Madani: Jurnal Ilmiah Multidisiplin
Volume 2, Nomor 5, Juni 2024, Halaman 449-458
Licenced by CC BY-SA 4.0
E-ISSN: 2986-6340
DOI: https://doi.org/10.5281/zenodo.11496678

Pengaruh Keamanan Two Factor Authentication Terhadap Pencurian Data (Cyber Crime) Pada Media Sosial

Tantri Aprilia[1], Bayu Seno Pitoyo[2], Achmad Fauzi[3], Reifa Galih Ramadhanti[4], Rizty Dwi Nurazizah[5], Eny Trisno Wanti[6], Muhammad Yusuf Nugroho[7], Bagus Naufal Putra Shawa[8], Andhika Rifki Prasetyo[9]
[1-9]Fakultas Ekonomi dan Bisnis Bhayangkara Jakarta Raya
Email: tanaprl3@gmail.com[1]

Abstract
Security management refers to effective and efficient steps that must be taken to carry out security efforts and prevent losses so that disturbances that can cause losses do not occur. In the 4.0 era, people are required to utilize the latest technology to make it easier to solve problems, including data security. Cybercriminals often steal and manipulate data. Various data security methods have been developed, one of which is two factor authentication (2FA) which is widely used on social media. Gen-Z's lack of awareness about data security often leads to data leaks or account hijacking. By using 2FA, this problem can be overcome and provide more protection against cyber threats. This research aims to determine the effect of two factor authentication security on data theft on social media. This research uses qualitative methods with data collected from previous research as reference material. The results of this research show that public awareness and enlightenment regarding cybercrime is related to the use of social media.
Keywords : *Two Factor Authentication, Cyber Crime, dan Media Sosial*

Abstract
Manajemen keamanan mengacu pada langkah-langkah efektif dan efisien yang harus dilakukan untuk melakukan upaya pengamanan dan mencegah kerugian agar tidak terjadi gangguan yang dapat menimbulkan kerugian. Di era 4.0, masyarakat dituntut untuk memanfaatkan teknologi terkini untuk mempermudah penyelesaian masalah, termasuk keamanan data. Pelaku kejahatan cyber sering mencuri dan memanipulasi data. Berbagai metode pengamanan data telah dikembangkan, salah satunya *two factor authentication* (2FA) yang banyak digunakan di media sosial. Kurangnya kesadaran Gen-Z tentang keamanan data sering menyebabkan kebocoran data atau pembajakan akun. Dengan menggunakan 2FA, masalah ini dapat diatasi dan memberikan perlindungan lebih terhadap ancaman cyber. Penelitian ini bertujuan untuk mengetahui pengaruh keamanan two factor authentication terhadap pencurian data pada media sosial. Penelitian ini menggunakan metode kualitatif dengan data-data yang dikumpulkan dari penelitian terdahulu sebagai bahan acuan. Hasil penelitian ini menunjukkan bahwa kewaspadaan dan pencerahan bagi masyarakat terhadap kejahatan *cybercrime* pada penggunaan media sosial.
Keywords: *Social Media, Cybercrime, and Two Factor Authentication*

PENDAHULUAN

Manajemen keamanan mengacu pada langkah-langkah efektif dan efisien yang harus dilakukan untuk melakukan upaya pengamanan dan mencegah kerugian agar tidak terjadi gangguan yang dapat menimbulkan kerugian. Manusia sebagai individu pada umumnya mempunyai dua keinginan utama dalam hidup, yaitu kebutuhan akan pangan dan kebutuhan akan rasa aman atau pertahanan diri agar dapat bertahan hidup (Hadiman, 2008).

Two Factor Authentication adalah proses otentikasi dua langkah dimana, selain menggunakan kata sandi, kode rahasia yang biasanya dikirim melalui layanan pesan singkat atau dibuat khusus untuk tujuan tersebut digunakan untuk memvalidasi akses oleh suatu akun (Setiawan, 2020).

Salah satu alasan media sosial begitu populer saat ini adalah karena media sosial memudahkan dan mempercepat orang dalam memproduksi dan berbagi konten. Teknologi informasi di era modern memudahkan segala hal selain pertukaran informasi dan balasan pesan. Teknologi informasi telah membuat banyak hal menjadi lebih mudah. Namun, jika ingin menggunakan media sosial dan mengkhawatirkan privasi data, ada banyak faktor yang perlu dipertimbangkan, termasuk keamanan dan perlindungan data. Saat ini, kebocoran informasi pribadi melalui media sosial merupakan hal yang sering terjadi.

Beberapa kasus cybercrime sering terjadi, seperti pencurian kartu kredit, hacking situs web tertentu, menyadap transmisi data orang lain, seperti email, dan memanipulasi data dengan memasukkan perintah yang tidak dikehendaki ke dalam program komputer. Dengan demikian, pelanggaran formal dan material mungkin terjadi dalam kejahatan komputer. Mengakses komputer orang lain tanpa izin disebut sebagai pelanggaran formal, sedangkan merugikan orang lain disebut sebagai pelanggaran materil. Karena cybercrime kini menjadi ancaman terhadap stabilitas, maka menjadi tantangan bagi pemerintah untuk mencapai keseimbangan antara teknologi computer khususnya jaringan internet.

KAJIAN PUSTAKA

Two Factor Aunthentication (2FA)

Dengan Two Factor Aunthentication (2FA), proses verifikasi keabsahan suatu akun dilakukan melalui langkah validasi kedua selain penggunaan password. Langkah kedua ini biasanya melibatkan penggunaan kode rahasia yang dibuat khusus untuk tujuan tersebut atau dikirim melalui layanan pesan singkat. Metode ini dapat menawarkan tingkat keamanan yang cukup baik pada layanan tertentu, seperti perbankan (Faridi, 2019). Pentingnya bagi remaja, khususnya pelajar, untuk memahami TFA atau Two Factor Aunthentication (Musu, Muhtamar, Palullu, & Patendean, 2022). Oleh karena itu, upaya penjangkauan dilakukan terhadap pengguna dalam menggunakan platform media sosial dan sering menjadi sasaran peretasan dan pembajakan akun.

Sistem keamanan yang dikenal sebagai otentikasi dua faktor meminta pengguna untuk memberikan dua bentuk identifikasi berbeda. Dengan melakukan ini, pengguna dapat membuat akun online mereka lebih aman (Saputra, 2021). Jika pengguna biasanya hanya menggunakan alamat email dan kata sandinya untuk masuk, maka langkah tambahan harus diambil untuk menerapkan autentikasi dua faktor. Situs web dengan autentikasi dua faktor biasanya tertaut ke nomor ponsel pengguna. Ilustrasi paling populer adalah otentikasi ponsel cerdas. Dalam hal ini, perangkat smartphone Anda akan menerima kode atau link one-time password (OTP) dari sistem (Szczygiel, 2023). Tujuannya adalah untuk mengkonfirmasi bahwa andalah yang login ke akun tersebut. Faktor kedua ini bisa didapatkan dengan meminta kode perangkat yang digunakan atau nomor CVV pada kartu kredit anda, bukan hanya smartphone saja. Akibatnya, pengguna biasanya perlu memverifikasi perilaku login mereka di ponsel cerdas mereka.

Otentikasi Faktor Tunggal (SFA), yang hanya memerlukan kata sandi, telah lama digunakan di perbankan online. Semakin banyak bank yang mulai menggunakan 2FA dalam beberapa tahun terakhir (Corkery, 2016). Proses 2FA mengharuskan pengguna untuk menyediakan dua bentuk otentikasi. Dengan menggunakan elemen dari dua kategori berbeda, identitas mereka dikonfirmasi (Dasgupta, Roy & Nag, 2017). Elemen verifikasi ini dapat dibagi menjadi satu dari lima kelompok:

1. Faktor pengetahuan, seperti frasa rahasia, PIN, atau kata sandi,
2. Barang Milik, seperti KTP, gantungan kunci, atau telepon pintar,
3. Faktor Inherensi: pengenalan suara, wajah, iris mata, dan sidik jari,
4. Indikator Geografis: alamat IP atau GPS,
5. Faktor Waktu: waktu lokal pelanggan, waktu sistem perangkat, dan waktu aktivitas masuk pada umumnya.

Kode sandi sekali pakai (OTP). Salah satu teknik paling populer untuk meningkatkan otentikasi adalah OTP sebagai 2FA. Mereka adalah string karakter alfanumerik atau numerik sekali pakai yang dihasilkan secara otomatis (Wigmore, 2018). Mereka tidak rentan terhadap serangan ulangan karena tidak dapat digunakan kembali. Artinya, menggunakan OTP dua kali akan menjadikannya tidak valid jika disadap oleh malware atau diketahui oleh seseorang yang mengawasi dari balik bahu seseorang. Kata sandi statis dapat digunakan sendiri, bersamaan dengan, atau sebagai tambahan OTP. Token keras, token lunak, dan layanan pesan singkat (SMS) adalah tiga cara paling populer bagi pelanggan untuk menerima OTP mereka.

Cyber Crime

Widodo (2013) mendefinisikan kejahatan dunia maya *(cyber crime)* sebagai segala aktivitas terkait komputer yang dilakukan oleh individu atau sekelompok individu yang berbadan hukum. Sebagai alat untuk melakukan aktivitas kriminal, dengan komputer sebagai sasarannya. Pertasan *(hacking)* adalah dimana pencuri dapat menyimpan materi terlarang, seperti perangkat lunak bajakan atau foto-foto pornografi, di sejumlah komputer jarak jauh. Selain itu, kejahatan yang muncul

termasuk serangan penolakan layanan, spam, pencurian kekayaan intelektual, dan penipuan lelang elektronik *(e-auction scam)* adalah contoh kejahatan dunia maya. Sejak penjahat dunia maya menggunakan teknologi baru untuk melancarkan serangan *cyber* terhadap pemerintah, perusahaan, dan individu, beberapa istilah ini sudah menjadi hal yang lumrah. Kejahatan-kejahatan ini mempunyai cakupan internasional, memberikan ancaman nyata bagi korban di mana pun dan menyebabkan kerugian yang signifikan baik secara fisik maupun virtual.

Kejahatan dunia maya adalah kejahatan yang dilakukan terhadap komputer dan sistem informasi dengan tujuan mendapatkan akses tidak sah ke suatu sistem atau mencegah pengguna yang sah untuk menggunakannya. *Cybercrime* berkembang dengan cepat, dan tren-tren baru sering bermunculan. Untuk mengatasi *Cybercrime*, penegak hukum harus selalu mengikuti perkembangan teknologi yang sedang berkembang dan memahami peluang yang ada untuk melakukan aktivitas kriminal. (Catur Nugroho, 2020) menyatakan bahwa beberapa istilah yang sering muncul dalam kejahatan dunia maya diantaranya:

1. Fraud
   Dalam industri Teknologi Informasi, istilah "fraud" mengacu pada tindakan penipuan yang disengaja dan melanggar hukum, berpotensi merugikan pihak ketiga, dan melibatkan kecurangan. Kesalahan yang disengaja, seperti tidak mengungkapkan informasi atau menyalahgunakan posisi seseorang untuk mendapatkan keuntungan, menimbulkan kerugian, atau membahayakan orang lain, disebut sebagai penipuan, menurut Chartered Institute of Public Finance and Accountancy (CIPFA). Pencurian, pemerasan, plagiarisme, dan pencurian merupakan contoh fraud dalam kehidupan sehari-hari.
2. Hacking
   Hacking adalah proses pembobolan suatu sistem dengan menggunakan sistem operasi sebagai gateway, atau dengan mencari dan menggunakan celah keamanan pada sistem atau jaringan komputer untuk mendapatkan akses ke sistem tersebut. Masuk ke suatu sistem dengan memanfaatkan algoritma peretasan kata sandi adalah salah satu contoh hacking (peretasan). Pelaku kejahatan peretasan ini dikenal sebagai "hacker", yang biasanya adalah seseorang yang senang mempelajari sistem komputer dan bahasa pemrograman. Hacker sering kali dipandang sebagai otoritas di bidangnya, menguasai seni dan ilmu perangkat lunak, serta mampu melakukan tugas yang tidak pernah dimaksudkan oleh pembuat sistem asli.
3. Cracking
   Meskipun tujuannya biasanya tidak baik, cracking beroperasi dengan prinsip yang sama dengan hacking. Cracker umumnya memiliki kecenderungan untuk mencuri, menghapus, bahkan mengubah data, termasuk informasi sensitif. Cracker berupaya mendistribusikan perangkat lunak tanpa membayar royalti kepada pemilik program atau memecahnya secara gratis. Mereka mengubah perangkat lunak untuk menghapus atau menonaktifkan elemen yang dianggap tidak diinginkan. Fitur-fitur ini biasanya dikaitkan dengan teknik perlindungan, seperti kunci perangkat keras, pemeriksaan tanggal, pemeriksaan CD, perlindungan hak cipta, versi uji coba/demo, nomor seri, dan iklan.
4. Carding
   Hal yang sama juga berlaku pada carding. Biasanya, carder mencari dan mencuri informasi akun dari sistem pembayaran atau perbankan online. Dengan membobol nomor rekening dan kata sandi, mereka mengambil kendali atas dana elektronik atau rekening pembayaran online pemegang rekening. Biasanya, carding dilakukan dengan kartu kredit atau di pengecer online yang berbeda.

Media Sosial

Media sosial pada dasarnya adalah kemajuan terkini dalam teknologi web yang berbasis internet dan memfasilitasi komunikasi di antara semua pengguna. Terlibat dalam partisipasi online, berbagi, dan pembentukan jaringan, serta penyebaran konten secara mandiri. Pengetahuan ini membawa kita pada kesimpulan bahwa orang menggunakan media sosial untuk berinteraksi satu sama lain secara online. Purnama (2011) menyatakan bahwa media sosial memiliki sejumlah keistimewaan, seperti:

1. Lakukan kontak: Jangkauan media sosial dari khalayak lokal hingga khalayak di seluruh dunia.
2. Ketersediaan: Masyarakat dapat dengan mudah mengakses media sosial dengan biaya yang terjangkau.

3. Kepraktisan: Karena media sosial tidak memerlukan pengetahuan atau pelatihan khusus, maka penggunaannya relatif mudah.
4. Realitas (jangka pendek): Penonton mungkin bereaksi lebih cepat saat menggunakan media sosial.
5. Abadi: Media sosial mempermudah dan mempercepat pengeditan atau penggantian komentar.

Dari segi metode kerja komputer, media sosial pada dasarnya sama. Tiga komponen sosialisasi perkenalan, komunikasi, dan kerja sama hadir di media sosial. yang, seperti komputer, menciptakan suatu sistem. Media sosial menciptakan sistem antara manusia dan Masyarakat (Puntoadi, 2017). Tergantung pada bagaimana pengguna menggunakan media sosial, keberadaan platform itu sendiri dapat memberikan dampak positif atau negatif.

Andreas Kaplan dan Michael Haenlein dalam (Bersosmed, 2017) mengidentifikasi enam kategori platform media sosial, yaitu:

1. *Collaborative Projects*. Wikipedia adalah ensiklopedia kolaboratif akses terbuka yang memungkinkan pengguna berkontribusi, mengedit, dan menambahkan konten. Wikipedia banyak digunakan oleh siswa untuk menyelesaikan pekerjaan rumah dan tugas mereka. Karena sifatnya yang "kolaboratif", satu-satunya hal yang perlu di ingat adalah siapa pun dapat menulis atau mengedit informasi. Setelah mempelajari lebih jauh dari wadah ini, maka diperlukan penjelasan menyeluruh mengenai hal tersebut.
2. *Content Communities*. YouTube adalah situs web yang banyak digunakan untuk berbagi video yang memungkinkan pengguna memuat, menonton, dan distribusikan klip video gratis. Kita dapat memposting video kita sendiri ke YouTube untuk mempromosikan film baru atau klip video baru untuk musisi.
3. *Blogs and microblogs*. Saat ini, Twitter adalah salah satu platform media sosial yang paling banyak digunakan. Implementasi langsung hanya dengan mengubah status untuk menarik pengguna secara efektif.
4. *Social Networking Sites*. Platform media sosial Facebook diperkenalkan pada Februari 2004. Awalnya media sosial dibuat dengan mempertimbangkan mahasiswa Universitas Harvard di Amerika Serikat, Facebook telah menjadi platform media sosial yang paling banyak digunakan secara global. Kita dapat berbagi file, gambar, dan video dengan teman dan keluarga di Facebook.
5. *Virtual game worlds*. Simulasi dunia maya berpindah dari surga eksperimental ke surga yang mendalam, terkait erat dengan jejaring sosial dan game online.
6. *Virtual social worlds*. Sebuah dunia virtual yang dihosting di internet, Second Life diperkenalkan pada tahun 2003. Platform Second Life diciptakan oleh firma riset Linden Research, Inc. Ketika media memberitakan komunitas virtual ini pada akhir tahun 2006 dan awal tahun 2007, hal itu menarik perhatian orang-orang di seluruh dunia.

Namun demikian penting untuk diingat bahwa kita harus menjadi penguna yang cerdas agar dengan adanya perubahan dan perkembangan media sosial yang cukup signifikan jangan sampai data privasi kita yang ada di media sosial terkena hacking dan kejahatan Cyber crime (Nenna Irsa Syahputri, 2023).

METODE

Metodologi penelitian jurnal ini memadukan teknik kualitatif dengan tinjauan pustaka yang dilakukan pada jurnal tinjauan pustaka. Dikumpulkan dari jurnal dan publikasi ilmiah yang berisi temuan penelitian sebelumnya, dengan tujuan memperluas dan menyempurnakan hipotesis yang telah diklarifikasi oleh peneliti sebelumnya. Jurnal penelitian ini menggunakan buku online, media online lainnya, dan Google Scholar sebagai sumber referensi.

Tabel 1 Penelitian Terdahulu

No.	Nama Penulis (Tahun)	Judul	Hasil Riset Terdahulu
1	Hero Raka Herdiantoro, M. Reza Redo Islami, (2023)	Implementasi Two-Factor Authentication (2fa) Dan Firewall Policies Dalam Mengamankan Website	Menerapkan aturan firewall dan 2FA untuk memperkuat keamanan situs web halaman administrator.
2	Guma Ali, Mussa Ally Dida, dan Anael Elikana	Two-Factor Authentication Scheme For Mobile Money: A	Model ancaman dan penanggulangan dalam

	Sam, (2020)	Review Of Threat Models And Countermeasures	skema 2FA untuk uang seluler.
3	Nenna Irsa Syahputri, Herlina Harahap, Rosyidah Siregar, Tommy Tommy, (2023)	Penyuluhan Pentingnya Two Factor Authentication Dan Aplikasinya Di Era Keamanan Digital	Memberikan edukasi dan praktik sederhana untuk pelajar di tingkat SMA dalam memanfaatkan two factor authentication untuk menambah tingkat perlindungan ekstra pada akun digitalnya.
4	Ahmed Buhari, Zayyad Isa Sulaiman, (2023)	Social Media And Cyber Security: Protecting Against Online Threats And Attacks	Dampak media sosial terhadap keamanan cyber dan melihat mekanisme pertahanan yang dapat digunakan untuk melindungi terhadap ancaman keamanan cyber tersebut.
5	Izabela Szczygiel, Sebastian Florczak, Adrian Jasiak, (2023)	Two Factor Authentication (2fa) Comparison Of Methods And Applications	Memberikan penjelasan rinci mengenai berbagai jenis two factor authentication serta manfaat dan keuntungan yang dapat dicapai melalui penerapan two factor authentication.
6	Mauli Bayu Segoro, Prasetyo Adi Wibowo Putro, (2020)	Implementation Of Two Factor Authentication (2fa) And Hybrid Encryption To Reduce The Impact Of Account Theft On Android-Based Instant Messaging (Im) Applications	Menerapkan keamanan aplikasi pesan instan dengan menggunakan hybrid encryption dan two factor authentication yang dibuat salin terkait. Diimplementasikan dalam 2 desain yaitu mengamankan login dan mengamankan pengiriman dan penerimaan pesan.
7	Mr R Suresh, Balachander K, Logesh Varman S, Sai Faris K S, (2024)	Two Factor Authentication By Using Decentralized File Storage System	Menerapkan metode 2FA yang terdesentralisasi dengan menggunakan proses otentikasi dan enkripsi kunci publik. Pengguna dapat membuat kata sandi yang berbeda tanpa perangkat utama.
8	Surya Bodhi, David Tan, (2022)	Keamanan Data Pribadi Dalam Sistem Pembayaran *E-Wallet* Terhadap Ancaman Penipuan Dan Pengelabuan *(Cybercrime)*	Memberikan penjelasan mengenai penegakan hukum terhadap tindak kejahatan *cybercrime* dari pemakaian *e-wallet* serta perlindungan data pribadi pada *e-wallet.*
9	I Gusti Ngurah Dwi Derrick, Ndaru Satrio, S.H., M. (I Gusti Ngurah Dwi, 2023) (Iwan Setiawan, 2024)H., (2023)	Analisa Tindak Pidana *Cyber Crime* Pada Bidang Perbankan Nasional Berupa Pencurian Data Kartu Kredit *(Carding)*	Memberikan penjelasan mengenai analisis tindak pidana *cyber crime* pada bidang perbankan terutama pada pencurian data kartu kredit *(carding).*

10	Iwan Setiawan, Fauzi G. Cempaka, Yono Reksoprodjo, (2024)	Pencurian Data Dan Informasi Di Indonesia Sebagai Kejahatan Cyber Dalam Perspektif Peperangan Asimetris	Memberikan penjelasan mengenai faktor-faktor dan langkah-langkah pemerintah Indonesia pada kasus pencurian data dan informasi di Indonesia sebagai kejahatan cyber dalam perspektif peperangan asimetris.
11	Selamet, (2022)	Pertahanan Pencegahan Serangan Social Engineering Menggunakan Two Factor Authentication (2fa) Berbasis Sms (Short Message System)	Memberikan penjelasan mengenai langkah-langkah teknis yang diambil untuk melawan serangan social engineering menggunakan otentikasi dua factor (2 FA) berbasis SMS dan pengembangan prinsip anti penyalagunaan dalam meneruskan kode verifikasi kepada intruder.
12	Eni Pudjiarti, S. F. (2023)	Analisa Kesadaran Masyarakat Terhadap Bahaya Cybercrime Pada Penggunaan Teknologi Dan Media Sosial	Memberikan penjelasan mengenai kesadaran Masyarakat terhadap cybercrime pada pengunaan teknologi dan sosial media dapat memberikan kesadaran dan kewaspadaan yang lebih tinggi terhadap bahaya cybercrime pada penggunaan teknologi dan sosial media.
13	Neneng Nuryati, d. (2022)	Two Factor Authentication Sistem Inventarisasi Barang Dan Manajemen Dana Bantuan Operasional Sekolah Dinas Pendidikan Nasional	Memberikan penjelasan mengenai penerapan 2FA pada sistem inventaris barang dan manajemen dana bos dalam membantu untuk mempermudah proses monitoring dan pencegahan agar tidak disalah gunakan oleh pihak lain.
14	Lanang Adi Saputra, F. M. (2024)	Ancaman Keamanan Pada Sistem Informasi Manajemen Perusahaan	Memberikan penjelasan mengenai pencegahan maupun mendeteksi ancaman ancaman yang masuk pada ruang lingkup keamanan sistem informasi perusahaan.
15	WIlem Musu, d. (2022)	Analisis Pola Penggunaan Fitur Autentikasi Dua Faktor Oleh Para Remaja Di Media Sosial	Memberikan penjelasan mengenai penggunaan fitur 2FA dalam melakukan aktifitas sosial media dan memberikan pemahaman mengenai pentingnya keamanan data dengan memanfaatkan fitur dengan mekanisme 2FA.

HASIL DAN PEMBAHASAN

Pencegahan Two Factor Aunthentication terhadap Pencurian Data

Diperlukan langkah preventif dalam menjamin keamanan data pribadi agar terhindar dari pencurian data ataupun kejahatan cyber lainnya. Faktor terpenting dalam keamanan teknologi saat ini adalah kode OTP yang tidak boleh diberikan kepada sembarang orang. Selain itu, Pencurian data dapat dihindari secara efektif dengan penggunaan otentikasi dua faktor (2FA). Dengan autentikasi dua faktor (2FA), akses ke akun atau data pribadi diamankan dengan dua lapisan perlindungan: kata sandi dan kode verifikasi tambahan yang diberikan melalui SMS, aplikasi autentikator, atau penggunaan sidik jari dan pengenalan wajah (Bodhi & Tan, 2022).

Menurut Charles P. Pfleeger, 2FA menambah lapisan keamanan signifikan, 2FA membuat peretasan jauh lebih sulit karena membutuhkan faktor kedua selain kata sandi. Lapisan keamanan tambahan yang disebut otentikasi dua faktor (2FA) digunakan untuk mencegah pengguna yang tidak diinginkan mengakses akun pribadi (Segoro & Wibowo Putro, 2020). Saat masuk ke akun, 2FA meminta untuk memberikan informasi verifikasi tambahan, seperti kode yang dikirimkan ke ponsel atau sidik jari pemilik akun, selain kata sandi. Penerapan 2FA, yaitu dengan cara:

a. Kode SMS/Email: Saat login, Anda akan dikirimi kode unik melalui SMS atau email yang harus dimasukkan untuk menyelesaikan proses login.
b. Aplikasi Autentikator: Aplikasi ini menghasilkan kode unik yang berubah berkala. Gunakan kode ini untuk login alih-alih kode SMS/email.
c. Sidik Jari: Login menggunakan sidik jari Anda di perangkat yang mendukung.
d. Pengenalan Wajah: Login menggunakan pengenalan wajah di perangkat yang mendukung.

Berikut adalah beberapa cara 2FA dapat membantu mencegah pencurian data:

1. Menambahkan lapisan keamanan tambahan: 2FA membuat lebih sulit bagi peretas untuk masuk ke akun orang lain, bahkan jika mereka mengetahui kata sandi Anda. Mereka juga perlu memiliki akses ke faktor verifikasi kedua Anda, seperti ponsel Anda atau sidik jari Anda.
2. Melindungi dari serangan phishing: Serangan phishing adalah upaya untuk menipu Anda agar memberikan informasi pribadi Anda, seperti kata sandi, ke situs web palsu. 2FA dapat membantu melindungi Anda dari serangan ini karena meskipun peretas dapat memperoleh kata sandi Anda dari situs web phishing, mereka masih memerlukan akses ke faktor verifikasi kedua Anda untuk masuk ke akun Anda.
3. Membatasi akses yang tidak sah: Jika akun Anda diretas, peretas mungkin dapat mengakses informasi pribadi Anda, seperti data keuangan atau email Anda. 2FA dapat membantu membatasi akses ini karena peretas masih memerlukan akses ke faktor verifikasi kedua Anda untuk masuk ke akun Anda.
4. Meningkatkan kepercayaan pengguna: 2FA dapat membantu meningkatkan kepercayaan pengguna terhadap layanan online dengan menunjukkan kepada mereka bahwa layanan tersebut berkomitmen untuk melindungi keamanan data mereka.
5. Memenuhi persyaratan kepatuhan**:** Beberapa industri, seperti layanan keuangan dan perawatan kesehatan, diharuskan untuk menerapkan 2FA untuk melindungi data sensitif pelanggan mereka.

Cara Kerja Two Factor Authentication pada Sistem Keamanan

Ada beberapa metode yang tersedia bagi pengguna untuk memverifikasi identitas mereka, dimulai dengan memasukkan kata sandi, menunjukkan identifikasi, dan menggunakan biometric seperti wajah dan sidik jari untuk memvalidasi. Metode kata sandi tetap menjadi pendekatan yang paling banyak digunakan, akan tetapi ada kemungkinan besar seseorang akan mengetahui kata sandi yang kita gunakan, sehingga dapat memberikan mereka akses ke semua data pribadi kita yang dilindungi oleh kata sandi tersebut. Oleh karena itu, diperlukan otentikasi dua faktor untuk memberikan sistem keamanan ganda yang kuat untuk melindungi data pribadi seseorang (Szczygiel, 2023).

Menggunakan otentikasi dua faktor menawarkan perlindungan yang kuat terhadap pencurian akun. Frekuensi pelanggaran basis data kata sandi baru-baru ini menyoroti kemungkinan resiko peretasan akun (Segoro & Wibowo Putro, 2020). Kebocoran kata sandi dari satu situs web dapat menyebabkan reaksi beruntun pada penyusupan akun karena pengguna sering menggunakan nama pengguna dan kata sandi yang sama di beberapa situs web. Hal ini karena penyerang dapat mengakses

akun lain menggunakan kredensial yang sama. Pengguna 2FA harus menyediakan beberapa faktor, seperti:

a. Kata sandi atau pengetahuan lain yang dimiliki pengguna,
b. Barang milik pengguna (seperti telepon atau peralatan lainnya), dan
c. Item yang mewakili pengguna (seperti sidik jari & pengenalan wajah).

Ken Reese (2019) menyatakan bahwa ada lima metode 2FA yang paling banyak digunakan adalah push, pregenerated-code, SMS, OTP, dan Universal 2nd Factor, berikut penjelasannya:

1. Push
   Teknologi yang digunakan dalam metode push ini biasanya peringatan memberikan dua pilihan. "Setujui" atau "Tolak" setiap upaya mengakses sistem. Tidak perlu memiliki ruang penyimpanan khusus untuk otentikasi push, tetapi server harus dapat memastikan perangkat yang sesuai menerima pemberitahuan push.
2. Pregenerated-code
   Sistem menghasilkan kode tertentu yang tidak dibatasi waktu. Karena risiko yang terkait dengan metode ini sama dengan risiko yang terkait dengan penggunaan kata sandi, metode ini biasanya hanya digunakan untuk pencadangan, karena itulah tujuan penggunaannya.
3. Short Message Service (SMS)
   Mengirim kode unik melalui SMS merupakan teknik 2FA yang paling banyak digunakan, biasanya terdiri dari kode enam digit yang unik. Ketika pengguna mencoba masuk ke sistem menggunakan metode ini, server biasanya terhubung ke modul GSM *(Global System for Mobile Communications)* untuk mengirimkan kode unik ke nomor mereka.
4. Timed One Time Password (TOTP)
   Langkah pertama dalam proses ini biasanya menyinkronkan generator kode unik dari penyedia tertentu, seperti otentikasi Microsoft dan otentikasi Google. Aplikasi otentikasi ini menggunakan beberapa komponen diantaranya adalah nilai hashing, stempel waktu, dan contoh kode verifikasi. Manfaat pendekatan ini adalah pengguna dapat mengautentikasi tanpa memerlukan jaringan seluler kedua.
5. Universal 2nd Factor
   Dibuat oleh Yubico dan Google. U2F ini menggunakan USB hardware device (security key) untuk authenticate pengguna. Pada proses authenticate pengguna harus terhubung ke security key melalui USB port pada device-nya.

Penggunaan Two Factor Authentication dalam Meningkatkan Kesadaran Pengguna Tentang Pentingnya Keamanan Cyber

Pada dasarnya, pengidentifikasi pengguna ditetapkan saat proses otentikasi, seperti nama pengguna, kode karyawan, atau alamat email, dengan pengguna memberikan data pribadi seperti kata sandi. Jika data pribadi yang diberikan benar, identitas pengguna dikonfirmasi, memungkinkannya untuk mengakses sistem dan menggunakan fungsi yang disediakan (Guma Ali, 2020). Implementasi otentikasi 2FA dapat menjadi solusi fleksibel dan andal untuk meningkatkan keamanan infrastruktur penting.

Biaya respons yang tinggi berdampak negatif pada niat pengguna untuk mengadopsi 2FA sebagai teknologi pelindung. Artinya, jika penggunaan merasa bahwa 2FA membutuhkan sedikit usaha, waktu, dan lebih nyaman, maka mereka akan lebih termotivasi untuk menggunakannya (Nenna Irsa Syahputri, 2023). Sebaliknya, keyakinan akan efektivitas 2FA dalam melindungi akun secara signifikan meningkatkan niat pengguna untuk mengaktifkannya.

Kesadaran teknologi memiliki hubungan positif yang signifikan dengan niat perilaku untuk menggunakan 2FA. Artinya, semakin sadar pengguna internet akan ancaman dan solusi online, semakin besar motivasi mereka untuk menggunakan 2FA sebagai perlindungan akun. Penemuan ini didasarkan pada penelitian Dinev & Hu (2007), yang menunjukkan bahwa kesadaran teknologi adalah faktor penting dalam menentukan niat perilaku untuk mengadopsi teknologi pelindung. Penelitian ini memasukkan kesadaran teknologi ke dalam model PMT, dengan asumsi bahwa kesadaran akan teknologi pelindung umumnya lebih rendah dibandingkan dengan teknologi lain.

Teknik 2FA adalah mekanisme perlindungan akun yang meminta konfirmasi dari pemilik akun untuk mencegah pencurian, pengintaian, dan penipuan oleh pihak lain. Mekanisme ini meminta pemilik akun untuk memasukkan kata sandi sekali pakai yang dikirimkan oleh server saat terdeteksi ada upaya masuk ke akun. Awalnya, 2FA banyak digunakan untuk mengamankan transaksi perbankan online, namun kini telah di adopsi oleh banyak layanan internet, termasuk media sosial (Szczygiel, 2023).

Mengedukasi masyarakat tentang dampak buruk kejahatan cyber dan memberikan saran untuk menghindarinya dapat meningkatkan kewaspadaan dan kesadaran. Kita harus tetap waspada dan berhati-hati saat menggunakan media sosial (Nenna Irsa Syahputri, 2023). Bagi yang ahli di bidang IT, penting untuk memberikan edukasi dan sosialisasi kepada orang-orang awam yang belum memiliki kesadaran dan kewaspadaan yang baik. Masih ada sebagian masyarakat yang belum sadar akan ancaman ini. Selain itu, kita harus terus mengikuti perkembangan terbaru tentang kejahatan cyber untuk memahami tanggapan dan respons publik serta cara mengatasinya.

SIMPULAN

Manajemen keamanan melibatkan langkah-langkah efektif dan efisien untuk mencegah gangguan dan kerugian. Salah satu metode pengamanan data yang telah dikembangkan adalah two factor authentication, yang banyak digunakan di media sosial. Media sosial saat ini memang sangat memfasilitasi masyarakat untuk berkomunikasi dan juga untuk melakukan kegiatan sosial lainnya tapi kita sebagai pengguna tetap harus selalu waspada, karena kejahatan cybercrime masih sangat mudah dilakukan oleh pelaku kejahatan cyber.

Agar data dan privasi kita yang ada di media sosial tetap aman bisa dilakukan dengan menggunakan sistem keamanan 2FA, seperti validasi kedua setelah password seperti kode OTP atau bisa juga dengan verifikasi wajah yang dapat membantu data kita lebih aman. Hasil penelitian ini menunjukkan bahwa mengedukasi masyarakat tentang dampak buruk kejahatan cyber dan memberikan saran untuk menghindarinya dapat meningkatkan kewaspadaan dan kesadaran. Karena, masih ada sebagian masyarakat yang belum menyadari ancaman ini, serta masyarakat perlu terus mengikuti perkembangan terbaru tentang kejahatan cyber untuk memahami tanggapan dan cara mengatasinya.

Berdasarkan jurnal diatas untuk menjadi pengguna yang cerdas, pembaca memerlukan perkembangan dalam system keamanan yang dilakukan untuk mencegah adanya cybercrime. Dalam menghindari pencegahan, guna 2FA ini, yakni metode push, OTP dan lainnya pembaca diharapkan agar memahami bagaimana cara kerja dalam proses pencegahan yang dilakukan 2FA secara signifikan. Namun demikian penting untuk diingat bahwa kita harus menjadi pengguna yang cerdas agar dengan adanya perubahan dan perkembangan media sosial yang cukup signifikan jangan sampai data privasi kita yang ada di media sosial terkena hacking dan kejahatan cybercrime. Disisi lain kita juga tidak tahu kapan kejahatan cybercrime akan datang ke kita jadi kita harus menjaga data sebaik mungkin.

REFERENSI

Ahmad Riffat, D. (2023). MENGGUNAKAN SOSIAL MEDIA DENGAN BIJAK UNTUK MENGHINDARI BAHAYA CYBER CRIME. *APPA : Jurnal Pengabdian Kepada Masyarakat*.

Ahmed Buhari, Z. I. (2023). SOCIAL MEDIA AND CYBER SECURITY: PROTECTING AGAINST ONLINE THREATS AND ATTACKS. *Researchgate*.

Catur Nugroho, S. M. (2020). *CYBER SOCIETY : Teknologi, Media Baru, Dan Disrupsi Informasi.* KENCANA.

Edy Soesanto, D. (2023). Keamanan Informasi Data Dalam Pemanfaatan Teknologi Informasi Pada PT Bank Central Asia (BCA).

Eni Pudjiarti, S. F. (2023). Analisa Kesadaran Masyarakat Terhadap Bahaya Cybercrime Pada Penggunaan Teknologi Dan Media Sosial. *BINA IN SANI ICT JOURNAL*.

Guma Ali, M. A. (2020). Two-Factor Authentication Scheme For Mobile Money : A Review Of Threat Models And Countermeasures. *MDIP*.

Haider Mehraj, D. (2021). Protection Motivation Theory Using Multi-Factor Authentication For Providing Security Over Social Networking Sites.

Hero Raka Herdiantoro, M. R. (2023). IMPLEMENTASI TWO-FACTOR AUTHENTICATION (2FA) DAN FIREWALL POLICIES DALAM MENGAMANKAN WEBSITE. *JMIK (JURNAL MAHASISWA ILMU KOMPUTER)*.

I Gusti Ngurah Dwi, D. S. (2023). ANALISA TINDAK PIDANA CYBER CRIME PADA BIDANG PERBANKAN NASIONAL BERUPA PENCURIAN DATA KARTU KREDIT (CARDING).

Iwan Setiawan, F. G. (2024). PENCURIAN DATA DAN INFORMASI DI INDONESIA SEBAGAI KEJAHATAN CYBER DALAM PERSPEKTIF PEPERANGAN ASIMETRIS. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*.

Ken Reese, T. S. (2019). A Usability Study Of Five Two-Factor Authentication Methods.

Lanang Adi Saputra, F. M. (2024). Ancaman Keamanan Pada Sistem Informasi Manajemen Perusahaan. *Researchgate*.

Mauli Bayu Segoro, P. A. (2020). Implementation Of Two Factor Authentication (2FA) And Hybrid Encryption To Reduce The Impact Of Account Theft On Android-Based Instant Messaging (IM) Applications. *Researchgate*.

Mitch Holmes, J. O. (2019). Online Security Behaviour: Factors Influencing Intention To Adopt Two-Factor Authentication.

Neneng Nuryati, D. (2022). Two Factor Authentication Sistem Inventarisasi Barang Dan Manajemen Dana Bantuan Operasional Sekolah Dinas Pendidikan Nasional.

Nenna Irsa Syahputri, D. (2023). Penyuluhan Pentingnya Two Factor Authentication Dan Aplikasinya Di Era Keamanan Digital. *Jurnal Pengabdian Masyarakat Bangsa*.

Octo Iskandar S.H M.H., D. H. (2021). BAHAN AJAR MATA KULIAH MANAJEMEN SEKURITI.

Potter, K. (2018). INCREASED USE OF TWO-FACTOR AUTHENTICATION FORCE NEW SOCIAL ENGINEERING TACTICS. *Proqouest*.

R Suresh, K. B. (2024). Two Factor Authentication By Using Decentralized File Storage System. *Researchgate*.

Rasa Bruzgiene, K. J. (2021). Securing Remote Access To Information Systems Of Critical Infrastructure Using Two-Factor Authentication. *MDPI*.

Slamet. (2022). PERTAHANAN PENCEGAHAN SERANGAN SOCIAL ENGINEERING MENGGUNAKAN TWO FACTOR AUTHENTICATION (2FA) BERBASIS SMS (SHORT MESSAGE SYSTEM). *Jurnal SPIRIT*.

Surya Bodhi, D. T. (2022). KEAMANAN DATA PRIBADI DALAM SISTEM PEMBAYARAN E-WALLET TERHADAP ANCAMAN PENIPUAN DAN PENGELABUAN (CYBERCRIME). *UNES LAW REVIEW*.

Szczygiel, I. (2023). Two-Factor Authentication (2FA) Comparison Of Methods And Applications. *Advances In Web Development Journal*.

Wilem Musu, D. (2022). Analisis Pola Penggunaan Fitur Autentikasi Dua Faktor Oleh Para Remaja Di Media Sosial. *JURNAL SISTEM INFORMASI DAN TEKNOLOGI INFORMASI*.

Willy Sudiarto Raharjo, I. D. (2017). IMPLEMENTASI TWO FACTOR AUTHENTICATION DAN PROTOKOL ZERO KNOWLEDGE PROOF PADA SISTEM LOGIN. *Jutisi*.