SNHRP-II : Seminar Nasional Hasil Riset dan Pengabdian, Ke-II, 2019

Tersedia *online* di http://snhrp.unipasby.ac.id/

ISBN: 978-602-5793-57-8

SNHRP-II
UNIPA Surabaya

Pengukuran Kesadaran Keamanan Informasi dan Privasi Pada Ibu Rumah Tangga dan Remaja di Desa Jrebeng, Kecamatan Dukun, Kabupaten Gresik

Luvia Friska Narulita [1], Agung Kridoyono [2]

[1] Teknik Informatika, Fakultas Teknik, Universitas 17 Agustus 1945 Surabaya – Jl. Semolowaru 45 Surabaya

[2] Teknik Informatika, Fakultas Teknik, Universitas 17 Agustus 1945 Surabaya – Jl. Semolowaru 45 Surabaya

E-mail: luvia@untag-sby.ac.id

ABSTRAK

Penggunaan internet menjadi hal yang wajar di kalangan ibu rumah tangga dan remaja, seringkali ibu rumah tangga menggunakan internet untuk berbagai keperluan, misalnya belanja atau hanya sekedar untuk komunikasi. Begitu juga dengan remaja. Tidak jarang remaja memanfaatkan internet untuk hiburan atau untuk mengerjakan tugas sekolah. Mudahnya penggunaan internet, apalagi didukung dengan mudahnya memiliki telepon pintar atau smartphone, membuat pengguna internet semakin meningkat. Seiring meningkatkan penggunaan internet tersebut juga mendorong adanya kejahatan internet berupa penipuan, pencurian data maupun penyebaran berita palsu yang marak di kalangan masyarakat. Dalam penelitian ini dilakukan observasi dan pengumpulan data dari ibu rumah tangga serta remaja pengguna internet di Desa Jrebeng melalui penyebaran kuisioner untuk mengetahui tingkat kesadaran pengguna terhadap keamanan informasi. Pengukuran tingkat kesadaran terhadap keamanan informasi dilakukan dengan memperhatikan tiga variabel KAB, yaitu Knowledge, Attitude dan Behaviour yang dijabarkan lebih lanjut dalam pengukuran skala likert.

Kata kunci : kesadaran keamanan informasi, ibu rumah tangga

ABSTRACT

The use of the internet is a common thing among housewives and teenagers, often housewives use the internet for various purposes, for example shopping or just for communication. Teens use the internet for entertainment or to do the school work. The easy use of the internet, let alone supported by the ease of having a smartphone, makes internet users increase. Along with increasing internet usage it also encourages internet crime in the form of fraud, data theft and the spread of fake news that is rife among the people. In this study observations and data collection from housewives and teenagers of internet users in Jrebeng village through questionnaires to determine the level of user awareness of information security. Measurement of the level of awareness of information security is done by taking into account the three KAB variables, namely Knowledge, Attitude and Behavior which are further elaborated in the measurement of the Likert scale.

***Keywords** : information security awareness, housewives, teenagers*

1. PENDAHULUAN

Penggunaan internet yang semakin meluas di kalangan remaja dan ibu rumah tangga tidak lantas baik – baik saja, karena dengan semakin meluasnya penggunaan internet maka keamanan informasi juga dipertaruhkan. Salah satu faktor penyebab terjadinya pencurian data facebook adalah karena pengguna dengan mudahnya menyebarkan data pribadi melalui aplikasi permainan yang ada dalam facebook itu sendiri. Kasus penipuan melalui jejaring

sosial juga sering terjadi. Dengan adanya kasus – kasus tersebut, maka diperlukan adanya langkah – langkah untuk penanganan permasalahan kesadaran terhadap keamanan informasi.

Ibu rumah tangga adalah benteng pertama di keluarga, karena ibu rumah tangga akan mengajarkan banyak hal pada anak – anak dan keluarga mereka termasuk tentang internet. Ibu rumah tangga di Desa Jrebeng memang masih beragam, belum semua ibu rumah tangga menggunakan telepon pintar dan mengenal internet, tetapi putra putri mereka mulai mengenal internet dan menggunakan gawai dalam kesehariannya, karena itu pengetahuan terhadap keamanan informasi juga dibutuhkan oleh ibu rumah tangga.
Pengukuran tingkat kesadaran terhadap keamanan informasi menjadi penting dikarenakan dengan mengetahui tingkat kesadaran terhadap keamanan informasi tersebut, maka dapat dilakukan langkah selanjutnya untuk memberikan pelatihan atau penyuluhan tentang pentingnya keamanan informasi.

Dalam menghadapi usaha perolehan informasi secara ilegal, orang-orang berusaha mencegah tindak kriminal terkait informasi atau berusaha meminimalisasi kerusakan akibat tindak kriminal tersebut. Inilah yang disebut dengan keamanan informasi. Sederhananya, keamanan informasi menghargai nilai informasi dan melindunginya. Terkait keamanan informasi, dikenal istilah 4R keamanan informasi yakni*: Right Information* (Informasi yang benar), *Right People* (Orang yang tepat), *Right Time* (Waktu yang tepat) dan *Right Form* (Bentuk yang tepat). Pengaturan 4R adalah cara paling efisien untuk memelihara dan mengontrol nilai informasi. *Right Information* mengacu pada ketepatan dan kelengkapan informasi yang menjamin integritas informasi. *Right People* berarti informasi tersedia hanya bagi individu yang berhak yang menjamin kerahasiaan. *Right Time* mengacu pada aksesibilitas informasi dan penggunaannya atas permintaan entitas yang berhak, ini menjamin ketersediaan. Sedangkan *Right Form* mengacu pada penyediaan informasi dalam format yang tepat. Untuk menjaga keamanan informasi, 4R harus digunakan dengan tepat. Ini berarti bahwa kerahasiaan, integritas dan ketersediaan haruslah ditinjau ketika menangani informasi.

A. *Konsep Keamanan Informasi*

Ada beberapa konsep keamanan informasi yang dipaparkan oleh Chan dan Mubarak (2011) yang antara lain:

1. *Phishing*. Phising adalah usaha untuk mendapatkan informasi rahasia atau melakukan pencurian identitas dengan menggunakan e-mail atau website palsu yang meniru alamat situs atau alamat e-mail yang sebenarnya. Phising juga dilakukan dengan caracara non-teknis seperti *Social Engineering* atau dilakukan bersama dengan *Spam* (akan dibahas di bagian berikutnya) sebagai modus untuk melakukan phising. Phising merupakan ancaman umum terhadap aspek kerahasiaan keamanan informasi dan karena itu penting bagi karyawan untuk menyadari konsep dan bahayanya.

2. *Spam*.
Spam adalah surat atau pesan elektronik komersial yang tidak diinginkan oleh penerimanya. Mungkin tampak sepele, namun *Spam* bukan hanya mengganggu penerima namun berpotensi menimbulkan bencana atau mengganggu sistem. Sebagai contoh, kode berbahaya seperti virus atau trojan sering menggunakan *Spam* sebagai kendaraan untuk distribusi. Kode berbahaya dapat mengurangi performansi sistem dan membatasi akses ke pengguna, sehingga melanggar aspek ketersediaan informasi. Sealin itu dalam pesan *Spam*, terkadang memuat link yang

mengarahkan ke situs phising. Sementara kontrol teknis yang diterapkan organisasi untuk mencegah *Spam* memasuki sistem e-mail organisassi mungkin tidak dapat mengatasi 100%. Oleh karena itu, penting baki karyawan atau individu untuk menyadari konsep *Spam* dan bahaya yang terkait.

3. *Social Engineering*. Dalam konteks keamanan informasi, *Social Engineering* adalah penggunaan sarana non-teknis untuk melakukan pencurian identitas atau untuk memperoleh informasi rahasia. Penyerang dalam hal ini dapat menggunakan kombinasi dari manipulasi psikologis dan peniruan dalam rangka mendorong korban tidak bersedia dalam menyediakan informasi rahasia. Karena aspek yang sangat manusiawi dari *Social Engineering* tidak mungkin untuk mencegah serangan menggunakan kontrol teknis.

4. *Strong Password*. Password adalah kunci untuk otentikasi pengguna dan untuk mencegah akses tidak sah kedalam sistem. Selain *Social Engineering* dan praktek phising, password dapat diperoleh secara ilegal dengan menggunakan dua jensi serangan yang dikenal sebagai *password cracking*. Bukan masalahh apakah password dapat dipecahkan atau tidak, melainkan berapa lawa waku yang dibutuhkan untuk memecahkan kombinasi password tersebut. Semakin kuat sebuah password maka semakin lama waktu yang dibutuhkan untuk memecahkannya. Password yang kuat akan mengurangi kemungkinan serangan password dilakukan oleh penyerang. Kontrol teknis yang ada sudah mumpuni untuk membuat password yang kuat, namun tidak semua sistem informasi memiliki kontrol tersebut, oleh karena itu perlu kesadaran karyawan untuk meyakini bahwa password mereka cukup kuat. Pengetahuan mengenai konsep passsword ini menjadi sangat penting. Password yang kuat harus terdiri dari kombinasi yang cukup panjang antara huruf, angka dan simbol.

5. *Data or Information Integrity*. Integritas data dan informasi yang berkaitan dengan aspek integritas keamanan informasi memiliki ciri berikut:

a. Akurasi dan kebenaran, yaitu informasi harus kuat dan benar dalam artian data harus tepat dan sesuai dengan kenyataan, misalnya data tanggal lahir yang diinputkan ke d alam sistem tidak boleh memiliki ruang kemungkinan kesalahan.

b. Kepercayaan, memastikan akurasi dan kebenaran akan memastikan bahwa informasi yang tersimpan dalam sistem adalah representasi dari kenyataan sehingga seseorang dapat mempercayai informasi tersebut.

c. Keberlakuan dan ketepatan waktu, menggunakan tanggal lahir sebagai contoh, tanggal pasti kelahiran adalah variabel yang berubah dari waktu ke waktu. Informasi keberlakuan dipengaruhi oleh perubahan kenyataan dari waktu ke waktu dan harus dipenuhi.

6. *Social Networking*. Pendapat bahwa media sosial atau situs jejaring seperti Facebook dan Twitter sebagai sumber bocornya informasi rahasia sudah semakin relevan beberapa tahun terakhir ini. Media sosial dapat menjadi sumber kebocoran data ketika karyawan mengungkapkan informasi pribadi dan informasi yang berkaitan dengan tempat kerja di situs media sosial. Oleh karena itu, media sosial merupakan bagian penting untuk setiap rencana keamanan atau kebijakan. Kesadaran akan bahaya jejaring sosial dalam kaitannya dengan keamanan informasi sangatlah penting

B. *Kesadaran Keamanan Informasi*

Keamanan sistem informasi tidak hanya melibatkan kontrol keamanan teknis, namun juga melibatkan kontrol administratif, prosedural dan manajerial

(Papagiannakis, Pijl, & Visser, 2011). Cara pengguna (karyawan, manajer, personel IT) dalam menggunakan sistem informasi organisasi memainkan peranan penting dalam menjaga kelangsungan asset informasi perusahaan. Kesadaran keamanan adalah bidang ilmu keamanan yang berhubungan erat dengan faktor manusia mengenai keamanan aset informasi. Pengetahuan yang diperoleh dari sekolah adalah elemen utama untuk menciptakan kesadaran keamanan. Sangat penting untuk mengimplementasikan peraturan keamanan. *Chief Security Officer* bertanggung jawab untuk melakukan program pembelajaran dan atau mengimplementasikan elemen keamanan pada program pembelajaran Teknologi Informasi.

2. METODE PENELITIAN

Jenis penelitian yang digunakan adalah penelitian kuantitatif dimana data dikumpulkan dengan menggunakan kuesioner. Responden adalah remaja dan ibu rumah tangga yang menggunakan internet. Jumlah total responden adalah 75 orang yang terdiri dari 35 orang remaja putra dan putri serta 40 orang ibu rumah tangga. Penelitian ini menggunakan *attitude, knowledge* dan *behavior* dalam perspektif penggunaan *internet*. Beberapa pertanyaan dijawab dalam skala 3 poin yaitu setuju, tidak tahu dan tidak setuju (dimensi *attitude* dan *knowledge*), sementara yang lain hanya membutuhkan jawaban yang setuju atau tidak setuju. (dimensi *behavior*). Contoh pertanyaan yang diajukan dapat dilihat di Tabel 1. Kuesioner disebar secara offline

Tabel 1. Contoh Pertanyaan

Dimensi	Pertanyaan	Jawaban
Attitude	Saya mempertimbangkan sisi keamanan saat saya mengakses internet	1. Setuju 2. Tidak Tahu 3. Tidak Setuju
Knowledge	Jika saya tidak mempertimbangkan keamanan, saya bisa mengalami gangguan keamanan	1. Setuju 2. Tidak Tahu 3. Tidak Setuju
Behaviour	Saya selalu mempertimbangkan keamanan sebelum mengakses halaman tertentu	1. Setuju 2. Tidak Tahu 3. Tidak Setuju

Variabel operasional dalam penelitian ini terdiri
dari tiga dimensi, yaitu pengetahuan (apa yang
mereka ketahui tentang keamanan dan privasi), Sikap (bagaimana perasaan mereka tentang keamanan dan privasi), dan perilaku (apa yang mereka lakukan terhadap keamanan dan privasi)

Kerangka pemikiran dari penilitian ini menggunakan model Krueger dan Kerney (2006) yang mengadaptasi teori psikologi sosial yang mengusulkan tiga komponen untuk mengukur cara yang menguntungkan atau tidak menguntungkan terhadap objek tertentu. Komponen tersebut digunakan untuk mengembangkan tiga dimensi yang dikenal sebagai *knowledge* (pengetahuan seseorang), *attitude* (sikap seseorang) dan *behaviour* (perilaku seseorang. Dimensi *knowledge* digunakan untuk mengetahui bagaimana pengetahuan pengguna. Sedangkan Dimensi *attitude* digunakan untuk mengetahui bagaimana sikap pengguna dan dimensi *behaviour* untuk mengetahui hal-hal yang dapat dilakukan oleh pengguna.

Kerangka pemikiran kesadaran keamanan informasi menggunakan model Krueger dan Kerney (2006) untuk mengukur tingkat kesadaran terhadap keamanan informasi.

3. HASIL PENELITIAN

Dari kuisioner yang diberikan kepada ibu rumah tangga dan remaja di Desa
Jrebeng, didapatkan hasil sebagai berikut:

Tabel 2. Jenis kelamin responden

No	Jenis kelamin	Jumlah
1	Perempuan	60 %
2	Laki laki	40

Pada tabel 2 menggambarkan perbandingan jumlah responden berdasarkan jenis kelamin, dimana responden perempuan lebih banyak dibandingkan dengan responden laki – laki. Para ibu rumah tangga menggunakan internet melalui perangkat telepon pintar yang dimiliki. Untuk rentang usia dari responden, ditampilkan pada tabel 3.

No	Rentang Usia	Jumlah
1	<18 tahun	0
2	18 – 25 tahu	24
3	25 – 35 tahun	33
4	35 – 50 tahun	18

Untuk hasil dari kuesioner yang sudah disebarkan, dituliskan pada tabel – tabel berikut:
Rata – rata responden mengalami gangguan keamanan berupa SMS iklan maupun SMS tak dikenal. Dari semua responden, sebanyak 75% menyatakan pernah mendapatkan SMS tak dikenal ataupun SMS iklan.

Responden menggunakan telepon pintar untuk chatting, sosial media, membaca berita dan bermain game. Aplikasi yang dipasang di telepon pintar responden seringkali menampilkan iklan dan responden merasa bahwa iklan – iklan tersebut mengganggu. Sebagian responden tidak memperhatikan peringatan ketika akan memasang aplikasi baru di telepon pintar mereka. Hal tersebut menunjukkan attitude terhadap kesadaran terhadap keamanan informasi dan privasi masih kurang. Peringatan untuk permintaan akses ke dalam data yang ada di telepon pintar selalu diberikan ketika akan memasang aplikasi baru, tetapi peringatan tersebut sering diabaikan karena keinginan untuk segera menggunakan aplikasi. Padahal, dalam peringatan tersebut terkadang tertulis permintaan untuk mengakses data – data pribadi dari pengguna. Dari keseluruhan responden, hanya 35% responden yang memperhatikan, sedangkan 65% lainnya tidak memperhatikan.

Responden juga menyatakan bahwa mereka dapat memasang aplikasi pada telepon pintar mereka meskipun tidak berasal dari Google Play Store. Hal tersebut mengurangi tingkat keamanan pengguna, karena aplikasi yang tidak didapatkan secara resmi dari Google Play Store tidak dapat dijamin keamanannya. Sebanyak 60% responden menyatakan bahwa mereka masih mengijinkan untuk memasang aplikasi yang bersumber selain dari Google Play Store.

4. KESIMPULAN DAN SARAN

Dari hasil penelitian yang telah dilakukan di Desa Jrebeng, didapatkan kesimpulan bahwa kesadaran terhadap keamanan informasi masih rendah. Hal tersebut ditunjukkan dari kurangnya kesadaran untuk mengamankan diri dari aplikasi yang kurang bisa dipercaya sehingga informasi pribadi dapat diambil dan tersebar.

5. UCAPAN TERIMAKASIH

Peneliti mengucapkan terima kasih kepada Lembaga Penelitian dan Pengabdian Masyarakat Universitas 17 Agustus 1945 Surabaya atas dukungannya terhadap penelitian ini.

6. DAFTAR PUSTAKA

KRUGER, H., & KEARNEY, W. (2006). A PROTOYPE FOR ASSESSING INFORMATION SECURITY AWARENESS. *ELSEVIER*, 289 - 296.