JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Analisis Dampak Human Error Terhadap Kebocoran Data Pribadi di Kalangan Pengguna Digital

Dian Humaira[1], Nur Aza Fazlasya[2], Sadhi Alwi[3*], Putra Harapan Tafonao[4]
[1,2,3,4,5]Universitas Malikusssaleh, Indonesia
[1]dian.240170002@mhs.unimal.ac.id, [2]nur.240170012@mhs.unimal.ac.id, [3]sadhi.240170001@mhs.unimal.ac.id, [4]putra.240170030@mhs.unimal.ac.id

ABSTRACT

The rapid development of digital technology has increased the risk of personal data leakage, which is often caused by human error rather than system technical failures. This study aims to analyze the impact of human error, such as the use of weak passwords, clicking on phishing links, and sharing excessive information on social media, on the security of personal data. The research method used is a qualitative approach through literature review and analysis of recent data leakage cases. The results indicate that low digital literacy is the main factor contributing to human error. This study concludes that an increase in digital security awareness and education is essential to minimize the risk of data leakage caused by human factors.

Keywords: *Human Error, Data Leakage, Personal Data, Digital Security, Digital Literacy.*

PENDAHULUAN

Di era transformasi digital saat ini, penggunaan teknologi informasi telah menjadi bagian yang tidak terpisahkan dari kehidupan masyarakat. Berbagai aktivitas seperti komunikasi, transaksi keuangan, penggunaan media sosial, hingga penyimpanan data pribadi dilakukan melalui sistem digital. Kondisi ini menjadikan data pribadi sebagai aset yang sangat bernilai, namun juga rentan terhadap ancaman keamanan informasi.

Meskipun sistem keamanan teknologi terus mengalami perkembangan, kasus kebocoran data pribadi masih sering terjadi. Laporan *Data Breach Investigations Report* (DBIR) oleh Verizon (2023) menunjukkan bahwa sebagian besar insiden kebocoran data tidak hanya disebabkan oleh kegagalan sistem teknis, tetapi juga dipicu oleh kesalahan manusia (*human error*). Hal ini menegaskan bahwa faktor manusia merupakan salah satu titik lemah utama dalam rantai keamanan siber.

Human error dalam konteks keamanan digital mencakup tindakan yang tidak disengaja, kelalaian, maupun kurangnya pemahaman pengguna dalam menjaga keamanan data pribadi. Bentuk human error yang umum terjadi antara lain penggunaan kata sandi yang lemah, ketidaksadaran terhadap serangan phishing, penggunaan jaringan publik tanpa pengamanan, serta perilaku *oversharing* di media sosial. Rendahnya tingkat literasi digital dan kurangnya kesadaran terhadap risiko keamanan siber menjadi faktor utama yang memperbesar kemungkinan terjadinya kebocoran data pribadi.

Sejumlah penelitian sebelumnya telah membahas kebocoran data dari sisi teknis keamanan sistem. Namun, kajian yang secara khusus menyoroti peran human error sebagai penyebab dominan kebocoran data pribadi masih perlu dikaji lebih mendalam. Oleh karena itu, penelitian ini difokuskan pada analisis dampak human error terhadap kebocoran data pribadi di kalangan pengguna digital.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis berbagai bentuk human error yang berkontribusi terhadap kebocoran data pribadi serta dampaknya terhadap privasi pengguna digital. Selain itu, penelitian ini juga memberikan rekomendasi strategis untuk memitigasi risiko kebocoran data melalui peningkatan literasi dan kesadaran keamanan digital guna menciptakan lingkungan digital yang lebih aman.

TINJAUAN PUSTAKA

Kebocoran Data Pribadi

Kebocoran data pribadi merupakan kondisi ketika informasi sensitif, rahasia, atau dilindungi milik individu terekspos, diakses, atau digunakan oleh pihak yang tidak berwenang. Data pribadi mencakup informasi identitas seperti nama lengkap, alamat, nomor identitas, nomor telepon, hingga data keuangan dan akun digital. Menurut standar ISO/IEC 27001, kebocoran data dapat terjadi akibat kegagalan sistem, serangan siber, maupun kesalahan manusia dalam pengelolaan informasi.

Dalam konteks keamanan informasi, kebocoran data pribadi menjadi ancaman serius karena dapat menimbulkan dampak jangka panjang bagi individu. Furnell dan Clarke (2012) menjelaskan bahwa kebocoran data tidak hanya menyebabkan kerugian finansial, tetapi juga berpotensi merusak reputasi serta menurunkan tingkat kepercayaan pengguna terhadap sistem digital. Hal ini diperkuat oleh laporan Verizon (2023) yang menunjukkan bahwa insiden kebocoran data masih sering terjadi seiring meningkatnya penggunaan layanan digital.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Selain faktor teknis, kebocoran data pribadi juga dipengaruhi oleh perilaku pengguna dalam mengelola informasi digital. Kesalahan dalam pengaturan privasi, penggunaan kata sandi yang tidak aman, serta kurangnya pemahaman terhadap risiko keamanan siber menjadi faktor pendukung terjadinya kebocoran data. Oleh karena itu, kajian mengenai kebocoran data pribadi perlu mempertimbangkan aspek teknis dan non-teknis secara bersamaan.

Human Error dalam Keamanan Siber

Human error dalam konteks keamanan siber merujuk pada kesalahan atau kelalaian pengguna yang berkontribusi terhadap terjadinya pelanggaran keamanan informasi. Sasse, Brostoff, dan Weirich (2001) menyatakan bahwa faktor manusia sering kali menjadi titik lemah utama dalam sistem keamanan informasi, meskipun teknologi pengamanan telah dirancang dengan baik.

Beberapa bentuk human error yang umum terjadi antara lain penggunaan kata sandi yang lemah atau sama pada beberapa akun, ketidaksadaran terhadap serangan phishing, penggunaan jaringan publik tanpa pengamanan, serta perilaku oversharing di media sosial. Parsons et al. (2017) menjelaskan bahwa rendahnya kesadaran keamanan dan perilaku pengguna yang berisiko memiliki hubungan langsung dengan meningkatnya kemungkinan kebocoran data pribadi. Hadlington (2018) juga menegaskan bahwa rendahnya literasi digital dan sikap abai terhadap keamanan siber memperbesar peluang terjadinya kesalahan pengguna. Sementara itu, ENISA (2022) menyatakan bahwa sebagian besar insiden keamanan siber melibatkan faktor manusia, sehingga pendekatan keamanan tidak dapat hanya berfokus pada teknologi, tetapi juga harus mencakup edukasi dan peningkatan kesadaran pengguna. Berdasarkan kajian literatur tersebut, dapat disimpulkan bahwa human error merupakan faktor dominan dalam terjadinya kebocoran data pribadi di kalangan pengguna digital. Oleh karena itu, peningkatan literasi digital dan kesadaran keamanan siber menjadi langkah penting dalam meminimalkan risiko kebocoran data akibat kesalahan manusia.

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif. Teknik pengumpulan data yang digunakan meliputi:

1. **Studi Pustaka:** Menghimpun sumber referensi dari artikel ilmiah, laporan keamanan siber, dan jurnal terkait dampak perilaku manusia terhadap keamanan data.
2. **Analisis Kasus:** Mengamati fenomena kebocoran data terbaru yang disebabkan oleh faktor kelalaian pengguna di Indonesia.

HASIL DAN PEMBAHASAN

Berdasarkan hasil analisis, ditemukan beberapa faktor utama *human error* yang berdampak signifikan pada kebocoran data pribadi:

1. **Kelalaian Kata Sandi:** Penggunaan kata sandi yang sama untuk berbagai akun atau kata sandi yang mudah ditebak mempermudah serangan *brute force*.
2. **Serangan Phishing:** Kurangnya ketelitian pengguna dalam membedakan email atau situs web resmi dengan yang palsu menyebabkan penyerahan data secara sukarela kepada pelaku kejahatan.
3. **Penggunaan Jaringan Tidak Aman:** Mengakses data sensitif melalui Wi-Fi publik tanpa enkripsi tambahan (seperti VPN).

Tabel 1. Jenis Human Error dan Dampaknya terhadap Keamanan Data Pribadi
Sumber: Olahan penulis, 2024

Jenis Human Error	Cara Kerja / Mekanisme	Dampak terhadap Keamanan Data
Kata Sandi Lemah	Penggunaan sandi sederhana atau sama di banyak akun	Pengambilalihan akun dan pencurian identitas
Phishing	Mengklik tautan palsu atau lampiran berbahaya	Kebocoran kredensial dan akses ilegal
Oversharing	Membagikan data pribadi di media sosial	Serangan social engineering dan stalking
Jaringan Publik	Akses Wi-Fi tanpa enkripsi	Penyadapan data (Man-in-the-Middle)
Aplikasi Tidak Resmi	Instalasi aplikasi tidak terverifikasi	Penyusupan spyware dan pencurian data

Berdasarkan Tabel 1, dapat diketahui bahwa berbagai jenis *human error* memiliki mekanisme yang berbeda dalam menyebabkan terjadinya kebocoran data pribadi. Penggunaan kata sandi yang lemah, seperti sandi sederhana atau digunakan berulang pada beberapa akun, memudahkan pelaku kejahatan melakukan pengambilalihan akun dan pencurian identitas pengguna. Hal ini menunjukkan bahwa praktik manajemen kata sandi yang tidak aman masih menjadi salah satu penyebab utama pelanggaran keamanan data.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Selain itu, serangan phishing menjadi bentuk *human error* yang sering terjadi akibat kurangnya kewaspadaan pengguna dalam membedakan tautan atau situs resmi dengan yang palsu. Ketika pengguna secara tidak sadar memasukkan kredensial pada situs palsu, data tersebut dapat dengan mudah diakses oleh pihak yang tidak berwenang. Perilaku *oversharing* di media sosial juga meningkatkan risiko serangan *social engineering* dan stalking, karena informasi pribadi dapat dimanfaatkan oleh pelaku kejahatan untuk melakukan manipulasi atau penipuan.

Penggunaan jaringan publik tanpa enkripsi, seperti Wi-Fi umum, memungkinkan terjadinya penyadapan data melalui serangan *Man-in-the-Middle*. Sementara itu, instalasi aplikasi tidak resmi atau tidak terverifikasi berpotensi menyebabkan penyusupan *spyware* yang dapat mencuri data pribadi pengguna tanpa disadari. Secara keseluruhan, tabel ini menunjukkan bahwa sebagian besar kebocoran data pribadi tidak hanya disebabkan oleh kelemahan sistem, tetapi juga oleh perilaku dan kelalaian pengguna dalam menjaga keamanan data.

Tabel 2. Strategi Pencegahan Kebocoran Data akibat Human Error
Sumber: Olahan penulis, 2024

Strategi Pencegahan	Implementasi	Manfaat
Otentikasi Dua Faktor	Mengaktifkan 2FA	Lapisan keamanan tambahan
Enkripsi Data	VPN dan end-to-end encryption	Menjaga kerahasiaan data
Manajer Kata Sandi	Penggunaan password manager	Menghindari sandi berulang
Audit Privasi	Peninjauan pengaturan akun	Mencegah paparan data
Literasi Digital	Edukasi dan simulasi phishing	Mengurangi human error

Berdasarkan Tabel 2, dapat diketahui bahwa strategi pencegahan kebocoran data akibat *human error* memerlukan kombinasi antara solusi teknis dan peningkatan kesadaran pengguna. Penerapan otentikasi dua faktor (2FA) memberikan lapisan keamanan tambahan dengan mewajibkan verifikasi ganda, sehingga dapat mengurangi risiko pengambilalihan akun meskipun kata sandi pengguna berhasil diketahui pihak tidak berwenang.

Penggunaan enkripsi data, seperti VPN dan *end-to-end encryption*, berperan penting dalam menjaga kerahasiaan informasi saat proses transmisi data, terutama ketika pengguna mengakses jaringan publik. Selain itu, pemanfaatan *password manager* membantu pengguna dalam mengelola kata sandi yang kuat dan unik pada setiap akun, sehingga mengurangi risiko penggunaan kata sandi yang berulang.

Strategi audit privasi melalui peninjauan pengaturan akun secara berkala juga efektif dalam mencegah paparan data pribadi yang tidak disadari pengguna. Sementara itu, peningkatan literasi digital melalui edukasi dan simulasi serangan phishing berperan dalam meningkatkan kewaspadaan pengguna terhadap ancaman keamanan siber. Secara keseluruhan, tabel ini menunjukkan bahwa pencegahan kebocoran data akibat *human error* tidak hanya bergantung pada teknologi, tetapi juga pada perilaku dan kesadaran pengguna digital.

Berdasarkan hasil analisis pada Tabel 1, dapat diketahui bahwa sebagian besar kebocoran data pribadi disebabkan oleh kesalahan pengguna dalam mengelola keamanan akun digital. Penggunaan kata sandi yang lemah dan ketidaksadaran terhadap serangan phishing menjadi faktor yang paling dominan karena secara langsung membuka akses terhadap akun dan data pribadi pengguna. Selain itu, perilaku *oversharing* di media sosial, penggunaan jaringan publik tanpa enkripsi, serta instalasi aplikasi tidak resmi turut meningkatkan risiko serangan *social engineering*, penyadapan data, dan pencurian informasi. Temuan ini menunjukkan bahwa ancaman keamanan informasi tidak hanya berasal dari sisi teknis, tetapi juga sangat dipengaruhi oleh perilaku dan kebiasaan pengguna dalam beraktivitas di ruang digital.

Sementara itu, berdasarkan Tabel 2, penerapan teknologi keamanan seperti otentikasi dua faktor dan enkripsi data terbukti mampu mengurangi risiko kebocoran data pribadi secara signifikan dengan menambah lapisan perlindungan pada akun dan proses transmisi data. Penggunaan *password manager* dan audit privasi juga membantu pengguna dalam mengelola keamanan akun secara lebih efektif. Namun demikian, efektivitas penerapan teknologi tersebut sangat bergantung pada tingkat kesadaran dan literasi digital pengguna. Oleh karena itu, kombinasi antara solusi teknis dan edukasi keamanan digital menjadi kunci utama dalam meminimalkan risiko kebocoran data akibat *human error*.

KESIMPULAN

Dapat disimpulkan bahwa *human error* merupakan faktor dominan dalam insiden kebocoran data pribadi di kalangan pengguna digital. Kerentanan ini tidak hanya disebabkan oleh kelemahan teknis, tetapi lebih kepada perilaku dan rendahnya tingkat kesadaran keamanan pengguna. Oleh karena itu, diperlukan upaya kolaboratif antara penyedia layanan teknologi dan pengguna untuk meningkatkan literasi digital sebagai langkah preventif utama dalam melindungi privasi data di masa depan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada seluruh pihak yang telah memberikan dukungan serta informasi dalam penyelesaian penelitian ini. Terima kasih juga disampaikan kepada rekan-rekan sejawat

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

yang telah memberikan masukan berharga sehingga jurnal ini dapat terselesaikan dengan baik sesuai standar ilmiah.

REFERENSI

Alhogail, A. (2015). *Design and validation of information security culture framework*. Computers in Human Behavior.

ENISA. (2022). *Human factors in cybersecurity*. European Union Agency for Cybersecurity.

Furnell, S., & Clarke, N. (2012). *Power to the people? The evolving recognition of human aspects of security*. Computers & Security.

Hadlington, L. (2018). *Employees' attitudes towards cybersecurity and risky online behaviours*. Information & Computer Security.

Parsons, K., et al. (2017). *The human aspects of information security questionnaire (HAIS-Q)*. Computers & Security.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). *Transforming the weakest link—A human/computer interaction approach to usable and effective security*. BT Technology Journal.

Verizon. (2023). *Data Breach Investigations Report (DBIR)*. Verizon Enterprise.