Jurnal Serina Sains, Teknik dan Kedokteran
Vol. 1, No. 1, Feb 2023 : hlm 211-216 ISSN-L 2986-5204 (Versi Elektronik)

KESADARAN DAN KEPEKAAN MASYARAKAT TERHADAP ATURAN MENJAGA PRIVASI DAN DATA PENTING DALAM MENGGUNAKAN INTERNET

Ernestito Jovian[1], Mohammad Faraditya Eka Putra[2], Orlando Claudio[3], Manatap Sitorus[4]

[1]Jurusan Sistem Informasi, Universitas Tarumanagara
Email: inestjovian@gmail.com
[2]Jurusan Sistem Informasi, Universitas Tarumanagara
Email: mohammadfaraditya@gmail.com
[3]Jurusan Sistem Informasi, Universitas Tarumanagara
Email: orlando.825200021@stu.untar.ac.id
[4]Fakultas Teknologi Informasi, Universitas Tarumanagara
Email: manataps@fti.untar.ac.id

Masuk : 05-12-2022, revisi: 15-12-2022, diterima untuk diterbitkan : 20-12-2022

ABSTRAK

Seiring berkembangnya dunia digital, semakin banyak teknologi yang digunakan dalam masyarakat. Pengguna dari teknologi tentunya akan terus berkembang. Oleh karena itu, tidak sedikit orang yang memiliki tujuan buruk dan mengeksploitasi orang-orang yang masih awam di bidang tersebut. Penelitian ini bertujuan untuk menganalisis pengetahuan masyarakat umum mengenai hak privasi yang dimiliki oleh setiap masyarakat. Sebagian besar masyarakat pengguna internet masih belum memahami pentingnya data pribadi yang riskan dicuri oleh beberapa pihak yang tidak bertanggung jawab. Hal ini tentunya dapat merugikan masyarakat, bahkan dapat membahayakan pengguna internet. Melalui penelitian ini diharapkan dapat mengetahui tentang kepekaan masyarakat dalam menjaga data privasi dan juga respon pengguna internet terhadap penelitian. Ancaman yang sangat nyata ini merupakan ancaman yang bersifat universal. Ancaman ini tentu saja telah menyerang masyarakat Indonesia dengan luas baik masyarakat umum dan juga pemerintahan. Belakangan ini contoh beberapa ancaman yang terjadi di pemerintah seperti salah satu peretas membocorkan dan mengantongi 26 juta history browsing pelanggan IndiHome, Kebocoran 1,3 data registrasi SIM Card, kebocoran data KPU, dan juga daftar surat ke Presiden Indonesia.Tentu saja data-data yang sangat krusial ini menjadi sebuah bukti bahwa ancaman dibidang ini sudah merupakan ancaman tingkat tinggi dan perlu ditangani segera baik. Dalam penelitian ini akan membahas dalam skala besar maupun skala kecil.

Kata kunci: Privasi, Pencurian, Internet, Data Pribadi, Ancaman.

ABSTRACT

As the digital world develops, the more technology it is certainly used by the public. The user from the technology naturally will continue to grow. Therefore, many people have bad purposes and exploit many people that are still new in the field of internet. This study's purpose is to analyze the general public's knowledge of the privacy rights that each person has. Most people that use the internet still do not know about the importance of their personal data that is at risk to be stolen by irresponsible people. This case of course can be detrimental to many people in the environment, can even be dangerous for them. Through this research, our group wanted to find out about people's sensitivity in protecting data privacy and also their response to research. This very real threat is a universal threat. This threat, of course, has attacked the Indonesian people at large, both the general public and the government. Lately there have been a few threats that occur in the government like one of the hackers that hacked and took 26 million history browsers from an indihome user customer. 1.3 SIM Card registration data leaks, KPU data leaks, and also a list of letters to the President of Indonesia. Of course, the data that is very crucial becomes proof that the threat in this field has already become a high-level threat and needs to be handled as well as possible. In this research we will discuss on a small scale or big scale.

Keywords*: Privacy, Theft, Internet, Personal Data, threat*

1. PENDAHULUAN

Isu tentang pentingnya melindungi hak privasi di Indonesia dalam beberapa tahun terakhir, jumlah pengguna ponsel dan internet telah meningkat. Pemilihan topik ini tentu saja karena beberapa dari yang terkena dampak dari kasus ini. Pengambilan topik ini adalah untuk mencari tahu seberapa sadar dari lingkungan sekitar kita dan seberapa waspadanya pengguna internet terhadap pengambilan data digital dan juga pencurian data pribadi. Banyak kasus yang mengemuka terutama terkait dengan hilangnya data pribadi seseorang yang mengarah pada kecurangan semakin memperkuat wacana tentang urgensi penguatan melindungi hak atas pengguna internet atas privasinya.

Oleh karena itu masyarakat perlu mendapat himbauan berlebih tentang menjaga data privasi pada saat sedang menggunakan internet. Tentu saja negara ini harus merencanakan reformasi baik secara paradigma maupun politik. Tantangan baru ini bertujuan untuk memastikan privasi melindungi semua warganya. Kesadaran pemerintahan Indonesia dalam mengamankan ancaman dunia digital masih belum memadai dan juga belum siap tanggap dalam mengatasi masalah seperti ini karena masih dianggap masalah kecil dan juga sepele. Sampai pada pertengahan tahun kemarin seorang hacker yang memiliki nama samaran "Bjorka" melakukan pembobolan identitas dan juga data pengguna dalam skala yang sangat besar akhirnya menyadarkan masyarakat dan juga pemerintahan terhadap ancaman "semu" yang nyata ini.

Berdasarkan latar belakang, maka peneliti merumuskan masalah sebagai berikut: (a) bagaimana tingkat kesadaran masyarakat di indonesia dalam menggunakan internet?;

(b) langkah-langkah apa saja yang dibutuhkan untuk menjaga kesadaran masyarakat di indonesia untuk lebih bijak dalam pemanfaatan penggunaan internet?; (c) apakah tujuan dari penelitian ini adalah untuk mengetahui tingkat kesadaran masyarakat indonesia dalam menggunakan internet ?

2. METODE PENELITIAN

Penelitian akan menggunakan metode penelitian kuantitatif. Data dalam penelitian ini akan diperoleh melalui jawaban responden dari Google Forms yang disebarkan dan berisikan pertanyaan terkait dengan topik. Total responden yang akan diambil berjumlah 30 responden. Dalam penelitian ini akan mencari responden yang berumur minimal 17 tahun dan pengguna internet. Untuk hasil akhir, diharapkan untuk masyarakat luas untuk lebih mengetahui pentingnya privasi pribadi di internet dan lebih waspada terhadap ancaman yang ada di dunia maya.

3. HASIL DAN PEMBAHASAN

Tabel 1.

No	Pertanyaan	*Yes*	*No*
1.	Apakah anda tahu bahwa OTP(One Time Password) tidak boleh dibagikan kepada siapapun?	83.9%	16.1%
2.	Apakah anda pernah membuka link dari orang yang tidak dikenali ?	60%	40%
3.	Apakah anda tahu resiko jika membuka link phising ?	77.4%	22.6%
4.	Apakah anda sadar bahwa setiap data yang anda masukan melalui Internet tidak dapat ditarik kembali ?	61.3%	38.7%
5.	Tahukah Anda bahwa data diri tidak boleh disebarluaskan secara sembarangan, khususnya pada form yang terkoneksi pada internet?	74.2%	25.8%

https://doi.org/10.24912/jsstk.v1n1.27156

No	Pertanyaan	*Yes*	*No*
6.	Apakah anda pernah melakukan registrasi menggunakan nomor telepon anda pada website tertentu?	67.7%	32.3%
7.	Apakah anda sudah waspada terhadap cyber crime yang terjadi di dunia internet sekarang ini?	74.2%	25,8%
8.	Apakah kalian sudah tahu bahwa Undang-Undang Perlindungan Data Pribadi sudah disahkan baru-baru ini ?	46,7%	53.3%
9.	Apakah kalian sudah melakukan perlindungan data terhadap NIK sendiri sesuai dengan anjuran kominfo ketika data nik kita bocor?	50%	50%
10.	Seberapa tahu anda soal privacy breach in di internet?	43.3% Menjawab netral	10% Menjawab sangat paham
11.	Apakah anda termasuk orang yang awam terhadap istilah privacy breaching?	63.9%	36.1%
12.	Apakah akun yang anda miliki sekarang sudah memiliki keamanan ber autentifikasi yang berlapis?	80.6%	19.4%
13.	Apakah anda menggunakan mode incognito ketika menggunakan internet di luar ?	27.8%	73.2%
14.	Apakah anda pernah menggunakan VPN untuk menggunakan website ilegal ?	50%	50%
15.	Apakah anda sudah mengetahui resiko pada saat menggunakan VPN ? Terutama yang tidak berbayar.	61.1%	38.9%

Penjelasan Hasil Penelitian

Nomor 1

Menurut pertanyaan pertama sebagian besar responden telah mengerti link OTP tidak boleh dibagikan dengan siapapun, tetapi masih ada sebagian kecil responden masih berani membagikan link OTP yang tentu saja berbahaya bagi pengguna. Dikarenakan mungkin beberapa orang masih belum mengerti apa yang dimaksud dari one time password dan juga mungkin penerima pesan tidak membaca full dari deskripsi saat menerima pesan.

Nomor 2

Berdasarkan hasil digambar kedua, hampir setengah dari responden masih mau membuka link dari kontak orang yang tidak dikenal. Hal itu merupakan hal yang cukup berbahaya untuk dilakukan karena link dapat membawa virus ataupun dapat melakukan pencurian data. Dikarenakan mungkin responden tidak mengerti akan resiko dari membuka link dari pihak asing akan membawa dampak lebih. Sehingga lebih menyepelekan dan asal membuka saat menerima link.

Nomor 3

Sebagian dari responden sudah mengerti resiko dari link phising, tetapi masih ada yang mungkin belum mengerti apa yang dimaksud dari phising sendiri sehingga tidak dapat mengerti resiko dari membuka link phising,dikarenakan mungkin istilah bahasa asing masih jarang didengar di telinga responden dan juga kurangnya literasi responden.

Nomor 4

Menurut penelitian nomor 4 sebagian besar dari responden mengerti resiko dari data yang sudah dikirim tidak dapat ditarik kembali tetapi masih 38.7% responden belum memahami dari resiko

mengirim data pribadi ke internet. Mengirim data secara tidak berhati-hati dapat menyebabkan bocornya data pribadi dan bocornya informasi penting, apabila terjadi kebocoran data tentu saja identitas dapat diperjualbelikan dan tentu saja ini terjadi karena tidak diketahuinya resiko dari melakukan input data di tempat yang meragukan.

Nomor 5

Sebanyak 74.2% mengerti bahwa data pribadi tidak boleh disebarluaskan di internet. Tetapi tetap ada 25.8% yang masih belum mengerti dampak dari bocornya data pribadi apabila memberikan data pribadi di form online. Tentu saja ini masih terjadi karena ketidaktahuan dari resiko dari membeberkan data pribadi online apalagi di form-form yang tidak jelas sumbernya.

Nomor 6

Berdasarkan hasil jawaban dari responden sebagian besar pernah melakukan registrasi menggunakan nomor telepon di website tertentu. Biasanya website membutuhkan informasi data nomor telepon ketika pembuatan akun karena di akun tersebut berisi data-data customer misalkan website e-commerce karena membutuhkan alamat serta nomor telepon untuk pengiriman barang.

Nomor 7

Cyber Crime pada tahun ini sering terjadi terutama kasus Bjorka yang mencuri data warga indonesia dan dijual di forum tertentu. Hal ini yang menyebabkan masyarakat indonesia marah kepada kominfo karena dikatakan data kita aman. Sebenarnya kita juga harus bisa waspada terhadap cyber crime seperti jangan pernah melakukan tindakan ilegal. Menurut hasil jawaban responden sebanyak 74.2% sudah waspada terhadap serangan Cyber Crime yang bisa terjadi kapan saja dan sisanya sebanyak 25.8% menjawab tidak waspada terhadap serangan Cyber Crime.

Nomor 8

Kasus Cyber Crime yang baru terjadi membuat heboh seluruh masyarakat Indonesia Karena kasus ini DPR RI langsung melakukan pengesahan Undang-Undang perlindungan data pribadi agar bisa ditindak pidanakan karena sebelum pengesahan Undang-Undang banyak kasus Cyber Crime yang lewat begitu saja tidak ada tindak pidananya. Karena pengesahan Undang-Undang yang dianggap telat dan kurang informatif membuat sebagian besar responden menjawab tidak tahu tentang pengesahan Undang-Undang perlindungan data pribadi.

Nomor 9

Kasus Bjorka membuat heboh seluruh masyarakat Indonesia dengan kebocoran data NIK masyarakat Indonesia dan Kominfo selaku yang menyimpan data NIK masyarakat indonesia membuat pernyataan yang bikin geram masyarakat Indonesia yaitu disuruh menjaga NIK secara masing-masing hal ini membuat masyarakat bertanya terus gunanya Kominfo apa. Sebagian responden menjawab sudah menjaga NIK sesuai anjuran Kominfo dan sebagiannya lagi belum.

Nomor 10

Pelanggaran privasi terjadi ketika ada akses tidak sah ke pengumpulan, penggunaan, atau pengungkapan informasi. Beberapa contoh pelanggaran privasi yang paling umum terjadi ketika informasi pribadi pasien, pelanggan, atau klien dicuri, hilang, atau diungkapkan secara keliru. Sebagian besar responden menjawab netral.

 https://doi.org/10.24912/jsstk.v1n1.27156

Nomor 11

Privacy Breaching terjadi ketika informasi pribadi dicuri atau hilang dan digunakan tanpa izin dari pemilik akun itu sendiri. Namun masih lumayan banyak responden yang masi awam terhadap istilah tersebut.

Nomor 12

Pada zaman sekarang ini semua orang akan sangat memerlukan pengamanan ekstra untuk akun pribadi sendiri agar tercegah dari oknum-oknum yang menyalahgunakan kemampuan khusus untuk hal yang kurang baik, dan disini para responden sebagian besar sudah memiliki keamanan ber autentifikasi yang berlapis.

Nomor 13

Mode incognito akhir-akhir ini cukup berguna ketika pengguna sedang ingin melakukan pencarian dalam internet yang bersifat lebih privat atau ketika sedang berada di luar rumah yang akan membuat user tidak terdetect dan tidak meninggalkan jejak riwayat pencarian. Namun masih lumayan banyak dari para responden yang tidak menggunakan mode incognito pada saat menggunakan internet di luar.

Nomor 14

VPN atau Virtual Private Network ini berguna untuk menyamarkan alamat IP dan mengenkripsi traffic internet ketika user menggunakanya yang mana akhirnya dapat memberikan user akses untuk membuka alamat atau konten yang diblokir di wilayah user akan dapat terbuka dengan aman.

Nomor 15

Pada saat ini sudah lumayan banyak responden yang mengetahui lebih lanjut tentang resiko berbahaya ketika menggunakan internet dengan menggunakan VPN terutama yang tidak berbayar karena VPN ini dapat memberikan serangan virus malware dari pihak yang tidak bertanggung jawab yang dapat memunculkan iklan-iklan yang tidak jelas terhadap device user.

Meskipun data pribadi dilindungi undang-undang, namun perlindungan data pribadi masih tersebar luas. Mengutip Pusat Keamanan Siber Australia, keamanan informasi dapat terjadi melalui penggunaan media sosial, yaitu ketika pengguna media sosial itu sendiri memberikan informasi pribadinya. Penyebaran informasi pribadi melalui media sosial seringkali mengarah pada kejahatan digital seperti pencurian identitas, penguntit, dan cyberbullying. Informasi pribadi yang tersebar di media sosial dapat memudahkan peretas untuk meretas akun seseorang. Hal ini dikarenakan beberapa peretas profesional memiliki keahlian untuk menggunakan banyak jenis data, meskipun hanya sebatas tempat dan tanggal lahir, untuk meretas akun seseorang. Oleh karena itu, informasi yang ada di dalam KTP, meskipun hanya sebatas informasi terkait tempat dan tanggal lahir, akan sangat berbahaya jika disebarluaskan.

Berdasarkan penelitian dan hasil survey yang dilakukan bahwa masih banyak yang belum paham dan mengerti resiko dari memberikan data dengan tidak dipikir dua kali berikut adalah beberapa tips mengenai yang seharusnya dilakukan saat berinteraksi dengan identitas pribadi:

a) Kode OTP sama halnya seperti kunci rumah. Bahkan, mereka yang mengatasnamakan institusi seharusnya tidak akan meminta kode OTP.

b) Kominfo menghimbau masyarakat agar waspada jika ada yang meminta kode OTP melalui email, aplikasi chat, telepon maupun SMS dari mereka yang mengaku sebagai suatu institusi resmi.
c) Selain itu, Kominfo juga memperingatkan masyarakat agar selalu waspada terhadap situs palsu atau phising dan penipuan dengan menggunakan fitur penerusan panggilan (call forwarding).
d) Tolak jika ada yang meminta untuk menekan *kode* nomor pengganti. Bisa jadi itu adalah penipuan menggunakan fitur penerusan panggilan untuk mengirimkan data telepon dan sms user pada pelaku," saran Kominfo.
e) Perlu diingat pelaku kejahatan akan berusaha dengan berbagai cara untuk memperoleh kode rahasia OTP user, baik melalui penipuan (social engineering) dan peretasan (hacking) sebagai sarana untuk mengeksploitasi uang elektronik atau uang yang tersimpan pada m-Banking.

Diatas merupakan langkah pencegahan mengenai penipuan yang bersangkutan dengan OTP. Juga para user harus lebih memperhatikan keamanan pada saat menggunakan browser. Serta selalu memperhatikan jika ada kode atau pesan yang masuk secara tidak diketahui oleh user agar menghindari kasus yang tidak diinginkan.

REFERENSI

Diah, S. (2021). Perlindungan Hukum Terhadap Hak Privasi Konsumen Dalam Pinjam Meminjam Online Ilegal *(Financial Technology Peer To Peer (P2p) Lending)* (*Doctoral dissertation*, Universitas Wijaya Putra)

Ishaq, M. (2020). Perlindungan hukum pembocoran identitas pribadi debitur oleh kreditur dalam layanan pinjaman *online* perspektif hukum positif dan hukum Islam: Studi di media konsumen. (*Doctoral dissertation*, Universitas Islam Negeri Maulana Malik Ibrahim).

Nafi'ah, R. (2020). Pelanggaran Data Dan Pencurian Identitas Pada E-Commerce. *Cyber Security dan Forensik Digital*, *3*(1), 7-13.

Nurdiani, I. P. (2020). Pencurian Identitas Digital Sebagai Bentuk Cyber Related Crime. *Jurnal Kriminologi Indonesia*, *16*(2).

Puspandari, R. Y. (2021). Kesadaran Hukum Masyarakat Dalam Memanfaatkan Media Sosial (Studi Terhadap Generasi Z di Kota Magelang). *Humani (Hukum Dan Masyarakat Madani), 11*(1), 11-22.

Sanjaya, R., & Irwansyah, I. (2019). Etika Dan Privasi Layanan Jasa Teknologi Finansial: Studi Fenomenologi Pada Korban Pelanggaran Privasi. *Journal Communication Spectrum: Capturing New Perspectives in Communication*, *9*(1), 14-29.

Soewardi, B. A. (2013). Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia. *Media Informasi Ditjen Pothan Menhan*, 31-35.

Sudama, I. W., Imanto, M. A., Wijayanti, S. W., Agustini, T. Y., & Fatoni, Z. (2021). Pengaruh Risiko Pencurian Identitas dan Persepsi atas Risiko terhadap Niat Belanja Online. *Indonesian Business Review*, *3*(2), 180-218.

Sulis Rudatin, N. (2018). Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit. *Jurnal Ilmiah Hukum Dirgantara*, *9*(1).

Syafrina, A. E. (2018). Privacy Threats In Big Data. *Jurnal Penelitian Komunikasi Dan Opini Publik, 22*(2).

 https://doi.org/10.24912/jsstk.v1n1.27156