STUDI KOMPETENSI DAN KESADARAN PENGGUNA E-LEARNING TERHADAP KEAMANAN SISTEM E-LEARNING PADA PENDIDIKAN TINGGI

[1]Rio Wirawan, [2]Haris Nizhomul Haq

[1,2]Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta

[1,2]Jl. RS Fatmawati Pondok Labu, Jakarta Selatan, Indonesia

E-mail: [1]Rio.wirawan@upnvj.ac.id, [2]harisnizhom@gmail.com

Abstract. *Weak security of information in particular in e-learning systems can open the risk of harming the elements that exist within the system environment. So this research has the purpose to analyze the fraud or attacks that are usually done by users and identify patterns of behavior or attitudes that allow damage to the security system in e-learning. This study aims to identify the level of awareness of users, especially students in using e-learning system. This study uses an experimental method of user e-learning in computer science faculty UPN "Veteran" Jakarta where the end result of this research is to identify the level of awareness of the user to the security of e-learning system.*

Keywods: E-learning, Competention, Awareness, Security.

Abstrak. *Lemahnya keamanan informasi pada khususnya dalam sistem e-learning dapat membuka resiko yang merugikan elemen-elemen yang ada didalam lingkungan sistem tersebut. Sehingga penelitian ini memiliki tujuan untuk menganalisa kecurangan maupun serangan yang biasa dilakukan oleh pengguna dan mengidentifikasikan pola perilaku ataupun sikap yang memungkinkan merusak sistem keamanan pada e-learning. Penelitian ini memiliki tujuan untuk mengidentifikasi tingkat kesadaran pengguna terutama mahasiswa dalam menggunakan sistem e-learning. Studi ini menggunakan metode eksperimental terhadap user e-learning di lingkungan fakultas ilmu komputer UPN "Veteran" Jakarta dimana hasil akhir dari penelitian ini adalah pengindentifikasian tingkat kesadaran user terhadap keamanan sistem e-learning.*

Kata kunci: E-learning, Kompetensi, Kesadaran, Keamanan.

1. Pendahuluan

Seiring dengan penggunaan e-learning sebagai unsur pendukung proses belajar mengajar dimana memberi kemudahan akses terhadap penggunanya tanpa mengenal batas waktu dan lokasi, keamanan sebuah sistem menjadi salah satu aspek penting didalam sistem e-learning. Telah banyak penelitian yang dilakukan terkait dengan keunggulan dan manfaat yang diperoleh dari e-learning, namun masih sedikit yang memberikan perhatian lebih terhadap peranan keamanan informasi didalam lingkungan e-learning. Keamanan informasi menjadi sangat penting didalam lingkungan e-learning dimana lemahnya aspek ini mampu membuka peluang resiko yang bisa merugikan elemen-elemen yang ada di dalam lingkungan e-learning.

Berikut ini beberapa serangan atau kecurangan yang umumnya dilakukan di dalam lingkungan e-learning (Kritzinger, 2008):

- Mahasiswa yang mencegat (intercept) pekerjaan tugas mahasiswa lainnya dan mengumpulkan tugas tersebut sebagai hasil pekerjaannya.
- Mahasiswa yang mendapatkan hak akses yang tidak sah (unauthorized) terhadap database nilai tugas dan mengubah nilai tugasnya maupun mahasiswa lain.
- Mahasiswa yang mendapatkkan bantuan dari sumber-sumber (resources) yang ada di dalam lingkungan e-learning untuk digunakan pada ujian.

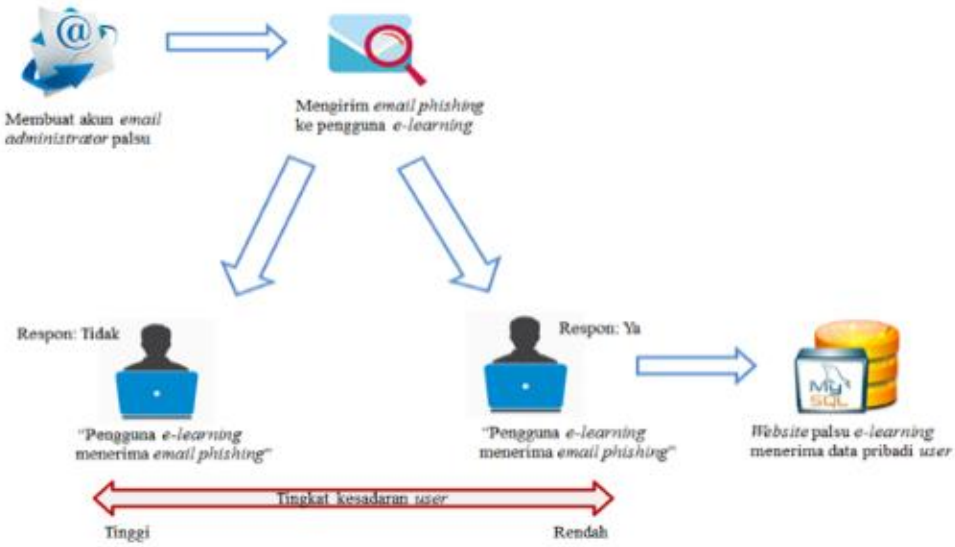
2. Metodologi Penelitian

Penelitian ini akan dilakukan untuk menilai dan mengukur tingkat kesadaran dan kompetensi pengguna dalam isu keamanan sistem e-learning pada peringkat pendidikan tinggi. Untuk menilai tingkat kesadaran dan kompetensi mahasiswa dilakukan 3 (tiga) metode untuk mencapai tujuan penelitian ini.

Metode Pertama

Untuk menilai dan mengukur tingkat kesadaran user e-learning di lingkungan Fakultas Ilmu Komputer Universitas Pembangunan Nasional "Veteran" Jakarta dilakukan metode eksperimen. Objek dari studi ini adalah mahasiswa dari tiap jurusan yang ada di Fakultas Ilmu Komputer yaitu mahasiswa S1 Jurusan Sistem Informasi, mahasiswa S1 Jurusan Teknologi Informasi dan mahasiswa D3 Jurusan Manajemen Informasi angkatan 2013, 2014, 2015 dan 2016.

Studi ini menggunakan serangan phishing yang disebarkan ke email masing-masing mahasiswa dengan menggunakan email dari admin e-learning yang mengarahkan mahasiswa untuk memperbarui informasi personal di website e-learning palsu. Hasil data tersebut akan tersimpan ke dalam database untuk di analisa seperti yang terlihat pada Gambar 1.

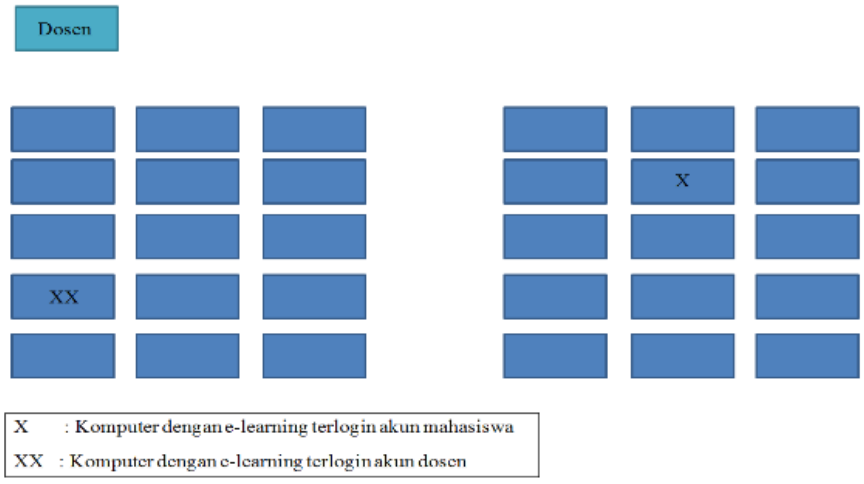


Gambar 1. Pengumpulan Data Metode Pertama

Metode Kedua

Pada metode kedua, dilakukan simulasi yang akan dijalankan didalam ruang laboratorium Fakultas Ilmu Komputer. Simulasi ini dilakukan untuk mengetahui kompetensi mahasiswa apabila menemukan halaman e-learning yang sudah terlogin dengan akun milik mahasiswa lain ataupun milik dosen apakah dimanfaatkan untuk melakukan kegiatan yang dapat merugikan orang lain seperti merubah data informasi, password, atau mengambil data hasil pekerjaan orang tersebut. untuk simulasi ini, akan disiapkan beberapa komputer yang diambil secara random yang didalamnya pada halaman website e-learning sudah terlogin dengan akun milik mahasiswa lain dan juga milik dosen lain. Pada simulasi ini setiap komputer yang ada pada laboratorium komputer akan diawasi dengan menggunakan aplikasi pengendali komputer yang dapat menghubungkan komputer secara *remote* sehingga aktivitas setiap mahasiswa dapat terawasi dengan baik.

Skema penelitian pada metode kedua ini, seperti yang terlihat pada Gambar 2. dilakukan penyetingan dua komputer dengan akun yang sudah terlogin akun mahasiswa dan juga akun dosen. Yang akan diawasi oleh peneliti diruangan lain pada saat kelas praktikum di ruang laboratorium komputer. Pengawas yang berada pada ruangan lain tersebut akan melihat respon dari mahasiswa yang menemukan komputer dengan keadaan website e-learning terlogin akun apakah akan memanfaatkan kesempatan tersebut atau mengabaikannya.



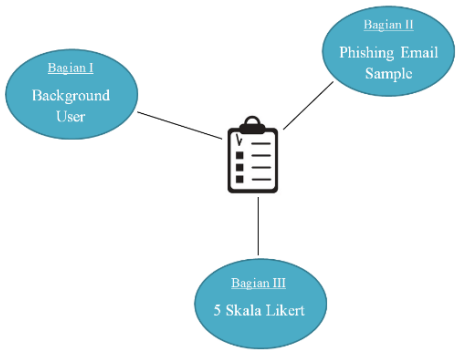
Gambar 2. Skema Komputer Metode Kedua

Metode Ketiga

Untuk metode ketiga, penelitian berfokus pada analisa data berdasarkan hasil survey melalui kuesioner yang dibagikan kepada mahasiswa untuk mengetahui pemahaman mahasiswa berdasarkan *background* maupun sikap mahasiswa tentang isu keamanan e-learning. Kuesioner diberikan kepada mahasiswa dengan tiga jenis kuesioner, bagian yang pertama kuesioner yaitu kuesioner untuk mengetahui *background user* dalam menggunakan komputer maupun internet secara umum maupun

https://doi.org/10.29313/ethos.v7i1.3850

pendidikan ilmu komputer secara khusus. Sedangkan bagian kedua kuesioner lebih kepada soal-soal email yang masuk kedalam kategori *phishing* atau email resmi (asli) yang digunakan untuk mengetahui tingkat pemahaman *user* tentang email *phishing*. sedangkan pada bagian ketiga lebih kepada pertanyaan untuk mengetahui tingkat kesadaran user tentang keamanan komputer secara *online* seperti yang terlihat pada Gambar 3.



Gambar 3. Komponen Kuesioner

Pada metode ini, menggunakan kuesioner skala *likert* berdasarkan tingkat setuju terhadap suatu *statement* tentang kesadaran keamanan e-learning dengan 5 (lima) opsi respon; (1) Sangat Tidak Setuju, (2) Tidak Setuju, (3) Netral, (4) Setuju, (5) Sangat Setuju.

Definisi E-learning

E-learning merupakan salah satu sistem pendidikan yang menggunakan aplikasi elektronik dengan media internet, jaringan komputer, maupun komputer standalone untuk mendukung kegiatan belajar mengajar (A.Ratnasari, 2012). Atau dapat disimpulkan, e-learning adalah konsep pendidikan yang memanfaatkan Teknologi Informasi dan Komunikasi untuk mendukung proses dan meningkatkan pengalaman belajar dan mengajar (Mohd Alwi dan Fan, 2010).

E-learning tidak hanya melibatkan mahasiswa sebagai pengguna yang dapat mengakses sistem ini untuk proses belajar, namun juga melibatkan dosen yang mana dapat menyediakan catatan ataupun materi pelajaran, soal-soal tugas maupun latihan untuk menilai performa peserta perkuliahannya, dan juga administrator (admin) sebagai penyedia maupun pengelola yang berperan sangat penting di dalam ketersediaan layanan maupun keamanan sistem e-learning.

Menurut A. Ratnasari, Learning Management System (LMS) merupakan platform aplikasi e-learning yang bertujuan untuk mengelola konten kegiatan pendidikan. LMS secara umum memiliki fitur-fitur standar pembelajaran elektronik antara lain: Fitur Kelengkapan Belajar Mengajar seperti silabus mata kuliah, materi mata kuliah (berbasis teks maupun multimedia), dan lain-lain; Fitur Diskusi dan Komunikasi seperti forum maupun instant messenger untuk sarana komunikasi; dan juga Fitur Ujian dan Penugasan.

Keamanan Sistem

Aspek lain untuk membuat aplikasi yang sukses terdiri dari kombinasi tiga faktor penting yaitu Teknologi, Proses, dan Manusia. Dengan membangun sebuah aplikasi yang mengandung data-data yang sangat penting, ketiga faktor tersebut harus saling mendukung satu sama lain. Penggunaan Teknologi memungkinkan untuk melindungi integrity dan confidentiality sistem dengan menggunakan enkripsi maupun firewall

untuk mem-block dan menolak hak akses yang tidak sah (unauthorized access) pada sistem e-learning.

Menurut Edhy Sutanta, 2008. Confidentiality yaitu segala usaha yang berkaitan dengan pencegahan pangaksesan terhadap informasi. Hal ini lebih berkaitan dengan privacy (data personal) dan secrecy (kerahasiaan). Sedangkan integrity secara umum berkaitan dengan jaminan bahwa sesuatu berada dalam kondisi seharusnya.

Sedangkan faktor akhir yaitu Manusia hampir selalu menjadi titik terlemah dalam setiap Proses maupun Teknologi. Human factor memberikan peranan yang vital dalam pemberian dukungan pada mekanisme keamanan.

3. Hasil Dan Pembahasan

1. Metode Pertama

Berdasarkan hasil penelitian pada Metode 1 dimana studi ini melibatkan 502 mahasiswa sebagai objek penelitian dari jumlah total 690 mahasiswa angkatan 2013, 2014, 2015 dan 2016.

Tabel 1. Detail Sampel Penelitian

Variabel	Jumlah (%)
Mahasiswa yang dikirim email phishing	**502**
Perempuan	*125(24.90%)*
Laki-laki	*377(75.10%)*
Angkatan:	
2013	*173(34.46%)*
2014	*138(27.49%)*
2015	*88(17.53%)*
2016	*103(20.52%)*

Tabel 1. Menampilkan detail sampel penelitian yang dilakukan terhadap mahasiswa di lingkungan Fakultas Ilmu Komputer Universitas Pembangunan Nasional "Veteran" Jakarta. Dari tabel tersebut terlihat bahwa mahasiswa laki-laki lebih dominan (75.10%) berbanding dengan mahasiswa perempuan. Sedangkan untuk angkatan, jumlah mahasiswa terbanyak dari angkatan 2013 (34.46%) sementara angkatan 2015 untuk mahasiswa yang paling sedikit (17.53%).

Tabel 2. Detail Respon Sampel Penelitian

Variabel	Jumlah(%)
Mahasiswa yang merespon email phishing	**125**
Perempuan	*37(29.60%)*
Laki-laki	*88(70.40%)*
Angkatan:	
2013	*67(53.60%)*
2014	*12(9.60%)*
2015	*17(13.60%)*
2016	*29(23.20%)*

Berdasarkan Tabel 2. Dapat terlihat bahwa mahasiswa yang merespon phishing email yang dikirimkan mencapai 125 mahasiswa (24.90%) dan yang tidak merespon phishing email sebanyak 377 mahasiswa (75.10%). Dari 125 mahasiswa, mahasiswa perempuan yang merespon phishing email sebanyak 37 mahasiswa mencapai 29.60% dari total mahasiswa perempuan yang dikirimi phishing email. Sedangkan mahasiswa laki-laki

https://doi.org/10.29313/ethos.v7i1.3850

sebanyak 88 mahasiswa mencapai 23.34%.

Pada tabel tersebut juga dapat terlihat bahwa angkatan 2013 (53.60%) terbanyak yang merespon phishing email dan mengirimkan data pribadi mahasiswa. Sedangkan untuk angkatan yang paling sedikit merespon adalah angkatan 2014 (9.60%) diikuti 2015 (13.60%) dan 2016 (23.20%).

2. Metode Kedua

Metode kedua ini dilakukan didalam ruangan laboratorium komputer Fakultas Ilmu Komputer UPN "Veteran" Jakarta dengan 8 (delapan) kali simulasi pada 3 ruangan lab dan matakuliah yang berbeda seperti yang terlihat pada Tabel 3.

Dan pada Tabel 4. Memperlihatkan respon dari tiap-tiap mahasiswa terhadap kondisi komputer yang tersetting e-learning dengan keadaan terlogin akun mahasiswa lain dan juga akun dosen.

Tabel 3. Detail Simulasi

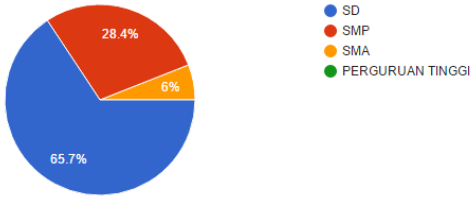
No. Sampel	Ruang Lab	Sampel Mahasiswa	Mata Kuliah	Akun Dummy
B1	B	Mahasiswa Jurusan MI Angkatan 2015	Algoritma Pemogramam	• Akun Mahasiswa Angkatan Senior (1310512076) • Akun Mahasiswa Angkatan Senior (1410512035)
C1	C	Mahasiswa Jurusan TI Angkatan 2015	Data Mining	• Akun Mahasiswa Angkatan Senior (1410512035) • Akun Dosen Matakuliah VB
C2	C	Mahasiswa Jurusan SI Angkatan 2015	Pemograman VB	• Akun Mahasiswa Angkatan Senior (1410501007) • Akun Dosen Matakuliah Pemograman VB
C3	C	Mahasiswa Jurusan SI Angkatan 2015	Sistem Basis Data	• Akun Mahasiswa Angkatan Senior (1310511017) • Akun Dosen Matakuliah Sistem Basis Data
D1	D	Mahasiswa Jurusan MI Angkatan 2014	Perancangan Basis Data	• Akun Mahasiswa Angkatan Senior (1310512015) • Akun Dosen Matakuliah Sistem Basis Data
D2	D	Mahasiswa Jurusan MI Angkatan 2014	Pemograman Java II	• Akun Mahasiswa Angkatan Senior (1310512080) • Akun Dosen Matakuliah Pemograman VB
D3	D	Mahasiswa Jurusan SI Angkatan 2014	Pemograman VB	• Akun Mahasiswa Angkatan Junior (1510511005) • Akun Dosen Matakuliah Pemograman VB
D4	D	Mahasiswa Jurusan TI Angkatan 2015	Jaringan Komputer	• Akun Mahasiswa Satu Angkatan (1510511005) • Akun Dosen Matakuliah Sistem Basis Data

Tabel 4. Detail Respon Mahasiswa Simulasi

No. Sampel	Akun Dummy	Respon	Kategori o Respon
B1	Akun Mahasiswa Angkatan Senior (1310512076)	Tidak menggunakan komputer diduga user tidak memperhatikan komputer	Netral
	Akun Mahasiswa Angkatan Senior (1410512035)	Membuka tab baru untuk browsing dan tidak merespon apapun pada akun tersebut	Netral
C1	Akun Mahasiswa Angkatan Senior (1410512035)	Tidak menggunakan komputer diduga user tidak memperhatikan komputer	Netral
	Akun Dosen Matakuliah VB	Hanya meminimize browser e-learning dan membuka facebook	Netral
C2	Akun Mahasiswa Angkatan Senior (1410501007)	Tidak menggunakan komputer diduga user tidak memperhatikan komputer	Netral
	Akun Dosen Matakuliah Pemograman VB	Menggunakan komputer dan kemudian langsung men-shutdown komputer	Positif
C3	Akun Mahasiswa Angkatan Senior (1310511017)	User menggunakan untuk browsing facebook dengan sesekali melihat profil akun user dummy dan tak ada respon lain	Netral
	Akun Dosen Matakuliah Sistem Basis Data	User melihat-lihat profil akun dosen dan kemudian melogout akun e-learning tersebut	Positif
D1	Akun Mahasiswa Angkatan Senior (1310512015)	Menggunakan komputer untuk kegiatan browsing tanpa melakukan apapun terhadap akun dummy	Netral
	Akun Dosen Matakuliah Sistem Basis Data	Tidak menggunakan komputer diduga user tidak memperhatikan komputer	Netral
D2	Akun Mahasiswa Angkatan Senior (1310512080)	User melihat e-learning dengan keadaan terlogin namun tidak melakukan hal lain. Hanya menonton youtube	Netral
	Akun Dosen Matakuliah Pemograman VB	Tidak menggunakan komputer diduga user tidak memperhatikan komputer	Netral
D3	Akun Mahasiswa Angkatan Junior (1510511005)	Tidak menggunakan komputer diduga user tidak memperhatikan komputer	Netral
	Akun Dosen Matakuliah Pemograman VB	Tidak menggunakan komputer diduga user tidak memperhatikan komputer	Netral
D4	Akun Mahasiswa Satu Angkatan (1510511005)	User melihat-lihat profil akun mahasiswa namum membuka tab baru dan tidak melakukan respon lain	Netral
	Akun Dosen Matakuliah Sistem Basis Data	Tidak menggunakan komputer diduga user tidak memperhatikan komputer	Netral

3. Metode Ketiga

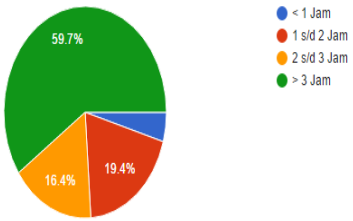
Pada metode ketiga ini, didapatkan berdasarkan *background* atau pengalaman user terhadap penggunaan komputer dan internet yang berkaitan erat dengan keamanan sistem ditampilkan pada gambar 5 dan gambar 6.



Gambar 5. Detail Background pengguna e-learning UPN "Veteran" Jakarta

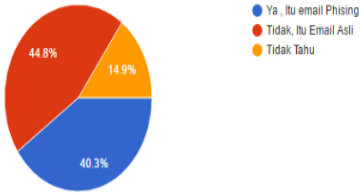
https://doi.org/10.29313/ethos.v7i1.3850

Gambar 5 memperlihatkan dan mendapatkan materi dan penggunaan komputer sejak tingkat sekolah dasar sebanyak 65.7% hal ini menunjukan telah lamanya mahasiswa mengetahui konsep dan penggunaan komputer.



Gambar 6. Detail waktu pengguna e-learning UPN "Veteran" Jakarta

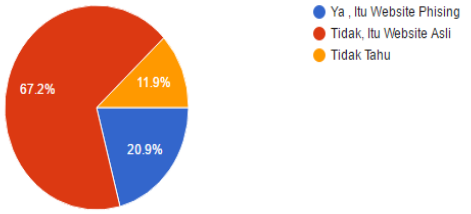
Gambar 6 memperlihatkan waktu penggunaan komputer lebih dari 3 jam sebanyak 59.7% hal ini menunjukan telah lamanya mahasiswa menggunakan penggunaan computer pada Gambar 7 dibawah ini menampilkan detail tingkat kesadaran sebuah email phising atau email asli. setelah diperlihatkan sebuah email phising.



Gambar 7. Tingkat Kesadaran atau Persepsi Mahasiswa terhadap email

Gambar 7 memperlihatkan masih nanyak nya ketidaksadaran mahasiswa terhadap email phising hal ini menunjukan hanya 40.3% menjawab dan mengetahui email phising yang tidak mengetahui sebanyak 44.8% dan yang tidak mengerti sebanyak 14.9%

pada Gambar 8. Menampilkan detail tingkat kesadaran sebuah website phising atau website asli. setelah diperlihatkan sebuah website phising



Gambar 8. Tingkat Kesadaran atau Persepsi Mahasiswa terhadap website.

Gambar 8 memperlihatkan masih nanyak nya ketidaksadaran mahasiswa terhadap website phising hal ini menunjukan hanya 20.9% menjawab dan mengetahui website phising yang tidak mengetahui sebanyak 67.2% dan yang tidak mengerti sebanyak 11.9%

4. Kesimpulan dan Saran

Berdasarkan studi yang dilakukan dengan menggunakan metode eksperimen yang telah dilakukan untuk mengidentifikasi tingkat kesadaran pengguna e-learning di lingkungan Fakultas Ilmu Komputer Universitas Pembangunan Nasional "Veteran" Jakarta yang melibatkan 502 (72.75%) mahasiswa. Melalui pengiriman phishing email yang dikirimkan ke email masing-masing pribadi, didapati 125 (24.90%) dengan jumlah angkatan 2013 (53.60%) terbanyak diikuti angkatan 2016 (23.20%), 2015 (13.60%), dan 2014 (9.60%) yang merespon ataupun memiliki tingkat kesadaran akan keamanan yang rendah. Dimana mereka telah mengirimkan data penting pribadi seperti alamat email dan username akun e-learning mereka.

Melalui pengiriman survey yang dilakukan untuk melihat secara personal kesadaran akan keamanan didapat masih lemahnya kesadaran akan keamanan

informasi mahasiswa terhadap email phising dan website phising.

Namun berdasarkan data yang tercantum pada Tabel 2. Terlihat bahwa untuk angkatan 2013 menjadi angkatan yang terbanyak terkena phishing email (53.60%). Untuk angkatan 2014, 2015, dan 2016 terlihat bahwa pengguna e-learning yang lebih lama masa kuliahnya, lebih tinggi tingkat kesadaran akan keamanannya (lebih sedikit yang merespon phishing email). Sehingga diperlukan studi yang lebih lanjut yang perlu dilakukan untuk menilai atau mengukur persepsi (pemahaman) dan juga background pengalaman user tentang isu keamanan seperti berbagi password dan menyimpan informasi penting pribadi melalui email maupun website yang mencurigakan.

Namun studi lanjutan masih perlu dilakukan untuk membantu mengukur dan juga menilai faktor-faktor lain yang terkait terhadap tingkat kesadaran atau kewaspadaan user terhadap keamanan sistem e-learning. Penyebaran kuisioner kepada mahasiswa yang dalam konteks ini menjadi pengguna (user) e-learning agar dapat mengidentifikasi persepsi (pemahaman) dan juga background pengalaman mereka pada isu keamanan sistem e-learning.

Daftar Pustaka

Kementerian Pendidikan dan Kebudayaan Republik Indonesia. 2013. Peraturan Menteri Pendidikan dan Kebudayaan Nomor 109 Tahun 2013 Tentang Penyelenggaraan Pendidikan Jarak Jauh Pada Pendidikan Tinggi.

Kritzinger, E. 2008. Information Security in an E-learning Environment. Social and Organizational Liabilities on Information Security.

Mohd Alwi,N.H. dan I.S. Fan. 2010. *E*-Learning and Information Security Management. International Journal of Digital Society(IJDS).

Ratnasari, Anita. 2012. Studi Pengaruh Penerapan E-learning Terhadap Keaktifan Mahasiswa dalam Kegiatan Belajar Mengajar Studi Kasus Universitas Mercu Buana Jakarta. Seminar Nasional Aplikasi Teknologi Informasi.

Sutanta, Edhy. 2008. Analisis Keamanan Sistem Aplikasi (Studi Kasus Aplikasi E-learning di IST AKPRIND Yogyakarta). Seminar Nasional Aplikasi Sains dan Teknologi.