

KEAMANAN DIGITAL DALAM PEMBELAJARAN PENDIDIKAN AGAMA ISLAM BERBASIS IT

Anggi Maulidia¹, Alfi Maulidiyah², Ilham Danil Ardinsyah³
dan M. Romadlon Habibullah, M.Pd.I⁴

¹²³⁴Program Studi Pendidikan Agama Islam, Universitas Nahdlatul Ulama Sunan Giri,
Bojonegoro, Indonesia

anggimaulidia620@gmail.com, maulidiyahalfi@gmail.com, ilhamdaniel080@gmail.com,
dan roma@unugiri.ac.id

Abstrak

Perkembangan teknologi informasi dan komunikasi (TIK) yang semakin pesat telah membawa perubahan signifikan dalam dunia pendidikan, khususnya dalam proses pembelajaran berbasis teknologi digital. Integrasi TIK membuka peluang terciptanya pembelajaran yang lebih fleksibel, interaktif, dan sesuai dengan tuntutan keterampilan abad ke-21. Namun, di balik berbagai kemudahan tersebut, muncul tantangan serius berupa ancaman keamanan digital yang berpotensi merugikan peserta didik, pendidik, maupun lembaga pendidikan. Artikel ini bertujuan untuk mengkaji secara komprehensif konsep keamanan digital dalam pembelajaran berbasis IT, meliputi pengertian dan ruang lingkup TIK, perkembangan TIK dalam dunia pendidikan, berbagai bentuk ancaman siber, prinsip-prinsip keamanan digital, serta strategi dan langkah praktis penerapannya di lingkungan pendidikan. Penelitian ini menggunakan pendekatan kepustakaan (*library research*) dengan menganalisis berbagai sumber literatur berupa buku, jurnal ilmiah, dan artikel yang relevan. Hasil kajian menunjukkan bahwa keamanan digital merupakan aspek fundamental yang harus menjadi perhatian utama dalam pembelajaran berbasis teknologi. Penerapan prinsip-prinsip keamanan digital secara konsisten, disertai edukasi dan kesadaran pengguna, dapat menciptakan ekosistem pembelajaran yang aman, bertanggung jawab, dan berkelanjutan. Dengan demikian, keamanan digital tidak hanya berfungsi sebagai pelindung teknologi, tetapi juga sebagai bagian penting dalam mendukung keberhasilan pembelajaran di era pendidikan digital modern.

Kata kunci: Teknologi Informasi dan Komunikasi; Keamanan Digital; Pembelajaran Berbasis IT; Pendidikan Digital; Literasi Digital

Abstract

The rapid development of information and communication technology (ICT) has brought significant changes to the field of education, particularly in technology-based digital learning processes. The integration of ICT creates opportunities for more flexible, interactive, and learner-centered education that aligns with the demands of 21st-century skills. However, behind these advantages, serious challenges have emerged in

Article History

Received: Januari 2026

Reviewed: Januari 2026

Published: Januari 2026

Plagiarism Checker No 234

Copyright : Author

Publish by : Tashdiq



This work is licensed under
a [Creative Commons](#)
[Attribution-NonCommercial](#)
[4.0 International License](#)

the form of digital security threats that may harm students, educators, and educational institutions. This article aims to comprehensively examine the concept of digital security in IT-based learning, including the definition and scope of ICT, the development of ICT in education, various forms of cyber threats, principles of digital security, as well as strategies and practical steps for its implementation in educational settings. This study employs a library research approach by analyzing various literature sources such as books, scientific journals, and relevant articles. The findings indicate that digital security is a fundamental aspect that must be a primary concern in technology-based learning. The consistent application of digital security principles, accompanied by user education and awareness, can create a safe, responsible, and sustainable learning ecosystem. Thus, digital security not only functions as a means of protecting technology but also plays an important role in supporting the success of learning in the modern digital education era.

Keywords: *Information and Communication Technology; Digital Security; IT-Based Learning; Digital Education; Digital Literacy*

1. Pendahuluan

Perubahan zaman yang ditandai dengan pesatnya perkembangan teknologi telah membawa dampak besar dalam berbagai aspek kehidupan manusia, termasuk dalam dunia pendidikan. Transformasi global yang didorong oleh revolusi digital menjadikan pendidikan sebagai salah satu sektor yang paling terdampak dan sekaligus terdorong untuk beradaptasi secara cepat dan sistemik. Kemunculan teknologi informasi dan komunikasi (TIK) membuka peluang yang sangat luas untuk merevolusi pendekatan tradisional dalam proses belajar mengajar menjadi lebih modern, fleksibel, dan personal. Namun, perkembangan tersebut juga menghadirkan tantangan baru, salah satunya adalah perlunya menjaga keamanan digital dalam proses pembelajaran yang berbasis teknologi. (Aulia Rahma Puteri et al, 2025)

Pendidikan di abad ke-21 menuntut tidak hanya mencetak lulusan yang cakap secara akademik, tetapi juga komunikatif, mampu berpikir kritis, kreatif, dan kolaboratif. Kemampuan ini tidak bisa lagi dikembangkan melalui model pendidikan konvensional yang bersifat satu arah dan kaku. Dalam konteks ini, TIK menjadi jembatan strategis yang dapat mengintegrasikan berbagai sumber belajar, gaya pembelajaran, dan interaksi sosial ke dalam satu sistem pendidikan digital yang dinamis. Menurut Munir, TIK dalam pendidikan bukan hanya alat bantu pengajaran, melainkan juga platform pengelolaan pengetahuan dan pengembangan karakter. Di Indonesia, adopsi TIK dalam dunia pendidikan semakin mendapat perhatian, terutama sejak pandemi COVID-19 memaksa sekolah dan perguruan tinggi beralih ke sistem pembelajaran daring. Hal ini mempercepat proses digitalisasi pendidikan sekaligus mengungkapkan berbagai tantangan struktural, seperti keterbatasan akses, rendahnya literasi digital, hingga kesiapan guru dan peserta didik dalam mengelola teknologi. Maka dari itu, pemahaman konseptual dan historis mengenai peran TIK dalam pendidikan menjadi penting agar integrasinya tidak bersifat reaktif, melainkan strategis dan transformatif. Lebih dari itu, pemanfaatan TIK dalam pendidikan bukan hanya berbicara tentang penggunaan alat, aplikasi, atau jaringan, tetapi juga tentang transformasi pedagogis. Perubahan ini menuntut guru untuk mendesain pembelajaran yang lebih kontekstual, interaktif, dan kolaboratif, sejalan dengan karakteristik generasi digital saat ini. Oleh sebab itu, dalam kajian ini akan dianalisis secara

komprehensif tentang (a) pengertian dan ruang lingkup TIK, (b) perkembangan historis TIK dalam dunia pendidikan, dan (c) implikasi pedagogis dari integrasi TIK ke dalam sistem pembelajaran.

Artikel ini membahas secara menyeluruh pentingnya keamanan digital dalam pembelajaran berbasis IT. Pembahasan mencakup konsep dasar keamanan digital, berbagai bentuk ancaman yang sering terjadi di lingkungan pendidikan, serta langkah-langkah strategis yang dapat diterapkan oleh guru, sekolah, maupun peserta didik dalam melindungi diri dari ancaman siber. Selain itu, artikel ini juga menyoroti peran penting lembaga pendidikan dalam menciptakan ekosistem pembelajaran yang aman, terarah, dan bertanggung jawab. Dengan adanya pemahaman yang tepat, diharapkan seluruh pihak dapat meningkatkan kewaspadaan dan menerapkan praktik keamanan digital secara konsisten dalam setiap aktivitas pembelajaran.

Dengan demikian, pendahuluan ini menegaskan bahwa keamanan digital merupakan aspek fundamental yang tidak dapat dipisahkan dari pembelajaran berbasis IT. Tanpa adanya perlindungan yang memadai, teknologi yang seharusnya menjadi sarana pendukung pembelajaran justru dapat menimbulkan kerugian dan risiko bagi penggunanya. Oleh karena itu, melalui pemaparan dalam artikel ini, diharapkan muncul kesadaran yang lebih kuat mengenai pentingnya menerapkan keamanan digital secara menyeluruh dalam lingkungan pendidikan modern.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan penelitian kepustakaan (*library research*). Penelitian kepustakaan adalah penelitian yang dilakukan dengan mengumpulkan data dan informasi dari berbagai sumber pustaka seperti buku, jurnal ilmiah, artikel, hasil penelitian, serta dokumen lainnya yang relevan dengan topik yang dikaji. Melalui pendekatan ini, peneliti tidak melakukan pengumpulan data lapangan, melainkan berfokus pada kajian teoritis dan analisis literatur untuk memperoleh pemahaman mendalam mengenai permasalahan penelitian.

3. Hasil dan Pembahasan

a. Pengertian Keamanan Digital

Keamanan digital telah menjadi isu yang semakin penting di era teknologi informasi dan komunikasi yang telah memberikan banyak manfaat bagi masyarakat. Akan tetapi teknologi baru ini juga memperkenalkan risiko baru. Ancaman keamanan digital dapat berupa serangan *malware*, peretasan, virus komputer, phishing, pencurian data, dan banyak lagi. Ancaman semakin kompleks dan sering kali mengakibatkan dampak yang merugikan, baik bagi individu maupun organisasi, baik secara materiil maupun psikologis. (Bambang Muryanto and Gilang Adikara, n.d.)

Berangkat dari situasi ancaman digital tersebut, maka penting untuk membekali pengguna internet dan media sosial untuk melindungi informasi, data, perangkat dan infrastruktur digital dari ancaman, serangan dan kejahatan di melalui teknologi digital. Ini mencakup segala hal yang terkait dengan keamanan komputer, jaringan komputer, sistem operasi, aplikasi dan data yang disimpan dalam lingkungan digital.

Keamanan digital, atau *digital security*, adalah upaya melindungi data, perangkat, dan informasi digital dari akses tidak sah, pencurian, atau kerusakan. Keamanan digital mencakup serangkaian tindakan dan teknologi yang digunakan untuk menjaga kerahasiaan, integritas, dan ketersediaan data serta sistem digital. (Adistiana & Hamami, 2024).

Secara umum, keamanan digital adalah perlindungan dari ancaman seperti virus komputer, *malware*, *ransomware*, *phishing*, dan serangan DDoS (*Distributed Denial of Service*). Namun, keamanan digital tidak hanya perlindungan data, tetapi juga memastikan data mudah diakses oleh pemiliknya dan tidak dapat dimodifikasi oleh siapapun yang tidak berwenang.

Pentingnya Keamanan Digital di Sekolah

Di era digital yang semakin maju, teknologi telah menjadi bagian tak terpisahkan dari dunia pendidikan. Siswa kini dapat mengakses berbagai sumber belajar secara daring, berkomunikasi dengan guru dan teman melalui platform digital, serta menggunakan media sosial sebagai sarana berbagi informasi. Namun, di balik kemudahan tersebut, ada tantangan besar yang harus dihadapi, yaitu keamanan digital. Kesadaran akan pentingnya keamanan digital menjadi hal yang wajib dimiliki oleh setiap siswa agar mereka dapat menggunakan internet dengan bijak dan terhindar dari berbagai risiko dunia maya. (Esturi Premata HatiEsturi Premata Hati, 2024).

Keamanan digital mencakup berbagai aspek, seperti perlindungan data pribadi, penggunaan internet yang bertanggung jawab, serta pencegahan terhadap ancaman siber, seperti peretasan, pencurian identitas, dan *cyberbullying*. Beberapa alasan mengapa kesadaran siswa terhadap keamanan digital sangat penting antara lain:

- 1) Melindungi Data Pribadi Banyak siswa sering membagikan informasi pribadi mereka secara daring tanpa menyadari risikonya. Informasi seperti alamat rumah, nomor telepon, atau bahkan kata sandi dapat disalahgunakan oleh pihak yang tidak bertanggung jawab.
- 2) Mencegah Cyberbullying Dunia digital memungkinkan interaksi sosial secara luas, tetapi juga membuka peluang bagi tindakan negatif seperti perundungan siber (*cyberbullying*). Kesadaran siswa tentang etika dalam berinternet dapat membantu menciptakan lingkungan digital yang lebih aman dan positif.
- 3) Menghindari Konten Berbahaya Internet menyajikan berbagai macam informasi, baik yang bermanfaat maupun yang berbahaya. Tanpa pemahaman yang baik tentang keamanan digital, siswa bisa saja mengakses konten yang tidak pantas atau terkena penipuan daring.
- 4) Menjaga Reputasi Digital Segala aktivitas yang dilakukan di dunia digital akan meninggalkan jejak. Jika siswa tidak berhati-hati dalam berkomentar atau membagikan sesuatu, hal tersebut bisa berdampak pada reputasi mereka di masa depan, termasuk dalam dunia pendidikan dan karier.

b. Prinsip-prinsip keamanan

Digital adalah panduan atau pedoman yang digunakan untuk memastikan keamanan sistem, data dan infrastruktur digital. Prinsip-prinsip ini membantu dalam melindungi informasi sensitif dari akses yang tidak sah, menjaga integritas data dan memastikan ketersediaan layanan yang kritis. (Muryanto and Adikara, n.d.) Berikut ini adalah beberapa prinsip utama keamanan Digital:

Prinsip-prinsip keamanan digital:

- 1) Kerahasiaan (*confidentiality*) Prinsip kerahasiaan berfokus pada perlindungan informasi agar hanya dapat diakses oleh pihak yang berwenang. Prinsip kerahasiaan memastikan bahwa datasensitif tetap terlindungi dari akses yang tidak sah atau pengungkapan yang tidak diinginkan.
- 2) Integritas (*integrity*) Prinsip integritas menjamin bahwa data dan informasi tetap utuh, tidak diubah atau dimanipulasi secara tidak sah. Prinsip integritas memastikan bahwa data tidak terpengaruh oleh perubahan yang tidak sah atau kehilangan integritasnya.
- 3) Ketersediaan (*availability*) Prinsip ketersediaan menekankan pentingnya memastikan bahwa sistem, data dan sumber dayaterkait tersedia ketika dibutuhkan. Prinsip ketersediaan memastikan bahwa layanan tetap dapat diakses dan digunakan oleh pengguna dengan minimal gangguan.

- 4) Keaslian (*authenticity*) Prinsip keaslian berfokus pada memverifikasi identitas dan keaslian entitas yang terlibat dalam transaksi atau komunikasi digital. Metode otentikasi seperti penggunaan kata sandi, kunci publik/privat atau sertifikat digital digunakan untuk memastikan bahwa entitas yang berpartisipasi adalah yang mereka klaim menjadi. Prinsip keaslian mencegah serangan pengguna palsu atau penggunaan identitas yang tidak sah.
- 5) Kontrol akses (*access control*) Prinsip kontrol akses berarti akses data atau sistem jaringan hanya diberikan kepada orang tertentu, hanya diberikan terbatas kepada beberapa orang dengan role atau departemen tertentu dalam suatu organisasi. Orang yang tidak diberi akses tidak dapat melihatnya, apalagi pihak eksternal organisasi.
- 6) Kebutuhan Paling Sedikit (*Least Privilege*) Prinsip ini menyatakan bahwa setiap entitas harus diberikan hak akses minimal yang diperlukan untuk menjalankan tugas atau fungsi mereka. Hal ini membantu mencegah penyalahgunaan atau akses yang tidak sah, karena setiap entitas hanya memiliki hak akses yang dibutuhkan secara spesifik.
- 7) Pertahanan Dalam Kedalaman (*Defense in Depth*) Prinsip ini melibatkan penggunaan serangkaian lapisan pertahanan dan kontrol keamanan untuk melindungi sistem dan data. Ini mencakup penggunaan *firewall*, deteksi serangan, enkripsi, pembaruan perangkat lunak dan kebijakan keamanan yang komprehensif. Prinsip pertahanan dalam kedalaman memastikan bahwa jika satu lapisan pertahanan gagal, masih ada lapisan lain yang melindungi sistem.

Prinsip-prinsip keamanan digital ini saling berkaitan dan saling mendukung untuk menciptakan lingkungan digital yang aman dan terlindungi. Dengan menerapkan prinsip-prinsip ini, organisasi dan individu dapat mengurangi risiko serangan dan melindungi informasi mereka dengan lebih efektif.

c. Strategi atau Cara Menerapkan Keamanan Digital

Ada banyak cara menjaga keamanan digital yang dapat diterapkan dalam aktivitas sehari-hari. Mengutip dari laman *The Commons Social Change Library* melalui artikel berjudul "*Digital Security Guide for Everyone*", setidaknya ada delapan cara efektif untuk meningkatkan keamanan digital. (Marhamah Ika Putri, n.d.) Bagaimana cara menerapkannya dan apa saja contoh keamanan digital? Berikut penjelasan lengkapnya:

- 1) Menggunakan Password yang Kuat
Menggunakan kata sandi yang kuat dan unik merupakan salah satu cara paling efektif untuk menjaga keamanan digital. Contoh penerapannya adalah dengan membuat kombinasi antara huruf besar, huruf kecil, angka, dan simbol untuk memperkuat kata sandi serta menghindari penggunaan informasi pribadi yang mudah ditebak.
- 2) Menerapkan Autentikasi Dua Faktor (*Two-Factor Authentication / 2FA*)
Autentikasi dua faktor atau *two-factor authentication* (2FA) adalah metode keamanan tambahan yang kini tersedia di hampir semua platform digital. 2FA bekerja dengan meminta verifikasi tambahan selain kata sandi, seperti kode OTP yang dikirim melalui SMS atau aplikasi autentikator, untuk mengakses akun.
- 3) Memperbarui Perangkat Lunak Secara Teratur
Jangan abaikan pembaruan perangkat lunak! Memastikan sistem operasi dan aplikasi diperbarui secara rutin adalah langkah penting untuk menutup celah keamanan yang bisa dimanfaatkan oleh peretas. Pembaruan ini biasanya mencakup perbaikan bug dan peningkatan keamanan.
- 4) Mengenkripsi Perangkat dan Data Sensitif
Enkripsi adalah salah satu cara melindungi data penting agar tidak mudah diakses oleh pihak yang tidak berwenang. Kamu bisa mengaktifkan fitur enkripsi bawaan pada perangkat seperti smartphone atau laptop untuk melindungi data sensitif, terutama jika perangkat hilang atau dicuri.

5) Waspada *Phishing* dan Penipuan *Online*

Sebagai pengguna internet, sangat disarankan untuk lebih bijak dalam beraktivitas di dunia digital agar terhindar dari phishing atau penipuan online. Jika menemui aktivitas mencurigakan, seperti tautan atau lampiran dari sumber yang tidak dikenal, sebaiknya jangan langsung dibuka, karena bisa saja itu merupakan upaya penipuan.

6) Manfaatkan Jaringan Pribadi Virtual (VPN)

Saat berada di tempat umum, pastikan untuk menggunakan VPN ketika mengakses jaringan Wi-Fi publik. VPN akan membantu mengenkripsi koneksi dan melindungi data pribadi dari risiko penyadapan.

7) Kelola Izin Aplikasi dengan Bijak

Sebelum menggunakan aplikasi tertentu, biasanya akan muncul permintaan izin akses terhadap berbagai data di perangkat. Bijaklah dalam memberikan izin akses terhadap informasi yang benar-benar dibutuhkan oleh aplikasi tersebut.

8) Lakukan Pencadangan Data Secara Berkala

Untuk menjamin keamanan digital, pastikan Anda rutin melakukan pencadangan data ke media penyimpanan eksternal atau layanan *cloud*. Ini penting sebagai langkah antisipasi jika terjadi serangan siber atau kerusakan perangkat yang dapat menyebabkan hilangnya data penting.

Memahami pentingnya keamanan digital memungkinkan kamu menggunakan internet secara lebih aman dan percaya diri.

d. Langkah Praktis Keamanan Digital

Di era digital, hampir semua aspek kehidupan kita terhubung dengan internet. Mulai dari belanja online, bekerja, berkomunikasi, hingga belajar, semuanya kini dilakukan secara digital. Namun, kemudahan ini juga membawa tantangan besar: bagaimana kita bisa menjaga keamanan di dunia maya?

Serangan siber, pencurian data, hingga penipuan online kini menjadi ancaman nyata yang bisa dialami siapa saja. Meski teknologi terus berkembang, keamanan digital tidak hanya tanggung jawab para ahli, tetapi juga dimulai dari langkah kecil kita sebagai pengguna. (Mutiara Aisyah, 2024).

Berikut adalah beberapa langkah sederhana yang dapat kita ambil untuk menciptakan dunia digital yang lebih aman:

1) Gunakan Kata Sandi yang Kuat dan Unik

Kata sandi (*password*) adalah kunci utama untuk melindungi akun dan data pribadi kita. Sayangnya, banyak orang masih menggunakan kata sandi yang lemah seperti “123456” atau “*password*”. Tips Membuat Kata Sandi yang Kuat:

- Gunakan kombinasi huruf besar, huruf kecil, angka, dan simbol.
- Hindari menggunakan informasi pribadi seperti tanggal lahir atau nama lengkap.
- Gunakan *password* manager untuk mengelola kata sandi unik untuk setiap akun.

2) Aktifkan Autentikasi Dua Faktor (2FA)

Autentikasi dua faktor adalah langkah tambahan untuk melindungi akun Anda. Dengan 2FA, Anda harus memberikan kode verifikasi tambahan selain kata sandi. Cara Mengaktifkan 2FA:

- Periksa pengaturan keamanan akun di platform seperti Gmail, Instagram, atau WhatsApp.
- Pilih opsi 2FA dan ikuti langkah-langkah untuk mengaktifkannya.

3) Hindari Mengklik Tautan yang Mencurigakan

Penipuan phishing sering kali mengarahkan Anda ke situs palsu yang mencuri data pribadi. Cara Menghindari *Phishing*:

- Periksa alamat pengirim email dengan teliti. Jangan klik tautan atau lampiran dari pengirim yang tidak dikenal.
 - Kunjungi situs web resmi langsung melalui browser, bukan dari tautan di email.
- 4) Selalu Perbarui Perangkat Lunak
Pembaruan perangkat lunak memberikan *patch* keamanan terbaru yang melindungi perangkat Anda dari ancaman. Tips Membarui Perangkat Lunak:
- Aktifkan pembaruan otomatis di perangkat Anda.
 - Unduh pembaruan hanya dari sumber resmi seperti *App Store* atau *Google Play*.
- 5) Lindungi Privasi Anda di Media Sosial
Informasi seperti lokasi, tanggal lahir, atau kebiasaan sehari-hari dapat dimanfaatkan untuk mencuri identitas Anda. Cara Melindungi Privasi Anda:
- Atur akun menjadi privat. Hindari membagikan informasi sensitif seperti alamat rumah atau nomor telepon.
 - Jangan membagikan jadwal perjalanan secara rinci.
- 6) Gunakan Wi-Fi Publik dengan Bijak
Wi-Fi publik sering kali tidak aman dan rentan terhadap serangan siber. Tips Aman Menggunakan Wi-Fi Publik:
- Hindari mengakses akun penting atau melakukan transaksi keuangan saat menggunakan Wi-Fi publik.
 - Gunakan VPN untuk mengenkripsi koneksi internet Anda.
 - Gunakan jaringan data seluler sebagai alternatif jika memungkinkan.
- 7) Cadangkan Data Anda Secara Rutin
Dengan mencadangkan data, Anda dapat memulihkan informasi penting meskipun perangkat Anda mengalami masalah. Cara Mencadangkan Data:
- Gunakan layanan cloud seperti Google Drive, Dropbox, atau iCloud.
 - Simpan salinan data penting di hard drive eksternal. c. Jadwalkan pencadangan secara otomatis.
- 8) Edukasi Diri dan Orang di Sekitar Anda
Keamanan digital adalah tanggung jawab bersama. Edukasi diri Anda tentang ancaman siber dan bagikan pengetahuan ini kepada orang lain. Tips Edukasi Keamanan Digital:
- Ikuti berita atau artikel terkait keamanan siber.
 - Ajarkan anak-anak atau orang tua cara menggunakan perangkat dengan aman.
 - Dukung diskusi tentang keamanan digital di komunitas Anda.

e. Contoh Penerapan Keamanan Digital dalam Pembelajaran PAI

Contoh penerapan keamanan digital dalam pembelajaran PAI adalah guru mengajarkan peserta didik untuk menjaga kerahasiaan akun pembelajaran daring, menggunakan sumber materi keislaman yang terpercaya, serta beretika dalam bermedia sosial sebagai wujud penerapan nilai amanah dan tanggung jawab dalam Islam.

Contoh penerapan kesadaran keamanan digital dalam pembelajaran PAI dapat dilakukan dengan mengintegrasikan materi akhlak dan etika bermedia digital, di mana guru PAI memberikan pemahaman kepada siswa tentang pentingnya menjaga data pribadi sebagai bentuk amanah, menghindari *cyberbullying* karena bertentangan dengan ajaran Islam tentang larangan menyakiti sesama, serta membimbing siswa untuk bersikap bijak dalam mengakses dan membagikan informasi di internet agar tidak merusak reputasi diri dan orang lain, sehingga nilai-nilai keislaman dapat terinternalisasi dalam perilaku siswa saat menggunakan teknologi digital.

Contoh penerapan prinsip-prinsip keamanan digital dalam pembelajaran PAI dapat diwujudkan melalui penggunaan sistem pembelajaran daring yang aman, di mana guru memastikan kerahasiaan data siswa dengan tidak menyebarkan informasi pribadi, menjaga

integritas tugas PAI dengan menekankan kejujuran dan larangan manipulasi atau plagiarisme, menjamin ketersediaan materi pembelajaran agar dapat diakses siswa saat dibutuhkan, serta menerapkan keaslian dan kontrol akses melalui akun resmi siswa, sehingga nilai-nilai Islam seperti amanah, kejujuran, dan tanggung jawab dapat diinternalisasikan dalam praktik pembelajaran berbasis digital.

Contoh penerapan strategi keamanan digital dalam pembelajaran PAI dapat dilakukan dengan membiasakan siswa menggunakan kata sandi yang kuat dan autentikasi dua faktor pada akun pembelajaran daring, mengakses materi PAI melalui perangkat dan aplikasi yang selalu diperbarui, serta mengajarkan sikap waspada terhadap tautan atau informasi keagamaan yang tidak jelas sumbernya sebagai bentuk *tabayyun*, sehingga siswa mampu mempraktikkan nilai-nilai amanah, kehati-hatian, dan tanggung jawab dalam penggunaan teknologi digital sesuai dengan ajaran Islam.

Contoh penerapan langkah praktis keamanan digital dalam pembelajaran PAI dapat dilakukan dengan membimbing siswa menggunakan kata sandi yang kuat dan autentikasi dua faktor pada akun pembelajaran, mengajarkan kehati-hatian dalam membuka tautan atau informasi keagamaan sebagai bentuk *tabayyun*, membiasakan pembaruan perangkat dan pencadangan tugas PAI secara rutin, serta menanamkan etika menjaga privasi di media sosial sebagai implementasi nilai amanah, kehati-hatian, dan tanggung jawab dalam Islam.

4. Simpulan

Keamanan digital merupakan kebutuhan yang tidak dapat dipisahkan dari kehidupan masyarakat modern, terutama dalam dunia pendidikan yang semakin bergantung pada teknologi informasi dan komunikasi. Perkembangan teknologi memang memberikan banyak kemudahan dalam proses pembelajaran, namun di saat yang sama juga menghadirkan berbagai risiko seperti pencurian data, peretasan, penipuan daring, hingga cyberbullying. Oleh karena itu, pemahaman yang baik mengenai keamanan digital menjadi hal yang sangat penting bagi seluruh pengguna teknologi, khususnya peserta didik dan pendidik di lingkungan sekolah.

Dalam konteks pendidikan, keamanan digital tidak hanya berkaitan dengan perlindungan data dan perangkat, tetapi juga menyangkut pembentukan sikap dan perilaku bertanggung jawab dalam menggunakan teknologi. Kesadaran siswa terhadap pentingnya menjaga data pribadi, bersikap etis di ruang digital, serta bijak dalam mengakses dan menyebarkan informasi perlu ditanamkan sejak dini. Penerapan prinsip-prinsip keamanan digital seperti kerahasiaan, integritas, ketersediaan, keaslian, dan kontrol akses menjadi landasan penting dalam menciptakan lingkungan pembelajaran yang aman dan terpercaya.

Selain itu, penerapan strategi dan langkah praktis keamanan digital, seperti penggunaan kata sandi yang kuat, autentikasi dua faktor, pembaruan perangkat lunak, kewaspadaan terhadap phishing, serta pencadangan data secara rutin, terbukti dapat meminimalkan risiko ancaman siber. Upaya ini akan lebih efektif apabila didukung oleh edukasi berkelanjutan dan kerja sama antara siswa, guru, sekolah, dan orang tua.

Dalam pembelajaran Pendidikan Agama Islam (PAI), keamanan digital juga dapat diintegrasikan dengan nilai-nilai keislaman seperti amanah, kejujuran, kehati-hatian (*tabayyun*), dan tanggung jawab. Dengan demikian, penggunaan teknologi digital tidak hanya aman secara teknis, tetapi juga selaras dengan pembentukan akhlak dan karakter peserta didik. Secara keseluruhan, keamanan digital bukan sekadar aspek pelengkap, melainkan fondasi penting dalam mendukung keberhasilan pembelajaran dan menciptakan ekosistem pendidikan digital yang aman, etis, dan berkelanjutan.

Daftar Referensi

- Hati, Esturi Premata. "Pentingnya Kesadaran Siswa Terhadap Keamanan Digital Dalam Dunia Pendidikan." SMPN 1 RINGINREJO, 2024.
<https://smpn1ringinrejo.sch.id/read/308/pentingnya-kesadaran-siswa-terhadap-keamanan-digital-dalam-dunia-pendidikan>.
- Marhamah Ika Putri. "Keamanan Digital: Strategi Efektif Untuk Mencegah Serangan Siber." tirto.id, n.d. https://tirto.id/keamanan-digital-pengertian-manfaat-dan-cara-menerapkannya-habQ#google_vignette.
- Muryanto, Bambang, and Gilang Adikara. "H a n d b o o k Digital Safety," n.d. Mutiara Aisyah. "Langkah Sederhana Untuk Keamanan Digital Yang Lebih Baik." Cloud Computing Indonesia, 2024. <https://event.cloudcomputing.id/tips-trik/langkah-untuk-keamanan-digital>.
- Puteri, Aulia Rahma, Wahyudin Nur Nasution, Muhammad Irwan, Padli Nasution, and U I N Sumatera Utara. "Jurnal Pendidikan Indonesia : Integrasi Teknologi Informasi Dan Komunikasi Dalam Pendidikan : Konsep , Perkembangan , Dan Inovasi Media Pembelajaran" 5, no. 4 (2025). <https://doi.org/10.59818/jpi.v5i4.1760>.
- VIDA.ID. "Keamanan Digital: Definisi, Cara Melindungi, Dan Manfaat," 2024. <https://vida.id/id/blog/keamanan-digital>.