KESADARAN ANCAMAN PRIVASI SERTA PERILAKU PERLINDUNGAN PRIVASI DALAM MENGGUNAKAN SOSIAL MEDIA

INFORMATION SECURITY AWARENESS AND PRIVACY PROTECTION BEHAVIOR IN USING SOCIAL MEDIA

Leona Elsa N.1, Anisa Nur C.2,Ni Putu Jeanny M.3 , Aisha Ramadhana I. S.4
E-mail : [1)]19082010004@upnjatim.ac.id , [2)] 19082010012@upnjatim.ac.id ,
[3)]19082010057@upnjatim.ac.id, [4)] 19082010109@upnjatim.ac.id

[1,2,3,4]Sistem Informasi, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jawa Timur

Abstrak

Banyak pengguna internet khususnya pengguna sosial media tidak menyadari banyaknya ancaman dan berbagai risiko yang dapat melanggar keamanan privasi dan pencurian identitas. Hal ini dikarenakan para pengguna sosial media yang kerap mengekspos detail pribadi tentang diri mereka sendiri. Informasi ini, jika dimasukkan ke tangan yang salah, dapat digunakan untuk merugikan pengguna baik secara virtual dunia dan di dunia nyata. Beberapa ancaman yang dapat mengancap data pribadi seperti *malware, phising attack, spamming, internet fraud, clickjacking* tidak dapat kita hindari. Berdasarkan beberapa penelitian terdahulu membuktikan tingkat kesadaran akan hal ini sebenarnya sudah cukup tinggi, namun mereka yang sadar terkadang belum bertindak untuk melindungi data privasi mereka. Oleh karena itu pengguna perlu melakukan perlindungan terhadap data privasi kita sendiri saat menggunakan sosial media. Selalu pahami kebijakan privasi sebelum menggunakan sosial media dan senantiasa melindungi privasi diri dengan membatasi konten-konten yang diposting dalam sosial media.
Kata kunci : *privasi, keamanan, informasi, sosial media*

Abstract

Many internet users, especially social media users, are not aware of the many threats and risks that can violate privacy security and identity theft. This is because social media users often expose personal details about themselves. This information, if entered into the wrong hands, can be used to harm users in both the virtual world and the real world. Some threats that can threaten personal data such as malware, phishing attacks, spamming, internet fraud, clickjacking cannot be avoided. Based on recent research The level of awareness of this is actually quite high, but those who are aware sometimes do not act to protect their privacy data. Therefore, users need to protect our own privacy data when using social media. Always understand the privacy policy before using social media and always protect your privacy by limiting the content posted on social media.
Keyword : *privacy, security, information, social media*

1. PENDAHULUAN

Dalam kesehariannya manusia pasti tidak pernah luput dari yang namanya penggunaan teknologi. Menurut survei Hootsuire oleh We Are Social terhitung hingga Januari 2021 pengguna internet mencapai 4,6 milyar (Hootsuite, 2021), hal ini berarti lebih dari setengah penduduk di seluruh dunia telah mengenal internet. Jumlah ini tentunya meningkat dari tahun ke tahun. Meningkatnya pengguna internet juga memberi dampak meningkatnya risiko terhadap privasi yang dapat mengancam informasi pribadi. Berdasarkan laporan U.S. Identity Theft: The Stark Reality yang dilakukan oleh Aite Group

terdapat peningkatan jumlah *cyber crime* khususnya pada ranah pencurian identitas meningkat 42% selama pandemi pada tahun 2020 hal ini menunjukkan bahwa pencurian identitas berkembang pesat dalam tingkat keparahan dan akan terus berkembang hingga metode otentikasi dan validasi baru diterapkan (Aite Group, 2020).

Kasus pencurian identitas sempat menjadi trending topik di Indonesia pada tahun 2020 lalu, salah satunya berasal dari platform *marketplace* terbesar di Indonesia , Tokopedia melaporkan bahwa mereka mengalami kebocoran data yang mempengaruhi 91 juta data pengguna dan dikabarkan bahwa data tersebut dijual di *dark web* (Waqas, 2020). Berita tentang pelanggaran keamanan menjadi tren paralel dalam masyarakat modern karena mereka memperburuk kekhawatiran tentang potensi pelanggaran privasi. Peningkatan ketergantungan pada teknologi untuk menyimpan dan mengomunikasikan informasi yang dapat diidentifikasi secara pribadi membuat pengguna teknologi menghadapi risiko privasi yang terus meningkat. Namun, para peneliti telah menemukan bahwa, tampaknya bertentangan dengan peningkatan masalah privasi, orang terus mengungkapkan volume informasi pribadi yang terus meningkat secara online dan tren ini tidak menunjukkan tanda-tanda penurunan (Barnes, 2006).

Statistik media sosial pada tahun 2021 menunjukkan bahwa pengguna Facebook berbagi lebih dari 300 juta gambar melalui platform jejaring sosial setiap hari (Stout, 2021). Mengingat jumlah foto dan video yang dibagikan di media sosial, jelas bahwa rata-rata orang lebih berisiko terhadap ancaman seperti pencurian identitas, penguntitan dunia maya, dan banyak lagi . Meningkatnya frekuensi insiden keamanan seiring dengan meningkatnya volume pengungkapan informasi yang dimediasi teknologi menimbulkan pertanyaan tentang bagaimana memotivasi pengguna teknologi untuk melindungi diri mereka sendiri (Ghazinour & Ponchak, 2017).

2. METODOLOGI

Penelitian ini menggunakan metode kajian literatur. Kajian literatur adalah survei artikel ilmiah, buku, dan sumber lain yang relevan dengan masalah tertentu, bidang penelitian, atau teori, dan dengan demikian, memberikan deskripsi, ringkasan, dan evaluasi kritis dari karya-karya ini. Kajian literatur dirancang untuk memberikan gambaran umum tentang sumber yang telah dijelajahi saat meneliti topik tertentu dan untuk menunjukkan kepada pembaca bagaimana penelitian yang cocok dengan bidang studi yang lebih besar (Abdullah Ramdhani, Muhammad Ali Ramdhani, 2014). Berikut adalah tahapan yang dilakukan untuk penelitian dengan kajian literatur :

2.1 Menentukan Bidang Penelitian

Banyak bidang penelitian yang dapat dipilih untuk mulai melakukan penelitian. Sebaiknya disesuaikan dengan bidang yang diminati atau sedang dipelajari. Bidang yang dipilih pada penelitian ini adalah *Information Security*. Hal ini mengacu sesuai dengan mata kuliah yang diikuti oleh peneliti.

2.2 Menentukan Topik Penelitian

Melakukan pencarian menggunakan *search engine* seperti google merupakan salah satu cara untuk menentukan topik penelitian. Dengan melakukan pencarian pada laman penyedia jurnal seperti *google scholar, ScienceDirect.com, IEEE Explore,* dan lain-lain, dapat membantu kita mencari referensi untuk bidang penelitian yang kita ambil. Selain itu cara lain menentukan topik peneitian adalah dengan menemukan hasil atau data dari survei atau review paper. Dari beberapa paper yang telah peneliti temukan, dapat peneliti temukan bahwa pernggunaan media sosial menempati trend yang cukup tinggi dibarengi dengan ancaman keamanan dalam penggunaannya. Oleh karena itu topik penelitian ini adalah *computer in behaviour* dalam penggunaan sosial media.

2.3 Menentukan Masalah Penelitian

Setelah menentukan topik penelitian yang diambil, peneliti mencari lagi paper yang relevan dengan topik yang dipilih. Paper dapat dicari pada laman google scholar,

ScienceDirect.com, IEEE Explore, dan lain-lain. Dari paper yang ditemukan kemudian mencari referensi dari paper-paper tersebut. Setelah itu mendata masalah-masalah yang dibahas dalam paper tadi. Masalah yang dipilih kemudian dipilih lagi hingga menemukan satu atau dua penelitian yang menarik untuk dijadikan masalah penelitian. Berdasarkan topik yang dipilih ditemukan banyak masalah dalam hal ancaman yang ada pada sosial media dan kesadaran masyarakat dalam akan hal tersebut.

2.4 Menuliskan Hasil dan Kesimpulan

Tahap terakhir adalah menuliskan hasil yang didapat dari masalah yang sudah ditemukan berdasarkan paper dan referensi yang digunakan. Setelah dirangkum kemudian hasilnya ditulis dalam hasil dan pembahasan lalu dibuat kesimpulan pada akhir penelitian.

3. HASIL DAN PEMBAHASAN

3.1 Ancaman Keamanan Privasi di Sosial Media

Sosial media telah mengalami peningkatan pesat dalam jumlah pengguna, terutama dalam beberapa tahun terakhir (Gross et al., 2005). Menjadi saluran komunikasi yang kuat, sosial media telah menjadi alat yang populer untuk meningkatkan pengetahuan informasi di seluruh dunia dan memfasilitasi interaksi sosial. Selain itu, sosial media adalah alat yang ampuh untuk tetap terhubung dengan teman dan anggota keluarga. Selain itu, para pelaku bisnis dapat menggunakan sosial media dengan tujuan pemasaran dan periklanan dan untuk meningkatkan reputasi bisnis.

Meskipun media sosial dapat menjadi cara yang baik untuk terhubung dengan orang-orang dengan minat yang sama, jumlah pengguna sosial media yang terus meningkat menyebabkan semakin banyak data yang tersedia terkait dengan hubungan sosial. Ketersediaan sejumlah besar informasi pribadi telah menarik perhatian para pelaku kejahatan siber dan memotivasi mereka untuk memulai serangan terhadap media sosial dengan mendapatkan akses ke informasi yang dibagikan oleh pengguna. Oleh karena itu, privasi pengguna sosial media dapat terancam. Sosial media dapat menjadi alat yang membuka jalan baru bagi para penjahat dan peretas untuk melakukan aktivitas yang tidak diinginkan atau penipuan seperti spamming, penyerangan melalui virus, phishing, dll, yang seringkali berujung pada pencurian informasi dan identitas (Sepideh Deliri, 2015).

Menurut sebuah artikel di Computer Weekly tahun 2019, penjahat dunia maya menghasilkan $3,25 miliar tahun lalu dengan mengeksploitasi platform sosial. Artikel tersebut merangkum informasi dari studi ekstensif yang dilakukan oleh University of Surrey mengenai tren meresahkan pemanfaatan media sosial untuk menyebarkan malware. Beberapa temuan itu antara lain sebagai berikut (Ashford, 2019):

- Laporan kejahatan dunia maya yang melibatkan media sosial tumbuh lebih dari 30.000 persen antara 2015 dan 2017 di AS dan empat kali lipat antara 2013 dan 2018 di Inggris.
- Lebih dari 1,3 miliar pengguna media sosial telah disusupi datanya dalam 5 tahun terakhir
- Antara 45 dan 50 persen perdagangan data ilegal dari 2017 hingga 2018 dapat dikaitkan dengan pelanggaran platform media sosial
- Dari 20 situs web global teratas yang menghosting perangkat lunak penambangan cryptocurrency, 11 adalah platform media sosial

Sosial media dapat menghadirkan ancaman baru bagi penggunanya karena potensi untuk mengakses sejumlah besar informasi pribadi yang diungkapkan oleh pengguna sosial media itu sendiri. Berbagai jenis aset rentan terhadap serangan di sosial media, termasuk informasi pribadi individu atau organisasi, identitas digital, aset keuangan, kekayaan intelektual , dan rahasia dan sumber daya perusahaan (Fire et al., 2014). Berikut ini adalah daftar teratas ancaman keamanan privasi yang dapat ditemui di sosial media :

1. *Malware* : *Malware* adalah perangkat lunak berbahaya yang dikembangkan untuk mengganggu operasi komputer untuk mengumpulkan kredensial pengguna dan mendapatkan akses ke informasi pribadinya. Dalam beberapa kasus, malware dapat menggunakan kredensial yang diperoleh untuk menyamar sebagai pengguna dan mengirim pesan menular ke teman online pengguna. *Koobface* adalah malware pertama yang berhasil disebarkan melalui sosial media seperti Facebook, MySpace, dan Twitter. Pada infeksi, *Koobface* mencoba mengumpulkan informasi login. Penelitian dari Bromium dari Februari tahun 2019 menemukan bahwa satu dari lima organisasi telah terinfeksi malware yang didistribusikan melalui platform media sosial. Yang lebih mengkhawatirkan adalah fakta bahwa 12 persen dari organisasi yang terinfeksi tersebut mengalami pelanggaran data sebagai akibatnya (Mcguire, 2019) Alasan lain mengapa platform media sosial menjadi cara yang efektif untuk mendistribusikan malware adalah kenyataan bahwa ada lebih banyak metode pengiriman untuk kode berbahaya seperti malvertising, tautan dan gambar bersama, plugin, dan media digital. Berbagi konten dan bahkan profil secara konstan mendorong penyebaran malware lebih jauh.
2. *Phising attack :* Seringkali dalam bentuk email, pesan teks, atau panggilan telepon, serangan phishing menampilkan dirinya sebagai pesan dari organisasi yang sah. Pesan-pesan ini mengelabui orang agar membagikan data sensitif, termasuk kata sandi, informasi perbankan, atau detail kartu kredit. Serangan phishing sering muncul sebagai platform media sosial. Menurut FBI, phishing adalah jenis kejahatan dunia maya yang paling umum pada tahun 2020—dan insiden phishing hampir dua kali lipat frekuensinya, dari 114.702 insiden pada 2019, menjadi 241.324 insiden pada 2020 (FBI, 2020). Sebuah studi (Amin et al., 2010) menunjukkan bahwa pengguna yang berinteraksi di situs jejaring sosial lebih cenderung jatuh ke penipuan phishing karena sosial. Selain itu, dalam beberapa tahun terakhir, upaya phishing dalam sosial media telah meningkat tajam. Menurut Laporan Intelijen Keamanan Microsoft (Microsoft, 2013), 84,5% dari semua phishing serangan menargetkan pengguna situs jejaring sosial. Salah satunya phishing serangan terjadi di Facebook, memikat pengguna ke Facebook palsu halaman masuk. Kemudian, serangan phishing menyebar di antara Facebook pengguna dengan mengundang teman untuk mengklik tautan yang diposting di aslinya ruang profil pengguna (Fire et al., 2014).
3. *Spammer: Spammer* adalah pengguna yang menggunakan sistem pesan elektronik untuk mengirim pesan yang tidak diinginkan, seperti iklan, ke pengguna lain. Spammer menggunakan media sosial platform jaringan untuk mengirim pesan iklan ke yang lain pengguna dengan membuat profil palsu (Fire et al., 2014). Contoh spamming jaringan dapat ditemukan di Twitter, yang telah mengalami banyak spam. Pada bulan Agustus 2009, 11% dari pesan Twitter adalah pesan spam. Namun, pada awal tahun 2010, Twitter telah berhasil menurunkan persentase pesan spam menjadi 1% (*State of Twitter Spam*, 2010). Pada akhir 2018, jumlah pengguna Twitter turun menjadi 321 juta pengguna aktif bulanan. Twitter melaporkan bahwa penurunan jumlah pengguna aktif bulanan terutama terkait dengan tindakan kerasnya terhadap akun spam dan bot (Aslam, n.d.).
4. *Internet Fraud : Internet Fraud* , juga dikenal sebagai penipuan dunia maya, mengacu pada penggunaan akses Internet untuk menipu atau memanfaatkan orang. Saat ini, menurut Asosiasi Administrator Sekuritas Amerika Utara (NASAA) (*INFORMED INVESTOR ADVISORY: SOCIAL NETWORKING*, 2011), dengan meningkatnya popularitas jaringan online, penipu telah beralih ke sosial media untuk membangun hubungan kepercayaan dengan korban mereka, dan kemudian mereka mengambil keuntungan dari data pribadi yang dipublikasikan di profil online korban. Dalam beberapa tahun terakhir, misalnya, penipu telah meretas akun pengguna Facebook yang bepergian ke luar negeri. Setelah mereka berhasil masuk ke akun pengguna, penipu dengan licik meminta bantuan teman pengguna untuk mentransfer uang ke

rekening bank penipu. Salah satu korban penipuan jenis ini adalah Abigail Pickett. Saat bepergian di Kolombia, Abigail menemukan bahwa akun Facebook-nya telah dibajak oleh seseorang di Nigeria, dan akun itu digunakan untuk mengirim permintaan uang kepada teman-temannya (Halliday, 2010).

5. *Clickjacking: Clickjacking* adalah teknik berbahaya yang menipu pengguna agar mengklik sesuatu yang berbeda dari apa mereka bermaksud untuk mengklik. Dengan menggunakan clickjacking, penyerang dapat memanipulasi pengguna untuk memposting pesan spam di akunnya (Fire et al., 2014). Contoh serangan clickjacking terjadi di Twitter pada tahun 2009 ketika Twitter diganggu oleh serangan "Jangan Klik". Penyerang men-tweet sebuah tautan dengan pesan "*Don't Click*" bersama dengan URL bertopeng (URL sebenarnya disembunyikan). Ketika pengguna Twitter mengklik pesan "*Don't Click*", pesan itu secara otomatis menyebar dan telah diposting ke akun Twitter mereka (McMillan, 2009).

3.2 Kesadaran Keamanan Privasi di Sosial Media

Kesadaran privasi akan menjadi salah satu perkembangan paling signifikan, memberikan tekanan pada pemerintah untuk menerapkan undang-undang perlindungan data, mendikte bagaimana perusahaan akan menangani data individu dan nilai-nilai apa yang harus dimasukkan untuk berjuang di pasar. Namun, perjalanannya masih panjang. Beberapa survei menunjukkan banyak individu masih tidak tahu bagaimana melindungi data mereka dan menunjukkan ketidakpercayaan dalam cara data mereka ditangani.

Berdasarkan survei yang dilakukan oleh Cisco di tahun 2019 menunjukkan data bahwa orang-orang peduli dengan privasi, dan sejumlah besar yang mengejutkan telah mengambil tindakan untuk melindunginya, sebanyak 84% responden menunjukkan bahwa mereka peduli dengan privasi, menjaga data mereka sendiri, peduli dengan data anggota masyarakat lainnya, dan mereka ingin lebih mengontrol bagaimana data mereka digunakan. Dari kelompok ini, 80% juga menyatakan bersedia bertindak untuk melindunginya (Survey, 2019).

Pengguna internet khususnya sosial media perlu memiliki kesadaran keamanan informasi, melihat semakin meningkatnya tren pencurian data pribadi di sosial media. Di Indonesia kesadaran masyarakat akan pentingnya keamanan informasi pribadi terbilang masih cukup rendah Hal ini bisa dilihat dengan masih ada orang-orang yang membagikan data-data pribadi seperti Nomor Kartu Induk (NIK) dan Kartu Keluarga (KK) di layanan internet, seperti media sosial. Padahal, tindakan itu sangat berbahaya jika data-data penting tersebut disalahgunakan oleh orang tak bertanggungjawab (Librianty, 2019).

Melalui media sosial juga, 93% masyarakat Indonesia membagikan data pribadi mereka ecara digital, yakni melalui media sosial. Sebanyak 44 persen masyarakat membagikan lewat publisitas, 21 persen berbagi data pribadi dengan orang asing, bahkan 10 persen pengguna membagikan nomor identifikasi pribadi (PIN). 22% pengguna membiarkan perangkat mereka tidak terkunci dan tidak diawasi ketika berada di tengah sekelompok orang. Selanjutnya, 23 persen pengguna memberikan perangkat mereka untuk digunakan orang lain selama beberapa waktu. Tujuan masyarakat membagikan data ini diketahui untuk memenuhi syarat pemasangan aplikasi pada gawai mereka (Evandio, 2020). Namun berdasarkan penelitian terdahulu, tingkat kesadaran keamanan informasi mencapai angka 76% hal ini menunjukkan kesadaran pengguna di Indonesia berada pada kriteria rata-rata (Akraman et al., 2018).

3.3 Perilaku Perlindungan Privasi dalam Menggunakan Sosial Media

Pengguna dapat mengontrol seberapa banyak informasi tentang diri yang dikeluarkan. Jadi, pengguna dapat mengeedit pengaturan privasi dengan benar. Juga, jika pengguna menemukan diri mereka dalam database beberapa situs "pencarian orang", pengguna dapat meminta mereka untuk menghapus detailnya, dan kemudian mengedit informasi yang dipublikasikan melalui jejaring sosial.

Orang dapat mencoba melindungi privasi online mereka dengan berbagai cara. Perilaku protektif didefinisikan sebagai "tindakan berbasis komputer khusus yang dilakukan konsumen untuk menjaga keamanan informasi mereka" (Milne, Labrecque, & Cromer, 2009, p. 450). Orang dapat melindungi privasi online mereka dengan membatasi informasi yang mereka bagikan, dan dengan mengadopsi langkah-langkah perlindungan privasi (Baruh et al., 2017; Büchi et al., 2017). Sebuah meta-analisis dari beberapa penelitian tentang privasi online menunjukkan bahwa kedua perilaku ini tampaknya tidak terkait (Baruh et al., 2017). Misalnya, orang yang melindungi privasi online mereka di situs jejaring sosial, tidak serta merta membatasi pengungkapan diri (Chen & Chen, 2015). Perilaku ini termasuk memasang pemblokir iklan, manajemen cookie, menggunakan mode pribadi , mengaktifkan fungsi *No Track* di browser, menahan diri untuk tidak mengungkapkan informasi pribadi (Chai et al., 2009; LaRose & Rifon, 2007), tidak menggunakan fitur "tandai" pada sosial media dalam foto atau video (Dienlin & Metzger, 2016), dan mengubah pengaturan privasi di situs jejaring sosial (Chen & Chen, 2015; Walrave, Vanwesenbeeck, & Heirman, 2012).

Namun, karena studi mengukur perilaku yang berbeda, dan beberapa tidak memberikan statistik deskriptif tentang perilaku protektif, tidak ada gambaran yang jelas tentang terjadinya berbagai metode yang digunakan orang untuk melindungi privasi online mereka. Selain itu, hasilnya bervariasi: Beberapa menemukan bahwa membersihkan cookie adalah praktik terbaik (Büchi et al., 2017; Chanchary et al., 2018), sedangkan yang lain menemukan bahwa menginstal pemeriksa virus dan memindai spyware lebih sering digunakan (Milne et al. al., 2009; Smit dkk., 2014). Selain itu, banyak penelitian berfokus pada perlindungan privasi orang di situs jejaring sosial, seperti Facebook (misalnya, Chen & Chen, 2015; Dienlin & Metzger, 2016; Dienlin & Trepte, 2015; Feng & Xie, 2014; Walrave et al., 2012). Ancaman privasi, bagaimanapun, berlaku untuk Internet secara keseluruhan dan tidak terbatas pada situs jejaring sosial. Berikut beberapa perilaku perlindungan privasi di media sosial:

1. Baca dan Pahami Kebijakan Privasi : Setiap situs web di internet memiliki ketentuan privasi, termasuk situs media sosial. Sebelum masuk ke media sosial apa pun dan mendaftarkan akun, penting bagi pengguna untuk membaca dan memahami ketentuan privasi mereka. Berikan perhatian khusus pada ketentuan privasi dari informasi yang Anda daftarkan dan setujui untuk dibagikan saat Anda mendaftar akun dengan platform media sosial. Misalnya, konten apa yang dapat dibagikan dengan pihak ketiga, dapatkah Anda menghapus konten Anda di situs web secara permanen.
2. Fitur Situs : Pengguna wajib membiasakan diri dengan fungsi situs media sosial sebelum membagikan aktivitas apa pun. Pahami siapa yang akan melihat aktivitas dan apakah mereka hanya penerima tertentu atau semua pengguna di platform. Di atas segalanya, pahami pengaturan privasi dan kerentanan privasi di situs media sosial.
3. Sesuaikan Pengaturan Privasi Pengguna : Untuk setiap platform media sosial yang digunakan, selalu periksa pengaturan privasi default di situs mereka. Sebagian besar pengaturan privasi default di media sosial memungkinkan berbagi informasi Anda dengan pengguna online pihak ketiga lainnya. Menyesuaikan pengaturan privasi default dapat membatasi jumlah informasi yang dapat dibagikan situs media sosial dengan pengguna lain di luar pengetahuan Anda.
4. Informasi Biografi : Untuk mendaftarkan akun di banyak platform media sosial, pengguna akan diminta untuk memberikan informasi biografi seperti nama lengkap, tahun lahir, usia, atau alamat. Simpan informasi ini untuk diri sendiri untuk membatasi apa yang diketahui pengguna media sosial lain . Informasi tersebut dapat memberikan data yang cukup bagi penjahat dunia maya untuk membahayakan pengguna.
5. Informasi Akun : Pertimbangkan dengan cermat jenis detail pribadi yang akan diberikan di profil media sosial. Jangan pernah memberikan informasi sensitif seperti sekolah terdekat, afiliasi politik, informasi rekening bank, tempat kerja sebelumnya atau saat ini, nomor Jaminan Sosial, atau kepentingan umum, antara lain. Memberikan informasi ini

mungkin tampak tidak berbahaya, tetapi dapat digunakan untuk menipu atau menayangkan iklan yang tidak perlu.
6. Teman atau Kontak : Berhati-hatilah saat menerima teman atau mengikuti teman atau kontak dengan mempertimbangkan alasan menggunakan situs ini. Sebelum menerima permintaan mengikuti atau berteman, cari tahu tentang orang tersebut, dan pahami (dari linimasa mereka) siapa mereka, apa yang mereka lakukan, dan jenis konten apa yang mereka bagikan.
7. Matikan Lokasi : Saat menyesuaikan pengaturan privasi, jangan pernah lupa untuk mematikan berbagi lokasi gadget. Dengan cara ini, Anda tidak akan memberikan ulasan ke tempat dan bisnis yang sering Anda kunjungi. Mematikan lokasi Anda mencegah Facebook, email, dan Pencarian Telepon Anda.
8. Hati-hati memposting foto secara online : Sebelum memposting foto apa pun, pikirkan dua kali. Memposting foto di media sosial telah diidentifikasi sebagai salah satu aktivitas jejaring sosial yang berisiko. Misalnya, gambar sederhana dan tidak berbahaya tentang anak tanpa nama mungkin sudah mengungkapkan terlalu banyak informasi. Mengiklankan keberadaan Anda melalui gambar dapat membuat Anda, orang yang Anda cintai, atau rumah Anda menjadi target yang menggoda bagi penjahat dunia maya.
9. Hindari Clickbait : Tidak ada media sosial yang akan bertanggung jawab atas aplikasi pihak ketiga Saat diminta untuk 'berkomentar di bawah untuk melihat keajaiban' atau 'memeriksa dengan siapa pengguna berulang tahun,' hindari mengklik umpan acak ini. Mereka adalah aplikasi pihak ketiga yang mencoba menangkap dan menyalahgunakan informasi pribadi.
10. Pilih kata sandi yang “kuat” dan aman. : Gunakan kata sandi yang berbeda di semua akun media sosial yang berbeda. Ubah kata sandi sesering mungkin. Hindari masuk ke komputer umum atau menggunakan ponsel teman untuk masuk ke akun media sosial.

4. KESIMPULAN DAN SARAN

Peningkatan pengguna internet yang secara signifikan terus bertambah dari tahun ke tahun dapat membuka peluang yang lebih besar pula terhadap pelaku kejahatan siber. Dengan fokus utama pada privasi dalam jaringan sosial media, terbukti bahwa pengguna sosial media telah meningkatkan pengungkapan informasi pribadi dengan membuat lebih banyak informasi tersedia secara online. Terlepas dari semua teknologi pemantauan keamanan proaktif yang digunakan oleh berbagai jaringan sosial online saat ini, penyerang dunia maya masih menemukan cara untuk melakukan aktivitas jahat, seperti penyebaran *malware, phising, spam,* dll yang merujuk pada pencurian data pribadi. Perlu adanya kesadaran akan bahaya ancaman privasi dalam menggunakan sosial media agar muncul sifat protektif untuk melindungi data pribadi dalam menggunakan sosial media.

5. DAFTAR RUJUKAN

[1] Abdullah Ramdhani, Muhammad Ali Ramdhani, A. S. A. (2014). Writing a Literature Review Research Paper: A step-by-step approach. *International Journal of Basic and Applied Science*, *03*(01), 47–56. https://digilib.uinsgd.ac.id/5129/1/08IJBAS%283%29%281%29.pdf

[2] Aite Group. (2020). *U.S. Identity Theft: The Stark RealityNo Title*. https://www.giact.com/aite-report-us-identity-theft-the-stark-reality/ [Accessed 19 October 2021]

[3] Akraman, R., Candiwan, C., & Priyadi, Y. (2018). Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia. *Jurnal Sistem Informasi Bisnis*, *8*(2), 1. https://doi.org/10.21456/vol8iss2pp1-8

[4] Amin, T., Okhiria, O., Lu, J., & An, J. (2010). Facebook: A Comprehensive Analysis of Phishing on a Social System. *Department of Electrical and Computer*

Engineering.
http://courses.ece.ubc.ca/eece412/term_project/reports/2010/facebook.pdf
[5] Ashford, W. (2019). *Cyber criminals earn $3bn a year exploiting social platforms*. https://www.computerweekly.com/news/252458334/Cyber-criminals-earn-3bn-a-year-exploiting-social-platforms [Accessed 19 October 2021]
[6] Aslam, S. (n.d.). *Twitter by the Numbers: Stats, Demographics & Fun Facts*. https://www.omnicoreagency.com/twitter-statistics/ [Accessed 19 October 2021]
[7] Barnes, S. B. (2006). *A privacy paradox: Social networking in the United States*. *11*(9). https://doi.org/https://doi.org/10.5210/fm.v11i9.1394
[8] Baruh, L., & Popescu, M. (2017). Big data analytics and the limits of privacy self-management. New Media & Society, 19, 579-596. doi:10.1177/1461444815614001
[9] Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: The importance of internet skills for online privacy protection. Information, Communication & Society, 20, 1261-1278. doi: 10.1080/1369118X.2016.1229001
[10] Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., & Upadhyaya, S. J. (2009). Internet and online
[11] information privacy: An exploratory study of preteens and early teens. IEEE Transactions on Professional Communication, 52, 167-182. doi:10.1109/TPC.2009.2017985
[12] Chanchary, F., Abdelaziz, Y., & Chiasson, S. (2018). Privacy concerns amidst OBA and the need for alternative models. IEEE Internet Computing, 22, 52-61. doi:10.1109/ MIC.2017.3301625
[13] Chen, H., & Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. Cyberpsychology, Behavior, and Social Networking, 18, 13-19. doi:10.1089/cyber.2014.0456
[14] Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. European Journal of Social Psychology, 45, 285-297. doi:10.1002/ejsp.2049Evandio, A. (2020). *Kesadaran Masyarakat Soal Data Pribadi Masih Rendah, Ini Buktinya*. https://teknologi.bisnis.com/read/20200810/101/1277388/kesadaran-masyarakat-soal-data-pribadi-masih-rendah-ini-buktinya [Accessed 19 October 2021]
[15] FBI. (2020). 2020 Internet Crime Report. *Federal Bureau of Investigation - Internet Crime Complaint Center*, 1–28. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
[16] Feng, Y., & Xie, W. (2014). Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. Computers in Human Behavior, 33, 153-162. doi:10.1016/j.chb.2014.01.009
[17] Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online social networks: Threats and solutions. *IEEE Communications Surveys and Tutorials*, *16*(4), 2019–2036. https://doi.org/10.1109/COMST.2014.2321628
[18] Ghazinour, K., & Ponchak, J. (2017). Hidden Privacy Risks in Sharing Pictures on Social Media. *Procedia Computer Science*, *113*, 267–272. https://doi.org/10.1016/j.procs.2017.08.367
[19] Gross, R., Acquisti, A., & Heinz, H. J. (2005). Information revelation and privacy in online social networks. *WPES'05: Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, 71–80. https://doi.org/10.1145/1102199.1102214
[20] Halliday, J. (2010). *Facebook fraud a "major issue."* https://www.theguardian.com/technology/2010/sep/20/facebook-fraud-security
[21] Hootsuite. (2021). *DIGITAL 2021: INDONESIA*. https://datareportal.com/reports/digital-2021-indonesia [Accessed 19 October 2021]
[22] *INFORMED INVESTOR ADVISORY: SOCIAL NETWORKING*. (2011).

https://www.nasaa.org/5568/informed-investor-advisory-social-networking/ [Accessed 19 October 2021]

[23] LaRose, R., & Rifon, N. J. (2007). Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. Journal of Consumer Affairs, 41, 127-149. doi:10.1111/j.1745-6606.2006.00071.x

[24] Librianty, A. (2019). *Kesadaran Soal Keamanan Data Pribadi di Indonesia Masih Rendah*. https://www.liputan6.com/tekno/read/4004034/kesadaran-soal-keamanan-data-pribadi-di-indonesia-masih-rendah [Accessed 19 October 2021]

[25] Mcguire, M. (2019). *Socıal Medıa Platforms And The Cybercrıme Economy*. 27. https://www.bromium.com/wp-content/uploads/2019/02/Bromium-Web-of-Profit-Social-Platforms-Report.pdf

[26] McMillan, R. (2009). *Researchers make wormy Twitter attack*. https://www.pcworld.idg.com.au/article/296382/researchers_make_wormy_twitter_attack/ [Accessed 19 October 2021]

[27] Microsoft. (2013). Microsoft Security Intelligence Report. *Microsoft Security Intelligence Report*, *16*, 1–19. http://download.microsoft.com/download/7/2/B/72B5DE91-04F4-42F4-A587-9D08C55E0734/Microsoft_Security_Intelligence_Report_Volume_16_English.pdf

[28] Sepideh Deliri, M. A. (2015). Security and Privacy Issues in Social Networks. In *Data Management in Pervasive Systems* (pp. 195–209). Springer Cham.

[29] *State of Twitter Spam*. (2010). https://blog.twitter.com/official/en_us/a/2010/state-of-twitter-spam.html# [Accessed 19 October 2021]

[30] Stout, D. W. (2021). *Social Media Statistics 2021: Top Networks By the Numbers*. https://dustinstout.com/social-media-statistics/#facebook-stats [Accessed 19 October 2021]Survey, C. C. P. (2019). *Consumer Privacy Survey*. *November*, 1–14.

[31] Waqas. (2020). *Tokopedia hacked – Login details of 91 million users sold on dark web*. https://www.hackread.com/tokopedia-hacked-login-details-sold-on-dark-web/ [Accessed 19 October 2021]

[32] Walrave, M., Vanwesenbeeck, I., & Heirman, W. (2012). Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 6(1), Article 3. doi:10.5817/CP2012-1-3