NUANSA INFORMATIKA ***p-ISSN :1858-3911* , *e-ISSN : 2614-5405***
Volume 18 Nomor 2, Juli 2024 https://journal.fkom.uniku.ac.id/ilkom

Kesadaran Keamanan Informasi atas Phising, Smishing, dan Vishing pada Warga Kota Cimahi

Ulfa Ladayya*[1], Deni Prayitno[2], Mamay Syani[3], Rizki Hikmawan[4], Nuur Wachid Abdulmajid[5]
[1,4,5]Pendidikan Sistem dan Teknologi Informasi, Kampus UPI di Purwakarta, Universitas Pendidikan Indonesia, Indonesia
[2]Dinas Komunikasi dan Informatika Kota Cimahi, Indonesia
[3]Politeknik TEDC, Indonesia
E-mail:
*[1]**ladayaulfa@upi.edu**,[2]deni.prayitno@cimahikota.go.id,[3]msyani@poltektedc.ac.id,[4]hikmariz@upi.edu,
[5]nuurwachid@upi.edu

Abstrak

Menjaga kerahasian informasi menjadi tantangan di zaman yang penuh dengan teknologi ini. Keamanan informasi merupakan aset bagi setiap orang, setiap perusahaan, pemerintahan, maupun bagi dunia. Keamanan informasi adalah sebuah cara untuk mencegah adanya penipuan ataupun menemukannya dari sebuah sistem yang berlandaskan informasi. Pengetahuan ini ditujukan untuk semua insan manusia di dunia, agar semua orang teredukasi secara dini dan dapat terhindar dari kasus penipuan. Dengan hadirnya teknologi yang membawa kebaikan bagi dunia, tentu saja harus mendapatkan perhatian yang baik bagi kita untuk selalu waspada akan tindak kejahatan yang dapat datang kapan saja. Contohnya seperti *phising*, *smishing*, dan *vishing*. Metode yang digunakan dalam penelitian ini adalah metode survei dan kajian literatur. Kegiatan survei angket dilakukan di Disdukcapil Kota Cimahi sebagai objek penelitian dan warga Kota Cimahi yang datang sebagai target penelitian. Dari hasil survei banyak dari responden warga kota Cimahi yang mendapatkan tindak kejahatan smishing. Sebagian responden memiliki kesadaran keamanan informasi yang baik. Lalu, dengan adanya website Dilandacita memudahkan responden untuk pengurusan kependudukan dan pencatatan sipil.

Kata Kunci*—Keamanan Informasi, phishing, smishing, vishing, website Dilandacita*

Abstract

Maintaining the confidentiality of information poses a significant challenge in today's technology-driven era. Information security is invaluable for individuals, businesses, governments, and global entities alike. It serves as a vital tool in preventing and identifying fraud within information-based systems. This knowledge is intended to educate people worldwide early on, helping them avoid falling victim to fraud. As technology advances for the greater good, it demands our vigilance against potential crimes like phishing, smishing, and vishing. The study utilized survey and literature review methods. Surveys were conducted using questionnaires at the Civil Registration Office of Cimahi City, targeting city residents. Survey findings indicated that many residents had experienced smishing incidents. Some respondents showed a commendable level of awareness regarding information security. Furthermore, the Dilandacita website aids respondents in handling population and civil registration matters efficiently.

Keywords*—Information Security, Phishing, Smishing, Vishing, Dilandacita Website*

Diajukan: 14 Juni 2024 *Disetujui: 16 Juli 2024* *Dipublikasi: 20 Juli 2024*

1. PENDAHULUAN

Teknologi hadir diantara insan manusia di dunia ini. Perubahan tersebut terjadi dari masa ke masa. Tentunya ini mewujudkan kemudahan bagi masyarakat semua di daerah manapun. Adanya teknologi tidak hanya memberikan kebaikan bagi kita, tetapi menghadirkan juga kejahatan yang tanpa disadari masyarakat

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

mengancamnya setiap detik, menit, jam dimanapun kita berada. Terkadang tidak semua orang menyambut teknologi untuk hal yang positif, kadang kala sebagian orang membawa teknologi ke arah yang negatif, seperti melakukan tindak kejahatan *phising*, *smishing*, dan *vishing*. Keamanan informasi tentu harus mulai disadari sejak dini. Oleh karena itu, perlu sekali edukasi kesadaran keamanan informasi bagi masyarakat diukur per beberapa bulan sekali, agar menekan tindak kejahatan teknologi yang sangat beragam.

Kesadaran keamanan informasi lebih berpusat kepada bagaimana seorang pekerja mencerna esensialnya dan juga keterkaitan dari peraturan, kebijakan dan panduan keamanan informasi, dan bagaimana mereka beraksi selaras dengan peraturan, kebijakan, dan panduan tersebut [1]. Dengan berkembangnya teknologi tentunya membuat semua masyarakat banyak melakukan aktivitas melalui internet. Berdasarkan data dari APJII mengenai penetrasi pengguna internet yang ada di wilayah Indonesia pada tahun 2019-2022 memperlihatkan terjadinya kenaikan jumlah orang pemakai internet yang mengakibatkan kenaikan [2].

Dengan meningkatnya pengguna internet, maka pasti kebocoran data pribadi warga negara kita sangatlah krusial. Seperti adanya kasus kebocoran data pengguna BPJS yang merugikan negara kira-kira sebesar 600 triliun rupiah yang dijelaskan dalam jurnal Hezkiel Bram Setiawan dan Fatma Ulfatun Najicha. Dari kasus tersebut seseorang ataupun kelompok yang melakukan tindakan peretasan ilegal tersebut akan dikenakan pidana. Perlu diketahui bahwasanya informasi sensitif milik warga negara kita dapat dijual.

Dengan begitu, pelaku dapat melakukan hal tersebut dari sudut manapun. Beberapa yang sering sekali terdengar ialah tindak kejahatan yang berhubungan dengan *email* (*phising*), berkorelasi dengan sms (*smishing*), dan berkaitan dengan suara (*vishing*). *Phising* merupakan ragam tindakan kejahatan yang membangun halaman situs *website* yang mana pelaku akan melakukan penyalinan sikap halaman situs web yang legal dan mendistribusikan url kepada seseorang yang sudah dijadikan sasaran dengan cara *spam*, teks, ataupun jejaring sosial seperti yang dipaparkan oleh Abdul Basil dan teman-temannya di dalam jurnalnya. Untuk prosedur pendistribusian *phising* yang dipakai untuk menyalurkan tindak kejahatan tersebut yakni terhadap sistem sasaran seperti dekstop, laptop, *smartphone*, dan lainnya. Dijelaskan bahwasanya sudah dikenali lima jenis proses pendistribusian *phising*, yakni dengan *email*, jaringan sosial *online* (OSN), layanan pesan singkat (SMS), *instant messenger* (IM), dan blog [3].

Sementara *smishing* merupakan formasi himpunan SMS dan *phising* yang mana pelaku akan mendistribusikan SMS yang mengandung isi yang berbahaya pada penerima SMS yang menjadi korban [4]. Isi dari pesan tersebut kadang-kadang akan memberikan *link* yang menunjukkan pengguna untuk membuka sistus *website* yang memiliki aplikasi yang sangat berbahaya. Saat melakukan *smishing*, pelaku akan melakukan perancangan antarmuka pengguna dengan baik sehingga pengguna tidak dapat mengenali yang mana situs web yang sah atau legal dengan yang palsu atau ilegal. Pelaku tersebut akan melakukan penyalinan kode sumber yang berasal dari situs yang legal agar terlihat sangat mirip dengan web yang dibangun olehnya. Begitu juga dengan *url* yang di transformasi agar sama dengan *url* web yang legal.

Vishing sendiri terlaksana saat pelaku berusaha untuk meraih informasi dari korban dengan telepon [5]. Tindakan-tindakan serangan tersebut berimbas sangat besar pada ekonomi dunia, mengambil dana organisasi dari kerugian moneter secara langsung, jam *downtime*, dan tempo remediasi yang dipaparkan oleh Biro Investigasi Federal (FBI) dan *Proofpoint* dalam jurnal Keith S. Jones dan teman-temannya. Menurut CyberEdge Group dalam jurnal yang sama, adanya penipuan yang menghabiskan kerugian dana sebesar US$19,7 Miliar terhadap 56 juta orang Amerika dalam 12 Bulan yang mendapatkan panggilan penipuan, maka mereka sudah menjadi pusat perhatian komunitas

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

keamanan siber. Oleh karena itu, langkah yang esensial untuk mengetahui dan menekan efek tersebut ialah dapat mengetahui cara penyerang melakukan *social engineering.*

2. METODE PENELITIAN

Penulis menggunakan metode penelitian deskriptif. Penelitian deskriptif yang dipakai adalah jenis penelitian survei. Survei disebar untuk beberapa warga Kota Cimahi. Selain itu, peneliti juga menggunakan metode penelitian kajian pustaka. Berikut merupakan alur penelitian yang dilakukan.

a) Mencari topik yang akan diteliti.
b) Memilah topik dan memfokuskan satu topik untuk diteliti.
c) Persiapan penelitian dengan membuat pertanyaan sesuai dengan topik yakni mengenai *phising, smishing,* dan *vishing.*
d) Melakukan pengecekan isi pertanyaan survei.
e) Mengerjakan perbaikan pertanyaan survei.
f) Melaksanakan penyebaran angket pada warga kota Cimahi selama 4 hari.
g) Selanjutnya melakukan penginputan data.
h) Lalu dilakukan pengolahan data pada data angket yang sudah terisi.

3. HASIL PENELITIAN

Keamanan Informasi merupakan cara kita melakukan preventif terhadap penipuan ataupun melakukan pendeteksian yang berlandaskan penipuan di suatu sistem berbasis informasi [6]. Adanya teknologi memudahkan semua manusia di bumi. Tentunya semua kemudahan tersebut membuat pengguna dapat mengakses apapun dengan mudah dan praktis. Hal tersebut tentunya membawa hal yang positif, namun di sisi lain memberikan dampak negatif dalam hal keamanan. Untuk itu, keamanan informasi sangatlah esensial dan harus menjadi pusat perhatian oleh orang banyak maupun organisasi yang berkaitan. Hal tersebut tentu memicu pertanyaan kepada tiap orang yang menggunakan internet. Kemungkinan besar atau kemungkinan kecil mereka sadar akan keamanan informasi. Untuk itu, lihatlah dari diri sendiri, apakah data personal gampang kita bagikan tanpa memikirkan hal tersebut menyebabkan kebocoran data ataukah kita sebagai seorang pekerja membawa data manajemen kita bocor, dan sebagainya. Untuk itu diperlukan manajemen keamanan informasi yang baik bagi perusahaan ataupun sebuah organisasi. Yang paling penting ialah kesadaran keamanan informasi dari masing-masing insan manusia di dunia ini, agar kita dapat saling menjaga satu sama lain data personal yang dimiliki dan menekan angka kebocoran data ataupun penyerangan data dalam sebuah sistem informasi.

Berdasarkan beberapa jurnal yang telah dibaca melahirkan beberapa pertanyaan yang digunakan untuk survei keamanan informasi mengenai *phishing* [7], *smishing* [8], dan *vishing* [9] pada warga Kota Cimahi.

3.1. Hasil survei kesadaran keamana informasi atas *phishing, smishing,* dan *vishing*

3.1.1 Perangkat Teknologi Informasi

a) Handphone

Berdasarkan survei yang telah dilakukan dengan pertanyaan "Apakah perangkat teknologi informasi yang Bapak/Ibu gunakan adalah handphone (HP) ?" didapati bahwa 100% warga Cimahi sekitar 96 orang memakai Handphone.

Gambar 3.1.1 a) Bagan perangkat teknologi informasi handphone (HP) yang digunakan

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

b) Laptop

Berdasarkan survei yang telah dilakukan dengan pertanyaan "Apakah perangkat teknologi informasi yang Bapak/Ibu gunakan adalah laptop?" didapati bahwa 66.7% atau 64 orang warga Cimahi memakai laptop dan 33.3% atau 32 Orang warga Cimahi tidak menggunakan laptop.

Gambar 3.1.1 b) Bagan perangkat teknologi informasi laptop yang digunakan

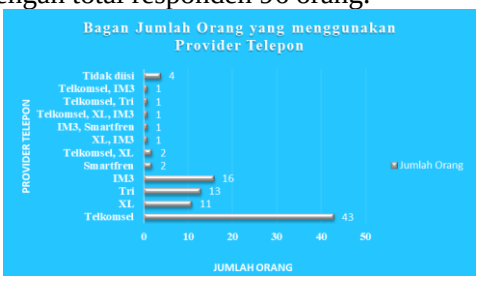
c) Ipad/Tab

Berdasarkan survei yang telah dilakukan dengan pertanyaan "Apakah perangkat teknologi informasi yang Bapak/Ibu gunakan adalah ipad/tab ?" didapati bahwa 4.2% atau 4 orang warga Cimahi memakai Ipad/Tab dan 95.8% atau 92 Orang warga Cimahi tidak menggunakan Ipad/Tab.

Gambar 3.1.1 c) Bagan perangkat teknologi informasi ipad/tab yang digunakan

3.1.2 Provider Telepon

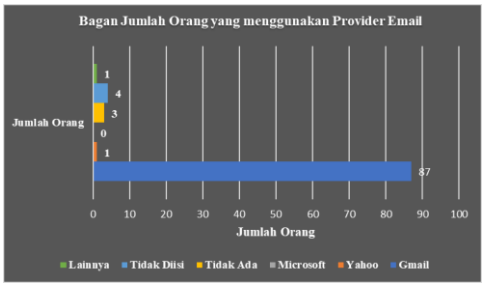
Berdasarkan survei yang telah dilakukan dengan pertanyaan "Yang manakah provider (nomor kartu telepon) yang Bapak/Ibu gunakan ? (Centang di kotak berikut)" didapati bahwa pemakai Telkomsel sebanyak 43 orang, pemakai XL sebanyak 11 orang, pemakai Tri sebanyak 13 orang, pemakai IM3 sebanyak 16 orang, pemakai *smartfren* sebanyak 2 orang, pemakai Telkomsel dan XL sebanyak 2 orang, pemakai XL dan IM3 sebanyak 1 orang, pemakai IM3 dan *smartfren* sebanyak 1 orang, pemakai Telkomsel, XL, dan IM3 sebanyak 1 orang, pemakai Telkomsel dan Tri sebanyak 1 orang, pemakai Telkomsel dan IM3 sebanyak 1 orang, dan tidak mengisi pertanyaan ini sebanyak 1 orang dengan total responden 96 orang.



Gambar 3.1.2 Bagan Jumlah Orang yang menggunakan Provider Telepon

3.1.3 Provider Email

Berdasarkan survei yang telah dilakukan dengan pertanyaan "Apa provider email yang Bapak/Ibu gunakan ?" didapati bahwa pemakai Gmail sebanyak 87 orang, pemakai *yahoo* sebanyak 1 orang, pemakai *microsoft* tidak ada, pemakai provider lainnya sebanyak 1 orang, tidak memiliki *email* sebanyak 3 orang, dan tidak mengisi pertanyaan ini sebanyak 4 orang.



Gambar 3.1.3 Bagan Jumlah Orang yang menggunakan Provider Email

3.1.4 Formulir *Online*

Berdasarkan survei yang telah dilakukan dengan pertanyaan "Sebelumnya apakah Bapak/Ibu pernah mengisi Google Formulir atau formulir online untuk melakukan sesuatu sehingga memberikan data pribadi?" didapati bahwa 73% atau 70 orang warga Cimahi memakai pernah mengisi formulir *online* dan 27% atau 26 Orang warga Cimahi tidak pernah mengisi formulir *online*.

p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

Gambar 3.1.4 Bagan Jumlah Orang yang mengisi Formulir Online

3.1.5 Memasukkan NIK/KK selain aplikasi Disdukcapil

Berdasarkan survei yang telah dilakukan dengan pertanyaan "Apakah Bapak/Ibu pernah memasukkan NIK atau KK di sistem selain dari aplikasi Disdukcapil ?" didapati bahwa 56% atau 54 orang warga Cimahi pernah input NIK/KK selain di aplikasi Dilandacita dan 44% atau 42 Orang warga Cimahi tidak pernah melakukan hal tersebut.

Gambar 3.1.5 Bagan Jumlah Orang yang pernah input NIK/KK selain Web Dilandacita

3.1.6 *Website* Digitalisasi Layanan Adminduk Kota Cimahi

Berdasarkan survei yang telah dilakukan dengan pertanyaan " Apakah adanya website Digitalisasi Layanan Adminduk Cimahi Kota lebih memudahkan pengajuan Bapak/Ibu di Disdukcapil?" didapati bahwa 74% atau 71 orang warga Cimahi menjawab bahwa *websiste* Dilandacita memudahkan dalam pengajuan dan 26% atau 25 orang warga Cimahi tidak menjawab tidak memudahkan dalam pengajuan.

Gambar 3.1.6 Bagan Jumlah Orang yang menjawab Web Dilandacita memudahkan pengajuan

3.1.7 KTP

Berdasarkan survei yang telah dilakukan dengan pertanyaan "Apakah Bapak/Ibu pernah memberikan foto KTP dan sebagainya di aplikasi online/mobile/website selain dari aplikasi Disdukcapil?" didapati bahwa 42% atau 40 orang warga Cimahi menjawab bahwa pernah memberikan foto KTP selain dari web Dilandacita dan 58% atau 56 orang warga Cimahi tidak pernah memberikan foto KTP selain di web Dilandacita.

Gambar 3.1.7 Bagan Jumlah Orang yang pernah memberikan foto KTP selain di web Dilandacita

3.1.8 Pembelian Kuota atau Pulsa di Konter/Aplikasi/ATM

Berdasarkan survei yang telah dilakukan dengan pertanyaan "Apakah Bapak/Ibu pernah mengisi kuota/pulsa di konter/aplikasi/ATM?" didapati bahwa 71% atau 68 orang warga Cimahi menjawab bahwa pernah pembelian kuota atau pulsa di konter/aplikasi/atm dan 29% atau 28 orang warga Cimahi tidak pernah pembelian kuota atau pulsa di konter/aplikasi/atm**.**

p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

Gambar 3.1.8 Bagan Jumlah Orang yang pernah membeli kuota/pulsa di konter/aplikasi/atm

3.1.9 Membayar Tagihan Bulanan secara *online*

Berdasarkan survei yang telah dilakukan dengan pertanyaan "Apakah Bapak/Ibu pernah membayar tagihan bulanan secara online?" didapati bahwa 60% atau 58 orang warga Cimahi menjawab bahwa pernah membayar tagihan bulanan secara *online* dan 38% atau 40 orang warga Cimahi tidak pernah membayar tagihan bulanan secara *online.*

Gambar 3.1.9 Bagan Jumlah Orang yang pernah membayar tagihan bulanan secara online

3.1.10 Pencarian Nama Lengkap di *Google*

Berdasarkan survei yang telah dilakukan dengan pertanyaan "Apakah Bapak/Ibu pernah mencoba mencari nama lengkap Bapak/Ibu di google? Apakah ada yang terekspos Bapak/Ibu?" didapati bahwa 19% atau 18 orang warga Cimahi menjawab bahwa pernah melakukan pencarian nama lengkap di *google* serta terekspos dan 81% atau 78 orang warga Cimahi tidak pernah melakukan pencarian nama lengkap di *google*.

Gambar 3.1.10 Bagan Jumlah Orang yang pernah mencari nama lengkap di google dan terekspos

3.1.11 Media Sosial

Berdasarkan survei yang telah dilakukan dengan pertanyaan "Media sosial apa yang Bapak/Ibu gunakan? (Centang di kotak berikut)" didapati bahwa warga cimahi yang menggunakan instagram sebanyak 28 orang, menggunakan *facebook* sebanyak 21 orang, menggunakan *youtube* sebanyak 5 orang, menggunakan *whatsapp* 5 orang, menggunakan *twitter* sebanyak 1 orang, menggunakan instagram dan facebook sebanyak 11 orang, menggunakan facebook dan youtube sebanyak 2 orang, menggunakan instagram dan youtube sebanyak 2 orang, menggunakan instagram, facebook, dan youtube 18 orang, tidak menyebutkan 1 orang, tidak ada 1 orang, dan tidak diisi 1 orang.

Gambar 3.1.11 Bagan Jumlah Orang yang memakai media social

3.1.12 *Phising*

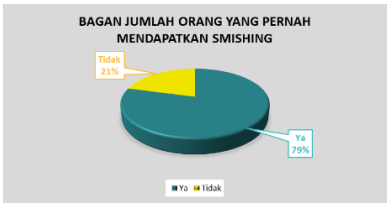
Berdasarkan survei yang telah dilakukan dengan pertanyaan "Apakah Bapak/Ibu pernah mendapatkan email yang mengatasnamakan pihak tertentu dan memancing Bapak/Ibu untuk klik link yang dicantumkan dalam email (*phising*)?" didapati bahwa 27% atau 26 orang warga Cimahi menjawab bahwa pernah mendapatkan *phising* dan 73% atau 70 orang warga Cimahi tidak pernah mendapatkan *phising*.

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

Gambar 3.1.12 Bagan Jumlah Orang yang pernah mendapatkan phising

3.1.13 *Smishing*

Berdasarkan survei yang telah dilakukan dengan pertanyaan "Apakah Bapak/Ibu pernah mendapatkan penipuan melalui SMS (smishing) ? (contoh memenangkan undian dan disertakan link untuk lanjutan hadiahnya)" didapati bahwa 79% atau 76 orang warga Cimahi menjawab bahwa pernah mendapatkan *smishing* dan 21% atau 20 orang warga Cimahi tidak pernah mendapatkan *smishing*.



Gambar 3.1.13 Bagan Jumlah Orang yang pernah mendapatkan smishing

3.1.14 *Vishing*

Berdasarkan survei yang telah dilakukan dengan pertanyaan "Apakah Bapak/Ibu pernah mendapatkan penipuan melalui telepon (*vishing*)?" didapati bahwa 53% atau 51 orang warga Cimahi menjawab bahwa pernah mendapatkan *vishing* dan 47% atau 45 orang warga Cimahi tidak pernah mendapatkan *vishing*.

Gambar 3.1.13 Bagan Jumlah Orang yang pernah mendapatkan *vishing*

3.1.15 Tindak kejahatan yang sering didapatkan

Berdasarkan survei yang telah dilakukan dengan pertanyaan "Tindak kejahatan yang mana yang sering Bapak/Ibu dapatkan? *phising*, *smishing*, atau *vishing*? (Centang di kotak berikut)." didapati bahwa yang mendapatkan tindak kejahatan *phising* sebanyak 8 orang, *smishing* sebanyak 35 orang, *vhising* sebanyak 5 orang. Sedangkan, yang mendapatkan ketiga tindak kejahatan tersebut sebanyak 7 orang, hanya mendapatkan dua tindak kejahatan yakni *phising* dan *vishing* sebanyak 2 orang, mendapatkan kejahatan *smishing* dan *vishing* sebanyak 9 orang, mendapatkan tindak kejahatan *phising* dan *smishing* sebanyak 2 orang, tidak sering mendapatkan tindak kejahatan-kejahatan tersebut sebanyak sebanyak 9 orang, tidak pernah mendapatkan tindak kejahatan-kejahatan tersebut sebanyak 14, tidak mengisi sebanyak 3 orang, tidak ada sebanyak 1 orang, tidak menjawab sebanyak 1 orang.

Gambar 3.1.14 Bagan Jumlah Orang yang sering mendapatkan tindak kejahatan

4. PEMBAHASAN

Kesadaran akan keamanan informasi sangatlah penting. Di era yang serba digital ini menjaga kerahasiaan, integritas, dan ketersediaan (CIA) ialah *challenge* yang harus dapat semua orang lewati [10]. Di zaman teknologi seperti ini semakin hari semakin banyak yang memakai internet untuk keperluan sehari-harinya. Tentunya setiap teknologi yang ada mempunyai informasi yang sangat sensitif terkait *user* maupun perusahaan. Oleh karena itu, mulai dari karyawan, *user*, hingga perusahaan harus mempunyai kesadaran akan keamanan informasi baik secara individu maupun secara kelompok.

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

Dengan adanya kesadaran akan keamanan informasi maka akan terhindar dari kerugian masalah keuangan, reputasi, dan aset yang esensial. Oleh karenanya, sebuah perusahaan harus dapat melindungi sistem yang dimilikinya. Begitu juga dengan keamanan sistem pribadi. Fokus utama dari perlindungan informasi ialah menjaga keorisinilan informasi untuk berbagai orientasi bisnis [11]. Setiap orang penting sekali untuk dapat mencerna dengan baik mengenai kesadaran keamanan informasi (*information security awareness)*, karena dengan memahaminya maka akan menekan risiko keamanan informasi. Kesadaran keamanan informasi sendiri cenderung ke arah bagaimana seorang karyawan dapat mengetahui bagaimana peraturan, tata tertib, dan petunjuk keamanan informasi di dalam organisasi atau perusahaan mereka. Model *Knowledge-Attitude-Behaviour* (KAB) sendiri sudah diaplikasikan terhadap lingkungan *information security awareness* yang mana berdasarkan hal itulah dapat dilihat bahwasanya saat wawasan seorang karyawan mengenai tindakan keamanan informasi yang bertambah, perilaku mereka meninggi, maka akan membentuk sikap keamanan informasi yang kian baik [12]. Artinya jika orang-orang dapat memahami peraturan, tata tertib, dan petunjuk keamanan informasi secara universal akan menekan pula risiko keamanan informasi yang ada. Begitu juga jika pengetahuan semua orang mengenai keamanan informasi meningkat dan sikap mereka meningkat, maka akan membangun sebuah perilaku keamanan informasi yang baik pula.

Jika semua orang mempunyai kesadaran akan keamanan informasi sejak dini, maka tindak kejahatan apapun dapat dicegah. Dewasa ini, tindak kejahatan yang banyak sekali bermunculan ialah *phising, smishing,* dan *vishing*. Dalam serangan *phising* pelaku mengumpulkan data sensitif milik korban, seperti akun *user*, rincian *login,* nomor kartu kredit atau debit, dan lainnya [13]. Umumnya pelaku akan membawa korban ke situs palsu yang mereka buat. Penyerangan diawali dengan pengiriman *link* situs palsu ke *email* korban, agar korban klik situs tersebut, mereka akan seolah-olah menjadi pihak yang terkenal dan banyak orang ketahui.

Selain *phising,* sejak dahulu pun marak sekali terjadi tindak kejahatan *smishing*. *Smishing* merupakan tindak kejahatan yang dilakukan melalui pengiriman sms kepada korban. Contoh nya seperti pelaku berpura-pura menjadi pihak yang dipercaya dan mengirimkan sms kepada korban bahwasanya ia mendapatkan hadiah jutaan rupiah. Tantangannya ialah pendeteksian *smishing* dalam konteks jumlah minimal informasi yang di berikan oleh pelaku atau penyerang [14].

Tidak hanya melalui SMS, serangan tindak kejahatan juga dapat melalui *vishing*. *Vishing* sendiri bersumber dari suara dan *phising* yang mana dilakukan untuk memvisualisasikan tindak kejahatan yang dilakukan dengan *voice over the internet protocol* (VoIP) [15]. Tindak kejahatan tersebut mengarah ke *phising* telepon untuk membohongi orang agar mereka memberikan informasi sensitif untuk sebuah verifikasi. Contohnya seperti panggilan dari bank. *Phising* respon suara yang saling melakukan aksi dengan memakai sistem tanggapan suara yang saling aktif untuk membuat sasaran menginput informasi personal yang mana seakan-akan hal tersebut datang dari bisnis atau bank yang sah. Tindak kejahatan ini dapat dilaksanakan dengan *email* suara, telepon rumah, ataupun telepon [16].

Seperti yang sudah kita ketahui, berita mengenai pelanggaran keamanan sudah menjadi tren di kalangan masyarakat *modern*, karena peristiwa tersebut sudah memperburuk kecemasan yang berkenaan dengan pelanggaran potensi privasi [17]. Banyak sekali jenis serangan yang dapat mengguncang keamanan informasi pribadi kita, bahkan kejahatan siber tersebut dapat mencuri informasi sensitive pengguna. Informasi pribadi kita dapat dicuri oleh orang yang tidak bertanggung jawab melalui beberapa bentuk seperti *phishing*, *smishing*, dan *vishing*. Salah satu metode rekayasa social yang digunakan untuk mendapatkan informasi pribadi adalah *phishing* [18]. Saluran dari komunikasi yang banyak sekali dipakai untuk melakukan penyerangan

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

phishing ialah *email*, pesan instan, dan lainnya [19]. Sedangkan *smishing* dilakukan oleh penyerang untuk mencuri informasi pribadi dari korban yang dituju dengan cara mengirimi mereka pesan sms daripada media lainnya. Biasanya isi dari sms terdiri dari data seperti aplikasi *smartphone, url* situs web, pesan ucapan, dan nomor telepon seluler [20]. Tindak kejahatan smishing ini lebih berbahaya jika dibandingkan dengan phishing karena Tindakan manusia dan upaya realisasi nya rendah yang mana lebih mudah mengelabui seseorang diperangkat seluler daripada desktop. Menurut orang-orang ponsel lebih aman dibandingkan computer. Padahal ponsel mempunyai keterbatasan dan tidak dapat langsung mengamankan ponsel terhadap ancaman smishing.

Sementara *vishing* (*voice phising*) ialah jenis tindak kejahatan rekayasa social yang sangat efektif dan terpusat memakai ucapan untuk mempengaruhi korban agar untuk memberikan data pribadinya ke penyerang. Saat ini tindak kejahatan *vishing* ini sukar sekali dideteksi, karena peretas menggunakan kecerdasan buatan untuk menyalin pola bicaranya [18]. Tindak kejahatan *vishing* ini dilakukan dengan bentuk *voice*, pesan tersebut memungkinkan penyerang mengatur korban untuk menelepon nomor atau mengunjungi sebuah situs web untuk memvalidasi data akun mereka ataupun mengatasi permasalahan keamanan [19]. Tindak kejahatan vishing ini merupakan serangan *phishing* yang sama yang dikerjakan memakai telepon dan layanan telepon seperti *telephone banking* [20].

5. KESIMPULAN

Dari survei kepada 96 reponden warga kota Cimahi (data yang dikumpulkan belum mewakili populasi warga) yang sedang memiliki keperluan di Dinas Kependudukan dan Pencatatan Sipil Kota Cimahi terlihat bahwasanya banyak dari responden yang menggunakan *handphone* daripada laptop dan ipad atau tab. Artinya banyak yang sudah memakai internet dalam segala aktivitasnya walaupun tidak semua dari responden menggunakan laptop maupun ipad atau tab. Selain itu terlihat pula *provider* telepon yang banyak digunakan oleh responden adalah telkomsel dan *provider email* yang banyak dipakai adalah *gmail.* Berkaitan dengan internet, warga Kota Cimahi yang mengisi survei banyak yang menjawab pernah mengisi formulir *online* yang mana artinya jika formulir itu bukan dari suatu organisasi yang sah, maka data pribadi akan terancam diambil alih oleh penyerang. Namun, jika tidak, maka akan aman di suatu badan organisasi yang sah. Selain itu masih banyak dari responden yang memasukkan NIK atau KK ke sistem selain *website* Dilandacita yang dimiliki oleh Dinas Kependudukan dan Pencatatan Sipil Kota Cimahi, tetapi dalam hal membagikan foto KTP, banyak dari responden yang menjawab tidak pernah mengirimkannya selain ke sistem *website* Dilandacita. Selain itu banyak dari responden juga yang membeli pulsa di konter/aplikasi/ATM serta melakukan pembayaran bulanan secara *online.* Berbeda dengan pencarian nama lengkap di *google* banyak sekali yang menjawab tidak pernah mencari apakah identitas nya tersebar di *google* dengan mencari nama lengkapnya. Banyak juga dari pengisian survei yang menjawab menggunakan media sosial *instagram* serta ketiga media sosial lainnya termasuk *instagram* dan bertambah dengan *facebook* dan *youtube*. Dari tiga tindak kejahatan yang paling sering didapati ialah *smishing*, tetapi daripada *vishing* masih lebih banyak yang mendapatkan tindak kejahatan *phising*. Terakhir banyak dari responden yang menjawab bahwasanya sistem *website* Dilandacita memudahkan dalam pengurusan kependudukan dan pencatatan sipil.

6. SARAN

Sarannya kedepannya semoga bisa melakukan penelitian untuk kota lainnya tentang *phishing, smishing,* dan *vishing*

REFERENSI

[1] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, “Individual Differences and

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

Information Security Awareness," *Comput. Human Behav.*, vol. 69, pp. 151–156, 2017, doi: 10.1016/j.chb.2016.11.065.

[2] H. B. Setiawan and F. U. Najicha, "PERLINDUNGAN DATA PRIBADI WARGA NEGARA INDONESIA TERKAIT DENGAN KEBOCORAN DATA," vol. 6, no. 1, pp. 976–982, 2022.

[3] A. K. Jain and B. B. Gupta, "A survey of phishing attack techniques, defence mechanisms and open research challenges," *Enterp. Inf. Syst.*, vol. 16, no. 4, pp. 527–565, 2022, doi: 10.1080/17517575.2021.1896786.

[4] S. Mishra and D. Soni, "Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis," *Futur. Gener. Comput. Syst.*, vol. 108, pp. 803–815, 2020, doi: 10.1016/j.future.2020.03.021.

[5] K. S. Jones, M. E. Armstrong, M. K. Tornblad, and A. Siami Namin, *How social engineers use persuasion principles during vishing attacks*, vol. 29, no. 2. 2020.

[6] A. Ramadhani, "Keamanan Informasi," *Nusant. - J. Inf. Libr. Stud.*, vol. 1, no. 1, p. 39, 2018, doi: 10.30999/n-jils.v1i1.249.

[7] M. H. Wibowo and N. Fatimah, "ANCAMAN PHISHING TERHADAP PENGGUNA SOSIAL MEDIA DALAM DUNIA CYBER CRIME," *JOEICT(Jurnal Educ. Inf. Commun. Technol.*, vol. 1, no. 1, pp. 1–5, 2017, [Online]. Available: https://www.jurnal.stkippgritulungagung.ac.id/index.php/joeict/article/view/69.

[8] A. D. Putra, J. D. Santoso, M. Y. Nugraha, and I. Ardiyansyah, "ANALISIS ANCAMAN SMISHING PADA SMARTPHONE MENGGUNAKAN STRIDE SEBAGAI PEMODELAN ANCAMAN," *J. Teknol. Inf. dan Komput.*, vol. 8, no. 3, pp. 173–179, 2022.

[9] K. Choi, J. L. Lee, and Y. T. Chun, "Voice phishing fraud and its modus operandi," *Secur. J.*, vol. 30, no. 2, pp. 454–466, 2017, doi: 10.1057/sj.2014.49.

[10] K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," *Comput. Secur.*, vol. 106, p. 102267, 2021, doi: 10.1016/j.cose.2021.102267.

[11] S. Hina and P. D. D. Dominic, "Information security policies' compliance: a perspective for higher education institutions," *J. Comput. Inf. Syst.*, vol. 60, no. 3, pp. 201–211, 2020, doi: 10.1080/08874417.2018.1432996.

[12] A. Wiley, A. McCormac, and D. Calic, "More than the individual: Examining the relationship between culture and Information Security Awareness," *Comput. Secur.*, vol. 88, pp. 1–31, 2020, doi: 10.1016/j.cose.2019.101640.

[13] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, "A comprehensive survey of AI-enabled phishing attacks detection techniques," *Telecommun. Syst.*, vol. 76, no. 1, pp. 139–154, 2021, doi: 10.1007/s11235-020-00733-2.

[14] S. Mishra and D. Soni, "DSmishSMS-A System to Detect Smishing SMS," *Neural Comput. Appl.*, vol. 0123456789, 2021, doi: 10.1007/s00521-021-06305-y.

[15] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," *Futur. Internet*, vol. 11, no. 4, 2019, doi: 10.3390/FI11040089.

[16] R. S. Deora and D. M. Chudasama, "Brief Study of Cybercrime on an Internet," no. June, 2021, doi: 10.37591/JoCES.

[17] S. Mamonov and R. Benbunan-Fich, "The impact of information security threat awareness on privacy-protective behaviors," *Comput. Human Behav.*, vol. 83, pp. 32–44, 2018.

[18] R. Fatima, A. Yasin, L. Liu, and J. Wang, "How persuasive is a phishing email? A phishing game for phishing awareness," *J. Comput. Secur.*, vol. 27, no. 6, pp. 581–612, 2019.

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

[19] S. Salloum, T. Gaber, S. Vadera, and K. Shaalan, "Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey," *Procedia CIRP*, vol. 189, no. 2019, pp. 19–28, 2021.

[20] C. Balim and E. S. Gunal, "Automatic Detection of Smishing Attacks by Machine Learning Methods," pp. 1–3, 2019.