MINI PROPOSAL TUGAS AKHIR

Program Studi Pendidikan Teknik Informatika dan Komputer
Fakultas Keguruan dan Ilmu Pendidikan - Universitas Sebelas Maret Surakarta

---

Identitas Mahasiswa

Nama Mahasiswa	:	Fariz Fakhrul Arifin
NIM	:	K3515019
Nomor Handphone / WA	:	085716543304
IPK Terakhir	:	3.45
Jumlah SKS Kumulatif	:	144

Deskripsi Rencana Tugas Akhir

Judul Rencana Tugas Akhir

ANALISIS SECURITY AWARENESS MAHASISWA DALAM MENGHADAPI ANCAMAN SOCIAL ENGINEERING MENGGUNAKAN SOCIAL ENGINEERING TOOLKIT (SET)

Jenis Penelitian ☐ Kualitatif ☑ Kuantitatif ☐ PTK ☐ Research and Development

☐ Lain-Lain (Sebutkan: .....)

Latar Belakang

Perkembangan internet saat ini menyebabkan pertukaran informasi sangat cepat, dapat melalui *social media*, *e-commerce*, *messaging* ataupun portal multimedia. Dalam pertukaran informasi tersebut ada informasi yang bersifat rahasia dan bersifat umum. Informasi yang bersifat rahasia sering kali hilang kerahasiaannya ketika informasi tersebut dikirimkan ke social media, hal tersebut seringkali menjadi sasaran serangan *social engineering* (Amin, 2014) .

Keamanan informasi adalah suatu upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin timbul kapan saja (Sarno dan Iffano, 2009) . Dalam keamanan informasi, dimana informasinya sendiri itu tidak memiliki arti fisik, keamanan informasi memiliki beberapa aspek aspek yang harus dipenuhi untuk menjaga keamanan informasi yaitu informasi yang diberikan harus akurat dan lengkap, informasi harus dipegang oleh orang yang berwenang, dan dapat diakses digunakan sesuai dengan kebutuhan, dan terakhir memberikan informasi pada format yang tepat. Akan tetapi dalam menjaga keamanan informasi ada faktor-faktor yang membuat keamanan informasi itu gagal dalam menjaga informasi atau bocornya informasi salah satunya yaitu kesadaran dalam menjaga keamanan informasi. Sebagai pengguna seharusnya dapat menyadari bahwa keamanan informasi itu sangat penting, oleh karena itu perlu adanya kesadaran keamanan infromasi dari pengguna itu sendiri, seperti penelitian yang dilakukan oleh Ghafir, Prenosil, Alhejailan, & Hammoudeh, (2016) . Hasil penelitian tersebut menyimpulkan bahwa *social engineering* merupakan serangan yang serius untuk keamanan informasi dimana pelaku *social engineering* mengeksploitasi pengguna untuk mendapatkan informasi yang sangat rahasia. Dan juga kesadaran keamanan dapat menjadi instrumen yang kuat untuk melawan *cybercrime* seperti *social engineering*.

Social engineering adalah jenis serangan yang memanfaatkan kelamahan psikologis manusia. Serangan social engineering dapat digambarkan dengan empat fase, yaitu pengumpulan informasi, mengembangkan hubungan, ekspolitasi dan eksekusi (Zulkurnain et al., 2015) . Dalam penyerangan *social engineering*, target dari penyerangan *social engineering* tidak sadar bahwa informasi yang dimiliki sedang dicuri. Tidak ada metode teknik untuk mengatasi *social engineering*, dikarenakan *social engineering* itu memanfaatkan kelemahan *user* dalam segi pengetahuan maupun *awareness* (Septiani et al., 2016) . Adapun cara untuk mencegah penyerangan tersebut yaitu dibutuhkan kesadaran, ketelitian terhadap informasi yang dibagikan oleh *user* itu sendiri dibandingkan pelaku *social engineering*. Seperti penyerangan *phishing* yang memanfaatkan kelemahan user, dikarenakan *user* masih lemah terhadap *social engineering* maka kesadaran terhadap keamanan informasi masih lemah (Suherman, Widodo, dan Gunawan, 2016)

Social engineering dapat terjadi dimana saja seperti di lingkungan kampus, lingkungan perkantoran ataupun lingkungan masyarakat. Tanpa disadari ada beberapa kemungkinan buruk ataupun risiko yang tidak terduga bisa terjadi begitu saja apalagi

dengan memanfaatkan kelemahan manusia sebagai penggunanya, seperti di kampus V UNS pabelan tidak semua mahasiswa mampu menyadari serangan *social engineering* ada beberapa contoh yang dialami oleh mahasiswa beberapa diantaranya mengalami serangan *phishing*. Selain menggunakan metode *phishing* dalam *social engineering* ada juga metode lainnya yaitu metode-metode *Dumpster Diving, Shoulder Surfing, Reverse Social Engineering, Windows Pop-up.* Dalam penyerangan *social engineering* yang sering kali digunakan yaitu *phishing attack*, *phisher* (sebutan untuk pelaku *phishing)* berupaya menipu untuk mendapatkan informasi yang bersifat sensitif dengan membuat halaman *web* yang sama persis dari bank, s*ocial media*, *e-commerce* atau *provider*, yang memanfaatkan kelemahan korban untuk mendapatkan informasi tersebut (Anti-Phishing Working Group, 2014) . Terlebih penyerangan pada *social media* sering terjadi karena keteledoran penggunanya itu sendiri, seperti peningkatan jumlah pengikut pada *Instagram*, dengan menggunakan suatu *website* yang mana harus memasukan *username* dan kata sandi.

Selain itu *social engineering* dapat menyerang siapa saja, terlebih lagi untuk orang yang kurang waspada mengenai *social engineering* akan menjadi sasaran empuk bagi pelaku *social engineering*, terutama bagi lingkungan kampus yang dimana mahasiswa setelah lulus akan menghadapi dunia kerja, harus mengetahui dan paham betul akan bahaya dari *social engineering*, yang bisa berdampak bagi tempatnya bekerja.

Berdasarkan penelitian yang dilakukan oleh (Dodge et al., 2007) , dalam penelitiannya melakukan serangan *phishing* terhadap beberapa kelas dianataranya *freshman, sophomores, junior,* dan, *seniors*. hasil penelitian tersebut menjelaskan dari keempat kelas tersebut dengan adanya pelatihan mengenai *phishing* dimana dalam pelatihan tersebut dapat menurunkan terjadinya serangan *phishing*.

Berdasarkan latar belakang yang telah dideskripsikan, penelitian ini akan meneliti tentang seberapa jauh pemahaman *user* tentang kesadaran keamanan informasi di lingkungan kampus. Karena dari lingkungan kampus dapat melatih kesadaran keamanan informasi lebih awal sebelum terjun kedunia kerja. Selain itu, penilitian ini juga bertujuan untuk meningkatkan kesadaran terhadap keamanan informasi sebagai upaya pencegahan *social engineering* terjadi.

Rumusan Masalah

1. Seberapa jauh kesadaran keamanan informasi terhadap serangan *social engineering* yang terjadi di lingkungan kampus V UNS?

2. Bagaimana cara meningkatkan kesadaran keamanan informasi terhadap *social engineering*?

Tujuan Penelitian

1. Mengetahui tingkat kesadaran terhadap keamanan informasi di wilayah kampus V UNS Pabelan.

2. Meningkatkan kesadaran keamanan informasi upaya pencegahan *social engineering* dengan menggunakan *Social Engineering Toolkit* (SETOOLKIT).