

1. Pendahuluan

Latar Belakang

Baru-baru ini muncul kasus peretasan terhadap mahasiswa UNDIP, dilaporkan bahwa 125 ribu data mahasiswa telah dicuri dengan informasi pribadi yang lengkap [1]. Oleh karena itu kesadaran dan pemahaman tentang keamanan adalah dasar untuk membangun keamanan yang baik dalam suatu organisasi. Bukti survei yang dipublikasikan membuktikan hal itu, pelatihan dan latar belakang pendidikan diakui memiliki hubungan yang signifikan dengan tingkat keamanan yang dapat dicapai, dan diutamakan dalam berbagai standar keamanan, banyak organisasi tidak mampu memanfaatkannya [2]. Pada saat ini masih banyak yang menggunakan otentikasi konvensional untuk keamanan akun, Sistem proses otentikasi konvensional hanya membutuhkan nama pengguna dan kata sandi untuk otentikasi. Metode ini, bagaimanapun, sangat nyaman untuk keamanan dari segala bentuk serangan serta otentikasi tanpa izin dengan hanya menggunakan *password* dan *username* [3].

Mahasiswa memerlukan kesadaran keamanan informasi, terutama internet yang sering digunakan sehari-hari [4]. Mahasiswa sebagai generasi Z memiliki hubungan erat dengan IT dan media sosial yang umumnya menggunakan proses otentikasi konvensional, oleh karena itu pada penelitian ini mengambil sampel pada mahasiswa Telkom University.

Oleh karena itu, pada penelitian ini digunakan tiga latar belakang mahasiswa yaitu jenis kelamin, tingkat semester, dan jenis pendidikan. Diketahui tingkat perilaku keamanan wanita jauh lebih rendah daripada laki-laki. Kesadaran akan keamanan pada wanita juga lebih rendah dibandingkan laki-laki bahkan terkadang wanita tidak sadar bahwa keamanannya diserang dikarenakan tingkat perilaku keamanan yang rendah tadi [2]. Ditemukan juga bahwa mahasiswa tingkat 1 maupun tingkat 4 bahkan yang sudah lulus tidak terlalu memahami ancaman cyber [3]. Jenjang pendidikan suatu mahasiswa tidak mempengaruhi kesadaran akan keamanan cyber namun pada penelitian ini akan diteliti lebih lanjut kesadaran pada mahasiswa IT dan non-IT.

Kata sandi adalah karakter yang disusun sebagai kunci hak atas data ataupun informasi [5]. Keamanan dengan kata sandi teks tetap paling umum digunakan untuk metode autentikasi akun. Sejak kata sandi teks yang rumit sulit di ingat, pengguna cenderung memilih kata sandi yang gampang dan mudah di ingat, akibatnya kata sandi lebih mudah ditebak, selain itu sering kali menggunakan kata sandi yang sama di berbagai akun agar mengurangi jumlah kata sandi yang harus di ingat berdasarkan akun yang dimiliki. Beberapa sistem mungkin sudah mengharuskan untuk mematuhi kebijakan agar menggunakan kata sandi yang rumit seperti mengharuskan ada beberapa huruf besar atau kecil, simbol, dan angka di dalam kata sandinya [6]. Tetapi masalah sebenarnya adalah pengguna itu sendiri, pengguna menggunakan pola huruf besar atau kecil dan angka atau simbol lainnya hanya di awal dan di akhir kata sandi, perilaku tersebut memudahkan upaya peretas akun untuk membaca pola kata sandi pengguna, perkembangan pola kata sandi baru sangat penting karena dapat mengurangi upaya peretas akun untuk menebak pola kata sandi [6].

Topik dan Batasannya

Berdasarkan uraian latar belakang yang telah dikemukakan diatas, maka perumusan masalah pada penelitian ini dapat disimpulkan sebagai berikut: “Apakah ada hubungan latar belakang mahasiswa terhadap *security awareness*?”.

Tujuan

Berdasarkan perumusan masalah yang ditemukan, penelitian ini bertujuan untuk: “Melakukan kajian terhadap hubungan latar belakang mahasiswa dengan tingkat *security awareness*”.