dengan mudah pelaku melakukan kejahatan siber dengan mengontrol dan mengakses akun nasabah (CNBC Indonesia, 2021).

Berdasarkan penjelasan permasalahan di atas, penggunalah yang memiliki peran penting dalam mengimplementasikan sistem keamanan informasi bukanlah teknologi, karena pengguna adalah penghubungnya (Mitnick & Simon, 2003). Oleh karena itu, pengguna harus selalu diarahkan dengan baik agar terhindar segala macam bentuk ancaman kejahatan. Karena permasalahan tersebut, maka perlu dilakukan penelitian terkait pengukuran tingkat kesadaran *cyber security* di kalangan pengguna layanan keuangan digital di Indonesia (Destya, 2020).

1.2 PERUMUSAN MASALAH

Berdasarkan penjelasan dari latar belakang di atas, maka penelitian ini akan melakukan pengukuran tingkat kesadaran keamanan kalangan pengguna layanan keuangan digital di Indonesia terkait keamanan *cyber security* dalam melakukan transaksi digital.

1.3 PERTANYAAN PENELITIAN

1. Bagaimana tingkat kesadaran kalangan pengguna layanan keuangan digital di Indonesia dalam mengimplementasikan sistem keamanan informasi?
2. Apa kriteria tertinggi kesadaran pengguna terhadap layanan keuangan digital di Indonesia?

1.4 TUJUAN PENELITIAN

Mengukur tingkat kesadaran *cyber security* pada kalangan pengguna layanan keuangan digital di Indonesia.

1.5 MANFAAT HASIL PENELITIAN

Harapan untuk hasil dari penelitian ini, yaitu mampu memberikan manfaat kepada seluruh lapisan masyarakat, yaitu:

1. Sebagai bahan edukasi untuk meningkatkan kesadaran masyarakat dalam melindungi dan menjaga data privasi dari ancaman kejahatan digital (*cyber crime*) dengan *cyber security*.
2. Sebagai referensi bagi peneliti lain untuk mengembangkan penelitian mengenai tingkat kesadaran *cyber security* atau seputar keamanan pada kalangan pengguna aplikasi keuangan digital atau penelitian yang terkait.