SURVEI TINGKAT PEMAHAMAN MAHASISWA MENGENAI ANCAMAN KEAMANAN SISTEM PADA *FACEBOOK*

Eddy Ryansyah [1], Muh. Yoga Fauzan [2], Reymen Maulana [3], Chaerur Rozikin [4]
Program Studi Informatika, Universitas Singaperbangsa Karawang [1, 2, 3, 4]
eddyryansyah1612@gmail.com [1], 2110631170154@student.unsika.ac.id [2],
2110631170140@student.unsika.ac.id [3], chaerur.rozikin@staff.unsika.ac.id [4]

Submitted November 16, 2022; Revised March 15, 2023; Accepted March 20, 2023

Abstrak

Facebook yaitu contoh dari platform yang bergerak di bidang sosial media, dan menjadi salah satu yang terlaris di Indonesia bahkan dunia, hampir dapat dikatakan satu orang di dunia mempunyai satu akun *facebook*. Platform ini digunakan sebagai wadah para penggunanya berinteraksi dengan para sahabat, relasi, rekan kerja bahkan keluarga di luar kota. Dalam aplikasi media sosial ini menyediakan banyak fasilitas sebagai berikut, berbagi status baik teks, gambar maupun video. Dan pada kesempatan kali ini penulis dan dalam tulisan mengangkat tema isu ancaman serangan pada *facebook* di antaranya *phising, link scam, clickjacking.* Dan dalam *paper* kali ini juga akan dianalisa mengenai penyebab dan cara kerja serangan serta cara penanganan atau pencegahan terhadap ancaman yang mengintai ini. Jenis penelitian yang digunakan merupakan pendekatan kuantitatif. Metode pengumpulan data yang dilakukan dengan cara survei dan menggunakan studi pustaka. Sampel yang terkumpul dalam penelitian ini sebanyak 58 responden yang semuanya mahasiswa dan pernah menggunakan *facebook*. Berdasarkan hasil penelitian, penulis menyimpulkan sebagian besar responden belum memahami bahkan mengetahui berbagai ancaman keamanan sistem pada *facebook.*
Kata Kunci : *Link Scam, Clickjacking, Phising, Facebook*

Abstract

Facebook is an example of a platform of social media and has become one of the best-selling media in Indonesia and even in the world. It may be said one person in the world has one facebook account. The platform is used as a forum for users to interact with friends, relations, colleagues, and even families outside the city. This social media application provides many facilities as follows, sharing statuses, in the form of texts, images, and videos. In this research, the researcher explores the theme of threats on facebook including phishing, link scam, and clickjacking. The researcher also analyzes the causes, how the lurking threats work and how to deal with or prevent them. The research uses a quantitative approach. The data collection method is carried out using a survey and a library research. The samples collected in the research are 58 respondents who are all students having used Facebook. Based on the research results, the researchers conclude that most respondents do not understand or even know the various system security threats on Facebook.
Keywords : *Link Scam, Clickjacking, Phising, Facebook*

1. PENDAHULUAN

Dengan bertambah maju nya teknologi sistem informasi tentunya membawa dampak baik maupun buruk. Teknologi merupakan gabungan dari dua buah kata yunani, *techne* yang mempunyai makna karya seni, karya kerajinan serta keterampilan akan sesuatu, serta *logia* yang mempunyai makna kata, maka dapat disimpulkan teknologi mempunyai makna pemahaman akan sistem kerja untuk menciptakan sesuatu [1]. Sistem adalah persatuan yang saling terhubung dan tidak dapat dipisahkan yang saling mendukung dalam membentuk suatu bangunan. Contoh umumnya ialah negara, negara terdiri dari beberapa daerah/provinsi yang saling bahu membahu dan penduduk sebagai penggeraknya [2]. Informasi yaitu penyebar luasan berita kepada masyarakat tentang

pengetahuan tertentu, akan tetapi informasi juga dapat diartikan sebagai ilmu pengetahuan bagi individu yang belum mengetahuinya [2].

Sebagai contoh yaitu kemudahan individu untuk mendapatkan berita yang terjadi jauh dari dirinya, sangat mudah dan cepat diterima. Dan karena itupun banyak individu yang kurang mengindahkan keamanan dari teknologi sistem informasi. Keamanan sistem informasi merupakan upaya dalam mempertahankan data dari tindak perusakan dan tindakan tidak bertanggung jawab lainnya dari individu maupun instansi. Dan yang paling banyak adalah kurangnya kesadaran dan pemahaman untuk melindungi data dalam penggunaan aplikasi *facebook.* Kesadaran yaitu situasi dimana individu memahami posisinya dan dapat membagi waktunya untuk mendapatkan hak dan melaksanakan kewajiban [3]. Pemahaman merupakan keterampilan dalam menangkap dan menginterpretasikan suatu pembelajaran atau diksi yang disampaikan seseorang [4]. *Facebook* yaitu salah satu platform pertemanan digital dan berbagi status yang sangat banyak digunakan sebagai wadah diskusi atau komunikasi [5]. Bentuk ancaman yang sering dijumpai pada platform *facebook* di antaranya *phising, click jacking attack, link scam. Phising* sendiri merupakan kata serapan dari kata *fishing* yang bermakna memancing, yaitu teknik penipuan yang dilaksanakan dengan perayuan target untuk menyerahkan data-datanya yang bersifat pribadi. *Click jacking attack* merupakan singkatan kata "*Click Hijacking*", dalam kasus ini *attacker* akan berusaha menguasai tombol klik milik *user* dan membohongi *user* untuk memilih suatu *link* yang sebenarnya isinya palsu, contohnya adalah ketika *user* diarahkan untuk memilih hadiah akan tetapi sebenarnya hanya ingin merekam data pribadinya. *Link scam* pada prinsip nya hampir sama seperti *phising*, cara kerjanya pun tidak berbeda jauh. Pada kasusnya para *hacker* akan bekerja dengan membagikan penipuannya juga kepada para kerabat dan menimbulkan pencurian data secara masif dan besar-besaran.

Ada beberapa cara untuk menangkal serangan *cybercrime* di *facebook.* Adapun pengertian dari *cybercrime* yaitu merupakan sebuah kejahatan atau kegiatan yang melanggar aturan dan hukum dengan media komputer dan jaringan komputer, yang merugikan individu maupun kelompok [6].

Cybercrime sebuah manifestasi buruk dari kemajuan bidang teknologi internet yang dimanfaatkan untuk melawan hukum dan merugikan seseorang atau instansi [7]. *Cybercrime* yaitu sebuah tindakan ilegal yang berfokus untuk menyerang dan melemahkan sistem keamanan dari target yang dituju [8]. Maka dari itu dibutuhkan suatu langkah pencegahan agar tidak terkena berbagai ancaman kejahatan. Di antaranya yaitu:

a. Tingkatkan kewaspadaan dengan selalu berhati-hati jika didapatkan situs yang mengharuskan untuk memencetnya dan disuruh memasukkan informasi pribadi.
b. Ganti secara berkala *password* media sosial yang dimiliki.
c. Gunakan sistem data yang sudah terindikasi memakai data enkripsi pada aplikasi, contohnya yaitu *WhatsApp* sebagai media komunikasi jarak jauh antar umat.

Tujuan penelitian ini dilakukan untuk mengetahui tingkat pengetahuan mahasiswa mengenai ancaman keamanan sistem pada *facebook* seperti *link scam*, *click jacking attack*, dan *phising.* Karena ancaman yang sangat serius, maka penulis tergerak untuk melakukan penelitian dan pembuatan jurnal dengan tema ini, agar tidak banyak lagi individu yang terjebak *cybercrime*. Diharapkan setelah jurnal ini selesai dikerjakan dan dipublikasi akan

semakin banyak orang yang lebih peduli dengan keamanan data pribadinya.

2. METODE PENELITIAN

Berdasarkan Kamus Besar Bahasa Indonesia, pengertian dari metode yaitu sebuah teknik dengan sistematis yang memiliki tujuan memuluskan keinginan tertentu dari seseorang untuk mewujudkan tujuannya [9].

Dalam penulisan *paper* jurnal ini penulis menggunakan teknik penelitian kuantitatif. Teknik penelitian kuantitatif adalah cara yang dilakukan penulis untuk menemukan pengetahuan atau keterangan dengan cara memberi data yang dalam bentuk angka. Metode pengumpulan informasi yang dilakukan dengan cara:

a. Survei

   Survei yaitu salah satu cara mengumpulkan data dengan menganalisa sekumpulan besar yang kemudian diambil sampel untuk mengetahui sifat, dan mengumumkan apa yang ada di dalam populasi tersebut [10].

   Penelitian pada komunitas/populasi besar ataupun kecil, kemudian data yang terkumpul dipelajari dan digunakan untuk memecahkan masalah yang terkait. Penulis membuat survei menggunakan *google forms* lalu menyebarkannya dengan cara *broadcast* di media sosial. Setelah melakukan survei menggunakan *google forms* dan menyebarkannya melalui media sosial, penulis telah melakukan pengujian reliabilitas dan validitas dari instrumen kuesioner yang digunakan.

   Untuk reliabilitas, penulis telah menghitung nilai *Cronbach's alpha* yang merupakan ukuran keandalan internal dari kuesioner. Nilai *Cronbach's alpha* yang diperoleh sebesar 0,83 menunjukkan bahwa kuesioner memiliki tingkat reliabilitas yang baik.

   Sedangkan untuk validitas, penulis telah melakukan validitas isi atau *content validity*, yaitu dengan mengevaluasi kecocokan antara pertanyaan dalam kuesioner dengan tujuan penelitian. Penulis juga telah melakukan validitas konstruk atau *construct validity*, yaitu dengan menguji hubungan antara variabel yang diamati dan mencari bukti bahwa kuesioner tersebut dapat memperkirakan variabel yang diamati. Hasil pengujian validitas menunjukkan bahwa kuesioner yang digunakan dalam survei memiliki validitas yang memadai untuk tujuan penelitian.

   Dengan demikian, hasil pengujian reliabilitas dan validitas kuesioner menunjukkan bahwa instrumen kuesioner yang digunakan dalam survei memiliki tingkat keandalan dan kevalidan yang baik dan dapat dipercaya untuk mengumpulkan data yang diperlukan.

b. Studi Pustaka

   Studi pustaka yaitu salah satu satu cara yang sering dilakukan oleh para pembuat paper jurnal yaitu dengan menggalang atau menghimpun semua data untuk mendukung suatu pendapat atau opini nya dengan menggunakan cara tertentu demi mencapai targetnya [11].

   Mencari referensi pada buku ataupun jurnal, lalu membaca dan mencatatnya. Setelah itu, akan diolah menjadi bahan penelitian. Penulis menggunakan jurnal terdahulu yang berkaitan dengan penelitian sebagai bahan referensi.

3. HASIL DAN PEMBAHASAN

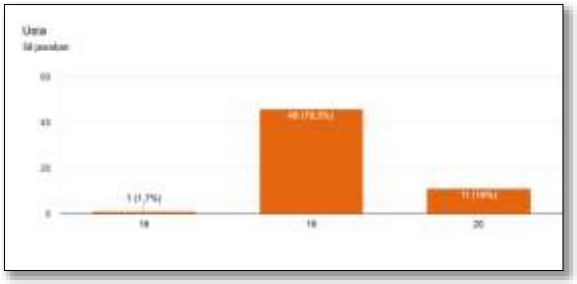
Hasil survei tingkat pemahaman mahasiswa terhadap ancaman keamanan sistem pada *facebook* menunjukkan bahwa mayoritas

responden memiliki pemahaman yang cukup tentang ancaman keamanan pada platform tersebut. Namun, masih ada sebagian responden yang kurang memahami atau bahkan tidak tahu tentang jenis-jenis ancaman tersebut.

Hal ini sejalan dengan penelitian sebelumnya yang dilakukan oleh Nurhayati, Ghazali, dan Ali pada tahun 2018 [12]. Dalam penelitian tersebut, ditemukan bahwa sebagian besar pengguna *facebook* di Indonesia kurang memahami ancaman keamanan seperti *link scamming* dan *phising*. Meskipun demikian, penelitian tersebut juga menunjukkan bahwa pengguna *facebook* di Indonesia cukup peduli terhadap keamanan akun mereka dan telah melakukan beberapa tindakan pencegahan.

Dalam upaya untuk meningkatkan pemahaman pengguna *facebook* tentang ancaman keamanan, perlu dilakukan edukasi dan sosialisasi secara terus-menerus. Langkah ini sejalan dengan rekomendasi yang diberikan oleh Wahab, AlMajali, dan Al-Saleh pada penelitian mereka yang diterbitkan pada tahun 2018 [13].

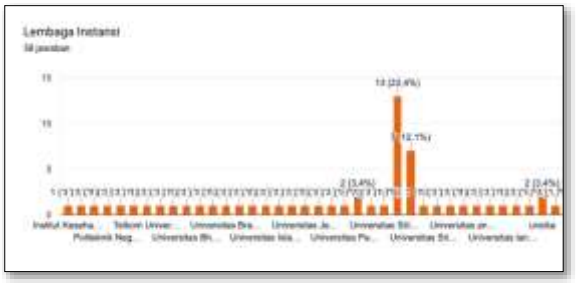
Berdasarkan sumber data primer, yaitu dengan metode observasi survei, maka diperoleh hasil sebagai berikut dalam bentuk grafik. Grafik yaitu salah satu bentuk komunikasi dengan tampilan visual menggunakan bantuan lambang titik koordinat ataupun goresan-goresan garis sederhana yang melewati garis sumbu:



Sumber : Survei dari Penulis

Gambar 1. Grafik Rentang Usia Peserta Kuisioner

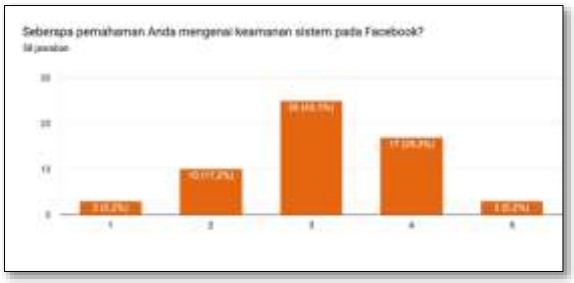
Dapat dilihat pada gambar di atas bahwa kebanyakan yang mengisi kuisioner berusia antara 18 sampai 20 tahun. Berdasarkan gambar 1 didapatkan data ada sebanyak 58 orang mengisi kuisioner dengan rincian, sebanyak 1 orang yang berusia 18 tahun (1,7%) dari keseluruhan peserta, 46 orang yang mempunyai usia 19 tahun atau sebanyak (79,3%) dari keseluruhan data, dan 11 orang yang berusia 20 tahun (19%) dari jumlah keseluruhan data. Hal ini menunjukkan bahwa rata-rata remaja-orang dewasa di Indonesia bermain atau pernah bermain *facebook*. Hal ini semakin menguatkan data Indonesia sebagai negara ketiga di dunia dengan pengguna *facebook* sebesar 202,2 juta jiwa per Juli 2022, jumlah tersebut mengalami penurunan sebesar 0,09% daripada bulan sebelumnya yaitu sebanyak 202,4 juta orang.



Sumber : Survei dari Penulis

Gambar 2. Grafik Asal Instansi

Berdasarkan data dari tabel di atas dapat dilihat yaitu mayoritas pengisi berasal dari mahasiswa Universitas Singaperbangsa Karawang dengan jumlah responden sebanyak 24 orang, disusul dengan 28 universitas dan perguruan tinggi lainnya yang masing-masing hanya memperoleh 1-2 responden saja. Hal ini dikarenakan penulis berasal dari Universitas Singaperbangsa Karawang dan kebanyakan yang mengisi adalah sahabat karib dari penulis.



Sumber : Survei dari Penulis

Gambar 3. Grafik Tingkat Pemahaman Akan Sistem Keamanan pada *Facebook*

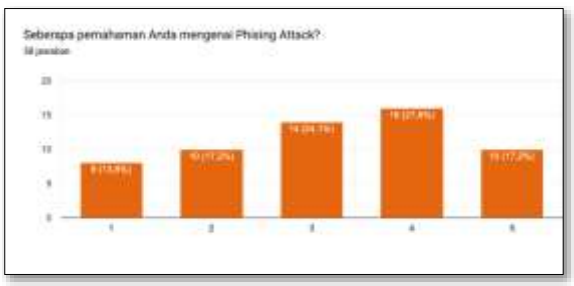
Selanjutnya dalam tabel di atas dimuat mengenai persentase tingkat pemahaman responden mengenai sistem keamanan pada *facebook,* dan data yang didapat cukup menyenangkan dimana rata-rata pengguna *facebook* sudah mengetahui dan paham mengenai sistem keamanan *facebook.* Di bawah ini merupakan rincian data yang didapat, sebanyak 3 orang atau sekitar 5,2% dari keseluruhan data yang memilih opsi 1 (Sangat tidak paham), 10 orang atau sekitar 17,2% memilih opsi 2 (Tidak paham), dan sebanyak 25 orang atau sekitar 43,1% memilih opsi 3 (Cukup paham), selanjutnya ada 17 orang atau sebesar 29,3% yang menjatuhkan pilihannya kepada opsi 4 (Paham), dan yang terakhir ada sekitar 3 orang yang merasa sangat paham atau sekitar 5,2% dari keseluruhan data yang masuk.

Sumber : Survei dari Penulis

Gambar 4. Grafik Tingkat Pemahaman Ancaman Sistem Keamanan pada *Facebook*

Selanjutnya penulis melakukan survei dengan subjek survei yaitu pemahaman ancaman keamanan sistem pada platform *facebook*. Karena pada dasarnya semua media sosial itu mempunyai risiko kebocoran data yang sangat tinggi, apabila kita sebagai pengguna tidak berhati-hati dalam penggunaannya. Tidak jarang kita dengar banyak *user* yang data pribadi nya tercuri dan kehilangan berbagai materiel. Maka karena itu, penulis tergerak untuk melakukan survei untuk mengetahui tingkat pemahaman masyarakat khususnya pada kaum mahasiswa, dan data nya sebagai berikut:

Ada 3 orang atau sekitar 5,2% yang memilih opsi 1 (Sangat tidak paham) mengenai apa saja ancaman keamanan sistem pada *facebook,* yang menunjukkan masih rendahnya tingkat literasinya. Kemudian ada sekitar 13 orang atau sekitar 22,4% yang memilih opsi ke 2 (Tidak paham), selanjutnya ada sebanyak 18 responden atau sekitar 31% yang memilih opsi 3 (Cukup paham) mengenai ancaman keamanan sistem pada *facebook,* di sini menunjukkan sudah mulai mudah didapatnya informasi mengenai ancaman keamanan sistem *facebook* dan sudah berkembang minat literasi daripada responden sendiri. Selanjutnya ada sekitar 16 responden atau sekitar 27,6% yang memilih opsi 4 (Paham), dan yang terakhir ada sekitar 8 responden yang memilih opsi 5 (Sangat paham) akan ancaman keamanan sistem pada *facebook.* Secara keseluruhan tingkat pemahamannya cukup baik, dan rata-rata memilih opsi cukup paham dan menandakan khususnya kaum *milenial* sudah paham dan siap akan kemajuan zaman.

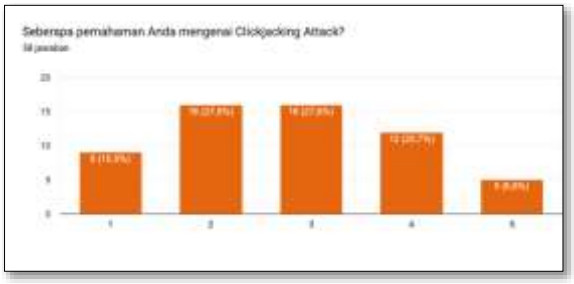


Sumber : Survei dari Penulis

Gambar 5. Grafik Tingkat Pemahaman Terhadap Bahaya *Phising Attack*

Pada grafik ini dituangkan fakta mengenai seberapa tingkat pemahaman responden mengenai bahaya serangan *phising* yang selalu mengintai ketika berselancar di media sosial. Pengertian dari bahaya sendiri ialah suatu keadaan dimana pada suatu tempat atau lokasi terdapat suatu kesempatan untuk terjadinya suatu insiden yang tidak diinginkan [14]. Dan untuk data yang didapat yaitu sebagai berikut:

Sebanyak 8 orang atau 13,8% responden memilih opsi 1 (Sangat tidak paham) yang artinya mereka tidak mengetahui apa yang dimaksud dengan *phising* itu sendiri, dan sebanyak 10 orang atau sekitar 17,2% menjatuhkan pilihannya ke opsi 2 (Tidak paham) dan artinya informasi mengenai *phising* sudah masuk ke mereka, akan tetapi masih kurang dalam hal pemahamannya. Dan yang ketiga ada sebanyak 14 orang atau sebanyak 24,1% yang memilih opsi 3 (Cukup paham) yang menunjukkan responden sudah mulai memahami apa itu *phising* dan dampak bahaya yang dihasilkan ketika terkena serangan *phising*. Selanjutnya ada sebanyak 16 orang atau sekitar 27,6% yang sudah mulai memahami apa yang dimaksud dengan *phising attack,* dan yang terakhir ada sebanyak 10 orang atau jika dalam bentuk persentase sebesar 17,2% yang sudah sangat paham dan hatam yang dimaksud dengan *phising attack.*



Sumber : Survei dari Penulis

Gambar 6. Grafik Tingkat Pemahaman Terhadap Bahaya *ClickJacking Attack*

Untuk tabel di atas menjelaskan mengenai tingkat pemahaman responden mengenai *clickjacking attack. Clickjacking attack* sendiri mempunyai definisi yang hampir mirip dengan *phising*, yaitu dimana seorang *hacker* akan memberikan sebuah email ataupun seperti *game* judi yang sebenarnya ketika diklik maka data pribadi bersangkutan akan direkam untuk digunakan sesuai dengan tujuannya. Adapun hasil dari survei nya sebagai berikut:

Yang pertama ada sebanyak 9 orang atau dengan persentase sebesar 15,5% dari keseluruhan data yang menyatakan mereka sama sekali tidak paham apa itu *clickjacking*, dan selanjutnya ada sebanyak 16 orang atau sekitar 27,6% yang menyatakan mereka sebenarnya sudah mengetahui yang dimaksud dengan istilah itu akan tetapi masih belum memahamai apa definisi sebenarnya dari istilah tersebut, dan yang ketiga ada sekitar 16 orang juga yang menyatakan mereka sedikit memahami atau cukup memahami objek yang dimaksud, dan pada grafik selanjutnya ada sekitar 12 orang atau dengan persentase sebesar 20,7% yang menyatakan mereka memahami dan mengerti apa itu *clickjacking* akan tetapi masih belum memahami cara mencegah dan mengatasinya jika sudah terlanjur terjangkit atau terpapar *clickjacking*, dan yang terakhir terdapat sebanyak 5 orang atau sekitar 8,6% yang mengklaim dirinya sangat memahami apa itu *clickjacking* dan sepertinya mereka sudah mengetahui cara menangkalnya.

Sumber : Survei dari Penulis

Gambar 7. Grafik Tingkat Pemahaman Terhadap Bahaya *Link Scam*

Pada grafik yang terakhir menunjukkan tingkat pemahaman para responden

mengenai *link scam,* dan inilah hasil dari survei yang kami lakukan. Yang pertama ada 5 orang atau sekitar 8,6% memilih opsi yang pertama yaitu sangat tidak paham mengenai apa yang dimaksud dengan *link scam,* dan sebanyak 8 orang atau sebanyak 13,8% yang memilih opsi ke 2 atau mereka tidak paham, dan yang ketiga ada sebanyak 20 orang atau jika dalam persentase sebesar 34,5% yang memilih opsi 3 yaitu dengan subjek cukup paham, dimana mereka sudah mulai melek akan informasi dan sedikit nya mereka sudah paham aka napa yang dimaksud dengan *link scam,* dan kemudian ada sekitar 16 atau sebesar 27,6% responden yang memilih opsi 4 atau masuk kriteria paham, yang menunjukkan bahwa sebagian besar orang yang berada di lingkungan ini sudah mengerti dan memahami mengenai apa itu *link scam* dan cara mengatasi dan menangkal nya. Dan hanya sebanyak 9 responden saja atau sekitar 15,5% saja yang mengisi kriteria sangat paham.

4. SIMPULAN

Berdasarkan penulisan ini yang menggunakan sumber data primer dari survei para mahasiswa, dan data sekunder dari studi pustaka, maka penulis mendapatkan beberapa kesimpulan:

a. Sebagian besar responden belum memahami bahkan mengetahui berbagai ancaman keamanan sistem pada *facebook.*
b. Penggunaan *facebook* yang tidak disandingi dengan kewaspadaan akan menimbulkan risiko. Adapun risiko yang dimaksud seperti *phising attack, clickjacking attack* dan *link scam*. *Phising attack* adalah jenis serangan *cyber* di mana penyerang mencoba memperoleh informasi rahasia seperti nama pengguna, kata sandi, dan informasi keuangan dengan menyamar sebagai sumber tepercaya melalui email, pesan instan, atau situs web yang palsu. Cara mengatasinya yaitu jangan pernah memasukkan informasi pribadi atau keuangan pada situs web yang tidak diketahui atau tidak terpercaya, selanjutnya jangan membalas email yang mencurigakan seperti meminta informasi pribadi, serta jika menerima email atau pesan yang mencurigakan, verifikasi sumbernya terlebih dahulu sebelum memasukkan informasi pribadi. *Clickjacking attack* adalah jenis serangan di mana penyerang menipu pengguna agar mengklik tautan atau tombol tertentu di situs web yang sebenarnya akan mengarahkan pengguna ke situs web yang berbeda atau melakukan tindakan yang tidak diinginkan. Untuk meminimalisir risiko ancaman tersebut dengan cara jangan mengklik tautan atau tombol yang mencurigakan atau tidak dikenal, kemudian, cek terlebih dahulu URL situs web dengan cermat sebelum memasukkan data keuangan atau informasi pribadi, lalu gunakan perangkat lunak keamanan untuk melindungi perangkat dari serangan *clickjacking*. *Link scam* adalah jenis serangan di mana penyerang menggunakan tautan palsu untuk mengarahkan pengguna ke situs web palsu yang terlihat mirip dengan situs web asli, dan meminta pengguna untuk memasukkan informasi pribadi atau keuangan. Untuk menghindari ancaman tersebut cara mengatasinya sama dengan dua ancaman yang telah dijelaskan sebelumnya.

DAFTAR PUSTAKA

[1] K. Afriyanti, “Analisis Perubahan Perilaku Konsumen Dan Strategi Pemasaran Di Era Perkembangan Teknologi Informasi Pada Neea ‘Sib Collection’ Di Desa Robayan Kalinyamatan Jepara,” IAIN Kudus, 2019.
[2] M. Rifauddin and A. N. Halida,

"Waspada Cybercrime dan Informasi Hoax pada Media Sosial Facebook," *Khizanah al-Hikmah J. Ilmu Perpustakaan, Informasi, dan Kearsipan*, vol. 6, no. 2, pp. 98–111, 2018, doi: 10.24252/kah.v6i2a2.

[3] R. Sapitri, A. S. Helmi, and M. A. S. Nalendra, "Peningkatan Kesadaran Kesehatan dan Keselamatan Kerja (K3) untuk Pekerja Usia 30 Tahun keatas dengan Televison Commercial dan Poster," *J. Logist.*, vol. 1, no. 1, pp. 24–29, 2022, [Online]. Available: https://journal.iteba.ac.id/index.php/logistica/article/view/49

[4] F. Yohanes and Sutriyono, "Analisis Pemahaman Konsep Berdasarkan Taksonomi Bloom dalam Menyelesaikan Soal Keliling dan Luas Segitiga Bagi Siswa Kelas VIII," *J. Mitra Pendidik.*, vol. 2, no. 1, pp. 23–35, 2018.

[5] H. A. K. Umam, "Pengaruh Penggunaan Facebook Terhadap Aktivitas Belajar Siswa Pada Mata Pelajaran Sejarah Kebudayaan Islam (Studi di MAN 2 Kota Serang)," Universitas Islam Negeri "Sultan Maulana Hasanuddin" BANTEN, 2017.

[6] A. Gani, "Cybercrime (Kejahatan Berbasis Komputer)," *J. Sist. Inf. Univ. Suryadarma*, vol. 5, no. 1, pp. 16–29, 2020, doi: 10.35968/jsi.v5i1.18.

[7] M. S. Akub, "Pengaturan Tindak Pidana Mayantara (Cyber Crime) dalam Sistem Hukum Indonesia," *Al-Ishlah J. Ilm. Huk.*, vol. 21, no. 2, pp. 85–93, 2020, [Online]. Available: https://jurnal.fh.umi.ac.id/index.php/ishlah/article/view/19

[8] A. Oya, M. Salahuddin, A.Haris, and L. Haryanto, "Pelanggaran Hukum dalam Tindakan Vandalisme di Ruang Cyberspace," *KAMBOTI J. Sos. dan Hum.*, vol. 1, no. 1, pp. 32–43, 2020, [Online]. Available: http://lldikti12.ristekdikti.go.id/jurnal/index.php/kamboti/article/view/35

[9] W. Wahidmurni, "Pemaparan Metode Penelitian Kualitatif," *UIN Maulana Malik Ibrahim Malang*, pp. 1–17, 2017, [Online]. Available: http://repository.uin-malang.ac.id/1984/2/1984.pdf

[10] N. F. Andhini, "Metode penelitian survey," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2017.

[11] M. Sari and A. Asmendri, "Penelitian Kepustakaan (Library Research) dalam Penelitian Pendidikan IPA," *Nat. Sci. J. Penelit. Bid. IPA dan Pendidik. IPA*, vol. 6, no. 1, pp. 41–53, 2020, doi: 10.15548/nsc.v6i1.1555.

[12] I. Nurhayati, A. F. Ghazali, and F. M. Ali, "Link scamming on Facebook: A case study of Indonesian users," *in 2018 International Conference on Information and Communications Technology (ICOIACT)*, pp. 69-73, 2018.

[13] A. Wahab, A. H. AlMajali, and Y. Al-Saleh, "A survey on Facebook security threats and mitigation techniques," *Journal of Information Security and Applications*, vol. 41, pp. 1-20, 2018.

[14] N. Panjaitan, "Bahaya Kerja Pengolahan Rss (Ribbed Smoke Sheet) Menggunakan Metode Hazard Identification and Risk Assessment Di Pt. Pqr," *J. Sist. Tek. Ind.*, vol. 19, no. 2, pp. 50–57, 2017, doi: 10.32734/jsti.v19i2.374.