PROSISI: Prosiding Seminar Nasional Saintek
Vol.1 No.1, 2026, Hal. 404-413
ISSN XXXX-XXXX

Analisis Kesadaran Mahasiswa Informatika Universitas Nurul Huda Terhadap Keamanan Data Pribadi Dan Penggunaan Two Factor Authentication (2fa)

Deni Alfian[1], Fikri Kurniawan[1], Vemas Angger Permana[1] Iwan Tri Bowo[1], Annisa Nur Azizah[2]

[1] Program Studi Informatika Universitas Nurul Huda

[2] Program Studi Matematika Universitas Nurul Huda

*E-mail: denialfian2604@gmail.com

Abstrak

Perkembangan teknologi digital yang sangat cepat telah mendorong penggunaan layanan yang berbasis internet di kalangan pelajar, tetapi di sisi lain telah menambah ancaman terhadap keamanan informasi pribadi. Masalah seperti pencurian identitas, penipuan online, kebocoran informasi, dan penyalahgunaan data pribadi menjadi hal yang harus diperhatikan oleh para pengguna teknologi, terutama mahasiswa informatika yang merupakan pengguna aktif dari layanan digital. Salah satu langkah yang dapat diambil untuk memperkuat keamanan akun digital adalah dengan mengadopsi fitur *Two Factor Authentication* (2FA) sebagai lapisan perlindungan tambahan. Penelitian ini bertujuan untuk mengevaluasi sejauh mana mahasiswa Informatika Universitas Nurul Huda menyadari pentingnya keamanan data pribadi serta pemanfaatan *Two Factor Authentication* (2FA). Metode yang digunakan dalam penelitian ini adalah pendekatan kuantitatif deskriptif yang melibatkan pengumpulan data melalui penyebaran kuesioner menggunakan Google Form kepada para mahasiswa Informatika Universitas Nurul Huda. Dengan penelitian ini, diharapkan dapat diperoleh pemahaman mengenai seberapa baik mahasiswa mengerti, berperilaku, dan sadar akan pentingnya menjaga keamanan data pribadi pada akun digital yang mereka gunakan sehari-hari. Selain itu, penelitian ini diharapkan dapat menjadi acuan untuk meningkatkan literasi tentang keamanan digital serta mendorong adopsi fitur keamanan tambahan guna mengurangi kemungkinan penyalahgunaan akun dan kebocoran informasi pribadi di lingkungan akademis.

Kata kunci : keamanan data pribadi, *two factor authentication*, 2FA, keamanan digital, mahasiswa informatika

Abstract

The swift progress of digital technology has led to an increase in the adoption of online services by university students, while simultaneously heightening the threat of breaches in personal data security. Issues like account hacking, phishing, data breaches, and the improper use of personal details have emerged as significant concerns that necessitate heightened vigilance from users in the digital realm, particularly among informatics students who frequently engage with technology and online services. One effective security strategy that can be adopted to enhance account safety is the implementation of Two Factor Authentication (2FA), which functions as an extra layer of protection. This study seeks to evaluate the awareness levels of Informatics students at Universitas Nurul Huda concerning personal data security and the application of Two Factor Authentication (2FA). A descriptive quantitative research approach was utilized, gathering data through surveys distributed via Google Forms to Informatics students at Universitas Nurul Huda. The findings from this study are anticipated to shed light on students' comprehension, habits, and awareness concerning the safeguarding of personal data within digital accounts utilized in their everyday lives. Furthermore, the outcomes of this research are expected to enhance digital security knowledge and promote the adoption of supplementary security measures to reduce the chances of unauthorized access and the compromise of personal data in the academic setting.

Keywords : *personal data security, two factor authentication, 2FA, digital security, informatics students*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi pada era digital telah membawa perubahan yang signifikan terhadap aktivitas masyarakat, khususnya mahasiswa, dalam mengakses, mengelola, dan menyimpan informasi. Berbagai layanan digital seperti media sosial, email, *cloud storage*, mobile banking, serta sistem informasi akademik telah menjadi bagian yang tidak terpisahkan dari kehidupan sehari-hari. Kemudahan yang diberikan oleh teknologi digital mendorong meningkatnya penggunaan layanan berbasis internet, namun di sisi lain juga meningkatkan risiko terhadap keamanan data pribadi pengguna. Ancaman seperti pencurian akun, phishing, kebocoran data, dan penyalahgunaan informasi pribadi menjadi permasalahan yang semakin sering terjadi pada lingkungan digital [1].

Data pribadi merupakan informasi yang bersifat sensitif dan memiliki nilai penting bagi setiap individu, seperti nama lengkap, alamat email, nomor telepon, kata sandi akun, identitas pribadi, hingga data akademik. Dalam penggunaan layanan digital, data tersebut berpotensi mengalami kebocoran maupun penyalahgunaan oleh pihak yang tidak bertanggung jawab apabila tidak disertai dengan sistem keamanan yang memadai. Tingginya aktivitas pengguna internet menyebabkan keamanan data pribadi menjadi salah satu aspek yang perlu mendapatkan perhatian serius, terutama di lingkungan akademik yang memiliki tingkat penggunaan teknologi cukup tinggi [2].

Mahasiswa informatika merupakan kelompok pengguna teknologi yang memiliki tingkat interaksi tinggi terhadap sistem digital dan internet. Secara teoritis, mahasiswa informatika memiliki pemahaman dasar mengenai teknologi informasi dan keamanan sistem. Namun demikian, tingkat kesadaran terhadap keamanan data pribadi tidak selalu berada pada tingkat yang optimal. Sebagian mahasiswa masih menggunakan kata sandi yang lemah, menggunakan kata sandi yang sama pada beberapa akun, jarang melakukan pembaruan kata sandi, serta kurang memperhatikan pengaturan privasi akun digital yang digunakan. Kondisi tersebut menunjukkan adanya perbedaan antara pemahaman teoritis dan penerapan praktik keamanan digital dalam kehidupan sehari-hari [3].

Peningkatan ancaman keamanan siber pada berbagai platform digital menunjukkan pentingnya penerapan sistem keamanan tambahan dalam melindungi akun pengguna. Salah satu metode keamanan yang banyak digunakan saat ini adalah *Two Factor Authentication* (2FA). *Two Factor Authentication* merupakan metode autentikasi yang menggunakan dua tahap verifikasi dalam proses login akun, yaitu kombinasi antara kata sandi dan kode verifikasi tambahan yang dikirimkan melalui SMS, email, atau aplikasi autentikasi tertentu. Penggunaan fitur 2FA dinilai efektif dalam meningkatkan keamanan akun digital karena mampu meminimalkan risiko akses tidak sah, pencurian akun, serta penyalahgunaan data pribadi [4].

Meskipun fitur *Two Factor Authentication* telah tersedia pada berbagai layanan digital seperti Google, Instagram, Facebook, dan aplikasi perbankan, tingkat penggunaannya di kalangan mahasiswa masih belum merata. Sebagian mahasiswa telah memanfaatkan fitur tersebut sebagai bentuk perlindungan tambahan terhadap akun digital yang dimiliki, sedangkan sebagian lainnya belum mengaktifkan fitur keamanan tersebut secara konsisten. Faktor kemudahan penggunaan, tingkat pemahaman teknologi, kebiasaan pengguna, serta rendahnya kesadaran terhadap risiko keamanan digital menjadi beberapa faktor yang memengaruhi penggunaan fitur *Two Factor Authentication* (2FA). Hal ini menunjukkan bahwa penerapan teknologi keamanan tidak hanya dipengaruhi oleh ketersediaan fitur, tetapi juga dipengaruhi oleh perilaku dan tingkat kesadaran pengguna terhadap pentingnya perlindungan data pribadi [5].

Beberapa penelitian sebelumnya menunjukkan bahwa tingkat kesadaran keamanan data pribadi di kalangan mahasiswa masih berada pada kategori sedang dan memerlukan peningkatan literasi keamanan digital. Penelitian mengenai kesadaran keamanan data pribadi mahasiswa menunjukkan bahwa sebagian besar pengguna masih kurang memahami pentingnya perlindungan data pribadi pada media digital serta belum menerapkan praktik keamanan akun secara optimal [6]. Selain itu, penelitian mengenai penerapan *Two Factor*

Authentication menunjukkan bahwa penggunaan autentikasi ganda mampu meningkatkan perlindungan akun digital dan mengurangi risiko penyalahgunaan data pribadi pada layanan berbasis internet [7].

Berdasarkan permasalahan tersebut, diperlukan suatu analisis untuk mengetahui tingkat kesadaran mahasiswa Informatika Universitas Nurul Huda terhadap keamanan data pribadi dan penggunaan *Two Factor Authentication* (2FA). Penelitian ini bertujuan untuk memberikan gambaran mengenai tingkat pemahaman, perilaku, dan kesadaran mahasiswa dalam menjaga keamanan data pribadi pada akun digital yang digunakan sehari-hari. Selain itu, penelitian ini juga bertujuan untuk mengetahui penggunaan fitur keamanan tambahan sebagai upaya perlindungan akun digital. Hasil penelitian diharapkan dapat memberikan kontribusi dalam meningkatkan literasi keamanan digital di lingkungan akademik serta menjadi referensi dalam pengembangan kesadaran keamanan informasi di kalangan mahasiswa.

METODE PENELITIAN

Penelitian ini menggunakan metode kuantitatif deskriptif untuk menganalisis tingkat kesadaran mahasiswa Informatika Universitas Nurul Huda terhadap keamanan data pribadi dan penggunaan *Two Factor Authentication* (2FA). Metode kuantitatif deskriptif digunakan karena penelitian ini bertujuan untuk menggambarkan tingkat pemahaman, perilaku, dan kesadaran mahasiswa dalam menjaga keamanan akun digital berdasarkan data yang diperoleh dari responden [7].

Populasi dan Sampel

Populasi dalam penelitian ini adalah seluruh mahasiswa Program Studi Informatika Universitas Nurul Huda yang aktif pada tahun akademik penelitian. Mahasiswa dipilih sebagai populasi karena merupakan pengguna aktif berbagai layanan digital yang berpotensi menghadapi risiko keamanan data pribadi dalam aktivitas sehari-hari [8].

Teknik pengambilan sampel menggunakan purposive sampling, yaitu teknik penentuan sampel berdasarkan kriteria tertentu yang sesuai dengan tujuan penelitian. Kriteria responden meliputi mahasiswa aktif Program Studi Informatika Universitas Nurul Huda, memiliki akun digital seperti email dan media sosial, serta bersedia mengisi kuesioner penelitian secara lengkap [9].

Jumlah sampel yang digunakan dalam penelitian ini sebanyak 30 responden yang memenuhi kriteria penelitian dan telah mengisi kuesioner secara lengkap.

Tabel 1. Ringkasan Karakteristik Responden

No.	Indikator Pertanyaan	Ringkasan Hasil
1	Semester responden	Responden penelitian terdiri atas 3 mahasiswa Semester 2 (10,0%), 6 mahasiswa Semester 4 (20,0%), dan 21 mahasiswa Semester 6 (70,0%). Dengan demikian, mayoritas responden berasal dari Semester 6.
2	Penggunaan fitur *Two Factor Authentication* (2FA)	Sebanyak 25 responden (83,3%) telah menggunakan fitur *Two-Factor Authentication* (2FA), sedangkan 5 responden (16,7%) menyatakan belum menggunakan fitur tersebut.
3	Kesadaran terhadap pentingnya menjaga keamanan data pribadi di internet	Sebanyak 28 responden (93,3%) menyatakan setuju, 1 responden (3,3%) menyatakan netral, dan 1 responden (3,3%) menyatakan tidak setuju terhadap pentingnya menjaga keamanan data pribadi di internet.
4	Pengetahuan mengenai penyalahgunaan data pribadi	Sebanyak 28 responden (93,3%) menyatakan setuju bahwa mereka mengetahui risiko penyalahgunaan data pribadi, sedangkan masing-masing 1 responden (3,3%) menyatakan netral dan tidak setuju.
5	Pengetahuan mengenai bahaya *phishing* atau penipuan online	Sebanyak 25 responden (83,3%) menyatakan setuju bahwa mereka mengetahui bahaya *phishing* atau penipuan *online*, 4 responden (13,3%) menyatakan netral, dan 1 responden (3,3%) menyatakan tidak setuju.

6	Tingkat pemahaman fungsi *Two Factor Authentication* (2FA)	Sebanyak 3 responden (10,0%) menyatakan sangat mengetahui, 8 responden (26,7%) mengetahui, 11 responden (36,7%) cukup mengetahui, 7 responden (23,3%) kurang mengetahui, dan 1 responden (3,3%) tidak mengetahui fungsi *Two Factor Authentication* (2FA).
7	Kehati-hatian dalam membagikan data pribadi di media sosial maupun internet	Sebanyak 24 responden (80,0%) menyatakan selalu berhati-hati dalam membagikan data pribadi, 4 responden (13,3%) menyatakan jarang, dan 2 responden (6,7%) menyatakan tidak pernah berhati-hati.
8	Persepsi terhadap penggunaan fitur *Two Factor Authentication* (2FA)	Sebanyak 22 responden (73,3%) menyatakan setuju bahwa penggunaan fitur *Two Factor Authentication* (2FA) dapat meningkatkan keamanan akun digital, 7 responden (23,3%) menyatakan netral, dan 1 responden (3,3%) menyatakan tidak setuju.

Sebanyak 30 mahasiswa Program Studi Informatika Universitas Nurul Huda yang memenuhi kriteria penelitian telah berpartisipasi sebagai responden melalui pengisian kuesioner secara daring menggunakan Google Form. Karakteristik responden disajikan pada Tabel 1, yang menunjukkan distribusi responden berdasarkan semester akademik serta penggunaan fitur Two Factor Authentication (2FA). Informasi karakteristik responden tersebut digunakan untuk memberikan gambaran umum mengenai profil sampel penelitian dan sebagai dasar dalam menginterpretasikan tingkat kesadaran mahasiswa terhadap keamanan data pribadi dan penggunaan mekanisme autentikasi ganda.

Teknik Pengumpulan Data

Pengumpulan data dilakukan menggunakan kuesioner daring melalui Google Form yang disebarkan kepada mahasiswa Program Studi Informatika Universitas Nurul Huda. Penyebaran dilakukan melalui media komunikasi digital seperti grup WhatsApp dan media sosial mahasiswa untuk mempermudah proses distribusi dan pengumpulan data penelitian [10].

Instrumen Penelitian

Instrumen penelitian yang digunakan berupa kuesioner tertutup dengan skala Likert lima tingkat, yaitu Sangat Setuju (SS), Setuju (S), Netral (N), Tidak Setuju (TS), dan Sangat Tidak Setuju (STS). Skala Likert digunakan untuk mengukur tingkat persetujuan responden terhadap pernyataan yang berkaitan dengan keamanan data pribadi dan penggunaan *Two Factor Authentication* (2FA) [11].

Indikator penelitian meliputi pemahaman mengenai keamanan data pribadi, kesadaran terhadap risiko kebocoran data, kebiasaan penggunaan kata sandi yang aman, pengetahuan tentang *Two Factor Authentication* (2FA), penggunaan 2FA pada akun digital, serta persepsi terhadap pentingnya perlindungan akun digital [12].

Tabel 2. Skala Likert Penelitian

Kategori Jawaban	Skor
Sangat Setuju (SS)	5
Setuju (S)	4
Netral (N)	3
Tidak Setuju (TS)	2
Sangat Tidak Setuju (STS)	1

Tahapan Penelitian

Tahapan penelitian dilakukan secara sistematis yang meliputi identifikasi masalah, studi literatur, penyusunan instrumen penelitian, penyebaran kuesioner, pengumpulan data, analisis data, dan penyusunan laporan penelitian. Tahapan tersebut dilakukan untuk memastikan proses penelitian berjalan secara terstruktur dan sesuai dengan tujuan penelitian [13].

Teknik Analisis Data

Data yang diperoleh dari hasil kuesioner dianalisis menggunakan metode analisis deskriptif kuantitatif. Analisis dilakukan dengan menghitung frekuensi dan persentase jawaban responden pada setiap item pertanyaan untuk mengetahui tingkat kesadaran mahasiswa terhadap keamanan data pribadi dan penggunaan *Two Factor Authentication* (2FA) [14].

Persentase jawaban responden dihitung menggunakan rumus berikut:

$$P = \frac{f}{N} \times 100\%$$

Keterangan:

P= Persentase

f= Frekuensi jawaban

N= Jumlah responden

Hasil analisis kemudian disajikan dalam bentuk tabel dan diagram untuk mempermudah interpretasi data serta memberikan gambaran yang lebih jelas mengenai tingkat kesadaran mahasiswa terhadap keamanan data pribadi dan penggunaan *Two Factor Authentication* (2FA) [14].

HASIL DAN PEMBAHASAN

Penelitian ini bertujuan untuk menganalisis tingkat kesadaran mahasiswa Informatika Universitas Nurul Huda terhadap keamanan data pribadi serta penggunaan fitur *Two Factor Authentication* (2FA). Pengumpulan data dilakukan melalui penyebaran kuesioner secara daring menggunakan Google Form kepada mahasiswa Program Studi Informatika Universitas Nurul Huda. Berdasarkan hasil pengumpulan data, diperoleh sebanyak 30 responden yang berpartisipasi dalam penelitian ini.

Berdasarkan karakteristik responden, mahasiswa yang mengikuti penelitian berasal dari semester 2, semester 4, dan semester 6. Mayoritas responden berasal dari semester 6 sebanyak 21 orang atau sebesar 70%, diikuti semester 4 sebanyak 6 orang atau sebesar 20%, serta semester 2 sebanyak 3 orang atau sebesar 10%. Data tersebut menunjukkan bahwa sebagian besar responden merupakan mahasiswa tingkat akhir yang memiliki pengalaman lebih luas dalam penggunaan teknologi digital dan layanan internet.

Instrumen penelitian disusun berdasarkan indikator kesadaran keamanan data pribadi dan perilaku penggunaan keamanan digital. Penyusunan indikator pertanyaan mengacu pada penelitian mengenai *cybersecurity awareness*, keamanan data pribadi, serta penggunaan autentikasi ganda pada layanan digital.

Tabel 3. Indikator Pertanyaan Kuisioner

No	Indikator Pertanyaan	Tujuan Pengukuran
1	Semester responden	Mengetahui karakteristik responden penelitian
2	Penggunaan fitur Two Factor Authentication (2FA)	Mengetahui tingkat penggunaan keamanan tambahan pada akun digital
3	Kesadaran terhadap pentingnya menjaga keamanan data pribadi di internet	Mengukur tingkat kesadaran responden terhadap keamanan data pribadi
4	Pengetahuan mengenai penyalahgunaan data pribadi	Mengukur pemahaman responden terhadap risiko penyalahgunaan data
5	Pengetahuan mengenai bahaya phishing atau penipuan online	Mengetahui tingkat pemahaman responden terhadap ancaman keamanan digital
6	Tingkat pemahaman fungsi Two Factor Authentication (2FA)	Mengukur pemahaman responden mengenai fungsi autentikasi ganda
7	Kehati-hatian dalam membagikan data pribadi di media sosial maupun internet	Mengetahui perilaku responden dalam menjaga informasi pribadi

Tabel 4. Data Semester Responden

Semester	Jumlah	Persentase
Semester 2	3	10%
Semester 4	6	20%
Semester 6	21	70%
Total	**30**	**100%**

Berdasarkan data penelitian, mayoritas responden berasal dari semester 6 dengan persentase sebesar 70%. Hal ini menunjukkan bahwa mahasiswa tingkat akhir lebih aktif berpartisipasi dalam penelitian terkait keamanan digital. Mahasiswa semester akhir umumnya memiliki intensitas penggunaan teknologi yang lebih tinggi dalam kegiatan akademik maupun komunikasi digital sehingga lebih memahami pentingnya perlindungan data pribadi.

Tabel 5. Penggunaan Fitur *Two Factor Authentication* (2FA)

Jawaban	Jumlah	Persentase
Ya	25	83,3%
Tidak	5	16,7%
Total	**30**	**100%**

Hasil penelitian menunjukkan bahwa sebagian besar responden telah menggunakan fitur *Two Factor Authentication* (2FA) pada akun digital mereka. Sebanyak 25 responden atau sebesar 83,3% menyatakan pernah menggunakan fitur 2FA, sedangkan 5 responden atau sebesar 16,7% belum pernah menggunakannya.

Data tersebut menunjukkan bahwa tingkat kesadaran mahasiswa terhadap penggunaan keamanan tambahan pada akun digital tergolong tinggi. Penggunaan 2FA dinilai mampu memberikan perlindungan tambahan terhadap ancaman peretasan akun dan akses tidak sah.

Tingginya persentase penggunaan fitur *Two-FactorAuthentication* (2FA) oleh responden menunjukkan bahwa sebagian besar mahasiswa telah menerapkan mekanisme keamanan tambahan pada akun digital yang dimiliki. Penerapan autentikasi dua faktor merupakan salah satu praktik keamanan yang direkomendasikan dalam menjaga kerahasiaan identitas digital karena proses autentikasi tidak hanya bergantung pada kata sandi, tetapi juga memerlukan faktor verifikasi tambahan, seperti kode autentikasi, perangkat tepercaya, atau autentikasi biometrik. Menurut *Microsoft Security,* penerapan *Two Factor Authentication* (2FA) dapat meningkatkan keamanan akun dengan mengurangi risiko akses tidak sah, pencurian kredensial, serta berbagai serangan siber yang memanfaatkan kelemahan autentikasi berbasis kata sandi [4].

Tabel 6. Kesadaran terhadap Pentingnya Menjaga Keamanan Data Pribadi di Internet

Jawaban	Jumlah	Persentase
Setuju	28	93,3%
Tidak Setuju	1	3,3%
Netral	1	3,3%
Total	**30**	**100%**

Sebagian besar responden menyadari pentingnya menjaga keamanan data pribadi di internet. Sebanyak 28 responden atau sebesar 93,3% menyatakan setuju, sedangkan masing-masing 1 responden atau sebesar 3,3% menyatakan tidak setuju dan netral.

Hasil tersebut menunjukkan bahwa mayoritas mahasiswa telah memiliki kesadaran yang baik mengenai pentingnya perlindungan data pribadi dalam aktivitas digital sehari-hari. Kesadaran ini menjadi faktor penting dalam mencegah penyalahgunaan data, pencurian identitas, serta akses ilegal terhadap akun pengguna.

Sejalan dengan hasil penelitian, IBM Security menjelaskan bahwa perlindungan data pribadi merupakan salah satu aspek fundamental dalam keamanan siber yang berfokus pada pengelolaan serta perlindungan informasi pribadi agar hanya dapat diakses, digunakan, diproses, dan dibagikan sesuai dengan hak akses serta tujuan yang telah ditetapkan. Dalam implementasinya, perlindungan data didukung oleh penerapan kebijakan, prosedur, dan mekanisme pengamanan yang bertujuan menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi. Penerapan prinsip-prinsip tersebut berperan penting dalam meminimalkan risiko penyalahgunaan data, kebocoran informasi, maupun akses tidak sah yang dapat mengancam keamanan dan privasi pemilik data [2].

Tabel 7. Pengetahuan Mengenai Penyalahgunaan Data Pribadi

Jawaban	Jumlah	Persentase
Setuju	28	93,3%
Tidak Setuju	1	3,3%
Netral	1	3,3%
Total	**30**	**100%**

Hasil penelitian menunjukkan bahwa mayoritas responden mengetahui bahwa data pribadi dapat disalahgunakan oleh pihak lain. Sebanyak 28 responden atau sebesar 93,3% menyatakan setuju, sedangkan sebagian kecil responden memberikan jawaban tidak setuju dan netral.

Data tersebut menunjukkan bahwa mahasiswa telah memahami adanya risiko penyalahgunaan data pribadi seperti pencurian identitas, penyebaran informasi tanpa izin, maupun tindakan kejahatan siber lainnya. Tingginya tingkat pemahaman responden menunjukkan bahwa kesadaran terhadap keamanan data pribadi sudah cukup baik

Tabel 8. Pengetahuan Mengenai Bahaya *Phishing* atau Penipuan *Online*

Jawaban	Jumlah	Persentase
Setuju	25	83,3%
Tidak Setuju	1	3,3%
Netral	4	13,3%
Total	**30**	**100%**

Sebanyak 25 responden atau sebesar 83,3% mengetahui bahaya *phishing* atau penipuan online. Sementara itu, 4 responden atau sebesar 13,3% memberikan jawaban netral dan 1 responden atau sebesar 3,3% menyatakan tidak setuju.

Hasil tersebut menunjukkan bahwa sebagian besar mahasiswa telah memahami ancaman keamanan digital yang sering terjadi di internet. *Phishing* biasanya dilakukan dengan cara mengelabui pengguna agar memberikan informasi penting seperti kata sandi, kode OTP, maupun data pribadi lainnya melalui situs atau pesan palsu.

Sejalan dengan hasil penelitian, Kaspersky menjelaskan bahwa *phishing* merupakan bentuk serangan siber yang bertujuan memperoleh informasi sensitif, seperti nama pengguna, kata sandi, kode OTP, maupun data pribadi lainnya, dengan menyamar sebagai pihak atau layanan yang tepercaya [8].

Tabel 9. Tingkat Pemahaman Fungsi *Two Factor Authentication* (2FA)

Tingkat Pemahaman	Jumlah	Persentase
Sangat Mengetahui	3	10%
Mengetahui	8	26,7%
Cukup Mengetahui	11	36,7%
Kurang Mengetahui	7	23,3%
Tidak Mengetahui	1	3,3%
Total	**30**	**100%**

Tingkat pemahaman responden mengenai fungsi *Two Factor Authentication* (2FA) masih tergolong bervariasi. Sebagian besar responden berada pada kategori cukup mengetahui sebesar 36,7%, sedangkan responden yang mengetahui sebesar 26,7%.

Data tersebut menunjukkan bahwa meskipun penggunaan 2FA sudah cukup tinggi, pemahaman mendalam mengenai fungsi autentikasi dua faktor masih perlu ditingkatkan. Edukasi mengenai keamanan digital diperlukan agar mahasiswa dapat memahami manfaat penggunaan 2FA dalam melindungi akun digital dari ancaman keamanan siber.

Tabel 10. Kehati-hatian dalam Membagikan Data Pribadi di Media Sosial maupun Internet

Jawaban	Jumlah	Persentase
Selalu	24	80%
Jarang	4	13,3%
Tidak Pernah	2	6,7%
Total	**3**0	**100%**

Sebagian besar responden menyatakan selalu berhati-hati dalam membagikan data pribadi di media sosial maupun internet, yaitu sebanyak 80%. Namun demikian, masih terdapat responden yang jarang bahkan tidak pernah berhati-hati dalam membagikan informasi pribadi.

Data tersebut menunjukkan bahwa tingkat kesadaran mahasiswa terhadap perlindungan privasi digital sudah cukup baik, meskipun masih diperlukan peningkatan literasi keamanan digital agar seluruh pengguna lebih bijak dalam membagikan informasi pribadi di internet.

Tabel 11. Persepsi Penggunaan *Two Factor Authentication* (2FA) dalam Meningkatkan Keamanan Akun Digital

Jawaban	Jumlah	Persentase
Setuju	22	73,3%
Tidak Setuju	1	3,3%
Netral	7	23,3%
Total	**30**	**100%**

Mayoritas responden memiliki persepsi positif terhadap penggunaan *Two Factor Authentication* (2FA). Sebanyak 22 responden atau sebesar 73,3% setuju bahwa penggunaan 2FA dapat meningkatkan keamanan akun digital.

Hasil tersebut menunjukkan bahwa mahasiswa memahami pentingnya penggunaan sistem keamanan tambahan untuk melindungi akun digital dari ancaman akses ilegal dan peretasan. Penggunaan verifikasi dua langkah dinilai efektif dalam meningkatkan keamanan akun digital, terutama pada layanan media sosial, email, dan aplikasi digital lainnya.

penggunaan *multi-factor authentication* dapat meningkatkan keamanan akun dengan menambahkan metode verifikasi tambahan pada proses login pengguna.

Sejalan dengan hasil penelitian, penerapan *multi-factor authentication* memberikan lapisan keamanan tambahan melalui penggunaan lebih dari satu metode verifikasi identitas sehingga mampu mengurangi risiko akses tidak sah terhadap akun digital [4], [5].

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan terhadap mahasiswa Program Studi Informatika Universitas Nurul Huda, dapat disimpulkan bahwa tingkat kesadaran mahasiswa terhadap keamanan data pribadi dan penggunaan *Two Factor Authentication* (2FA) berada pada kategori cukup baik. Mayoritas responden telah memahami pentingnya menjaga keamanan data pribadi dalam penggunaan layanan digital, mengetahui risiko penyalahgunaan data pribadi, serta memahami ancaman *phishing* atau penipuan daring yang sering terjadi pada media digital dan layanan berbasis internet.

Hasil penelitian menunjukkan bahwa sebagian besar responden telah menggunakan fitur *Two Factor Authentication* (2FA) pada akun digital yang dimiliki. Penggunaan 2FA dinilai mampu memberikan perlindungan tambahan terhadap akun pengguna karena proses autentikasi tidak hanya menggunakan kata sandi, tetapi juga memerlukan tahap verifikasi tambahan seperti kode OTP maupun aplikasi autentikasi.

Meskipun demikian, tingkat pemahaman mahasiswa mengenai fungsi dan penerapan *Two Factor Authentication* (2FA) masih menunjukkan variasi. Sebagian responden masih berada pada kategori cukup mengetahui dan kurang mengetahui terkait fungsi autentikasi ganda dalam melindungi akun digital. Hal tersebut menunjukkan bahwa literasi keamanan digital masih perlu ditingkatkan, terutama terkait penggunaan kata sandi yang kuat, pengelolaan privasi digital, serta penerapan fitur keamanan tambahan pada layanan digital yang digunakan sehari-hari.

Selain itu, mayoritas responden menyatakan selalu berhati-hati dalam membagikan data pribadi di media sosial maupun internet. Sikap tersebut menunjukkan adanya kesadaran terhadap pentingnya menjaga privasi digital sebagai bagian dari perlindungan data pribadi. Perilaku kehati-hatian dalam penggunaan media digital menjadi salah satu langkah penting dalam mengurangi risiko kebocoran data dan penyalahgunaan identitas digital.

Secara keseluruhan, penelitian ini menunjukkan bahwa mahasiswa Informatika Universitas Nurul Huda telah memiliki tingkat kesadaran yang cukup baik terhadap keamanan data pribadi dan penggunaan *Two Factor Authentication* (2FA). Namun demikian, diperlukan upaya peningkatan edukasi, sosialisasi, dan literasi keamanan digital secara berkelanjutan di lingkungan akademik agar mahasiswa dapat menerapkan praktik keamanan digital dengan lebih optimal dan konsisten dalam kehidupan sehari-hari.

DAFTAR PUSTAKA

[1] Alharthi, A., Regan, M., Robertson, S., & Alkhateeb, H. (2022). Factors Affecting Cybersecurity Awareness among University Students. Applied Sciences, 12(5), 2589. https://doi.org/10.3390/app12052589

[2] IBM Security. (2023). Data Privacy and Protection Overview. Tersedia pada: https://www.ibm.com/topics/data-privacy

[3] Furnell, S., & Papadaki, M. (2016). A Holistic Approach to Information Security Awareness. Computers & Security, 62, 413–428. https://doi.org/10.1016/j.cose.2016.07.005

[4] Microsoft Security. (2024). What is Two-Factor Authentication (2FA)? Tersedia pada: https://www.microsoft.com/en-us/security/business/security-101/what-is-two-factor-authentication-2fa

[5] Google Safety Center. (2024). 2-Step Verification. Tersedia pada: https://safety.google/authentication/

[6] Krol, K., Philippou, E., De Cristofaro, E., & Sasse, M. A. (2015). They Brought in the Horrible Key Ring Thing! Analysing the Usability of Two-Factor Authentication in UK Online Banking. Proceedings of the USEC Workshop. Tersedia pada: https://arxiv.org/abs/1501.04489

[7] Shirvanian, M., & Agrawal, S. (2021). 2D-2FA: A New Dimension in Two-Factor Authentication. arXiv:2110.15872. Tersedia pada: https://arxiv.org/abs/2110.15872

[8] Kaspersky. (2023). What is Phishing and How to Prevent It. Tersedia pada: https://www.kaspersky.com/resource-center/threats/phishing

[9] Da Veiga, A., & Eloff, J. H. P. (2010). A Framework and Assessment Instrument for Information Security Culture. Computers & Security, 29(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002

[10] Sugiyono. (2023). Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Bandung: Alfabeta.

[11] Ghozali, I. (2021). Aplikasi Analisis Multivariate dengan Program IBM SPSS. Semarang: Badan Penerbit Universitas Diponegoro.

[12] Arikunto, S. (2019). Prosedur Penelitian: Suatu Pendekatan Praktik. Jakarta: Rineka Cipta.

[13] ENISA. (2023). Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. European Union Agency for Cybersecurity. Tersedia pada: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

[14] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

[15] Hadlington, L. (2017). Human Factors in Cybersecurity; Examining the Link Between Internet Addiction, Impulsivity, Attitudes Towards Cybersecurity, and Risky Cybersecurity Behaviours. Heliyon, 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346