JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika

[E-ISSN 2656-0321]
[Vol 20 No 1]
[Januari 2026]

# ANALISIS KEAMANAN SIBER PADA SISTEM ELEKTRONIK BERBASIS PERSPEKTIF JARINGAN KOMPUTER DAN KETENTUAN BSSN: STUDI PADA IMBAUAN PHISHING DAN PENCURIAN KREDENSIAL

Firda Maulida Prayetno [a,1,*], Faiqotur Riski [b,2], Devi Linda Ayu Safitri [c,3]
[a,b,c] Informatika, UIN Sunan Kalijaga, Yogyakarta
[1] 24206051020@student.uin-suka.ac.id*; [2] 24206051002@student.uin-suka.ac.id; [3] 24206051018@student.uin-suka.ac.id
* Firda Maulida Prayetno

ARTICLE INFO

**Keywords**
phishing, credential theft, computer networks, BSSN, security advisory.

ABSTRACT

Phishing attacks and credential theft are a growing cyber threat in Indonesia, particularly in the context of the use of electronic systems for public services. The National Cyber and Crypto Agency (BSSN) regularly issues security advisories to warn the public about attack patterns, potential losses, and mitigation measures. This study aims to analyze security messages related to phishing and credentials from a computer network security perspective and their alignment with the BSSN security policy framework. The research method used is a content analysis of relevant BSSN security advisories, complemented by a literature review on network security, social engineering, and information security governance standards. The results show that phishing attacks exploit weaknesses in the network layer, authentication, and user awareness. Attacks are primarily carried out through social engineering, perpetuation to fake websites, man-in-the-middle attacks, and credential harvesting. This study's recommendations include implementing layered security, increasing user awareness, strengthening authentication, and implementing information security governance in accordance with BSSN regulations. This research is expected to contribute to an improved understanding of phishing threats in the context of national cybersecurity.

## 1. Pendahuluan

Perkembangan teknologi informasi menyebabkan peningkatan penggunaan sistem elektronik pada berbagai sektor pelayanan publik di Indonesia[1]. Di sisi lain, meningkatnya aktivitas digital memunculkan ancaman siber, salah satunya serangan phishing dan pencurian kredensial[2] yang merupakan serangan paling sering dilaporkan dalam beberapa tahun terakhir. Berdasarkan laporan BSSN, ancaman phishing meningkat karena metode ini memanfaatkan kelemahan manusia dan jaringan yang sulit dideteksi oleh pengguna awam[3].

BSSN sebagai lembaga pemerintah yang menangani keamanan siber nasional secara rutin menerbitkan imbauan keamanan (security advisory) sebagai bentuk edukasi dan peringatan terhadap ancaman siber yang sedang marak terjadi. Imbauan tersebut mencakup jenis ancaman, modus operandi, target serangan, serta rekomendasi mitigasi[4]. Hal ini menunjukkan pentingnya pemahaman terhadap pola serangan phishing dalam konteks keamanan jaringan komputer agar langkah mitigasi dapat dilakukan secara tepat. Serangan phishing sering dilakukan melalui media sosial, pesan singkat, maupun email, yang mengarahkan korban ke situs palsu untuk mencuri kredensial seperti kata sandi, data login, maupun informasi sensitif lainnya. Teknik yang digunakan penyerang tidak hanya berupa rekayasa sosial, tetapi juga memanfaatkan kelemahan jaringan seperti DNS spoofing, SSL stripping, atau man-in-the-middle attack[5].

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 20 No 1]
[Januari 2026]

Berdasarkan urgensi tersebut, penelitian ini dilakukan untuk menganalisis imbauan keamanan BSSN tentang phishing dan pencurian kredensial dari sudut pandang keamanan jaringan komputer serta relevansinya dengan tata kelola keamanan informasi menurut regulasi BSSN. Diharapkan penelitian ini dapat memberikan gambaran akademis mengenai pola ancaman dan mitigasinya.

## 2. Kajian Teori

Keamanan Jaringan Komputer

Keamanan jaringan komputer berfokus pada perlindungan data dan infrastruktur jaringan dari serangan yang dapat mengancam kerahasiaan, integritas, dan ketersediaan informasi. Ancaman yang berkaitan dengan phishing umumnya melibatkan teknik seperti man-in-the-middle attack, DNS spoofing, session hijacking, dan pencurian kredensial melalui protokol jaringan yang tidak aman. Kontrol keamanan yang sering digunakan mencakup firewall, IDS/IPS, enkripsi, DNSSEC, dan autentikasi multi-faktor[6].

Phishing dan Pencurian Kredensial

Phishing adalah teknik rekayasa sosial yang bertujuan mencuri informasi sensitif dengan memanipulasi korban agar memberikan data pribadi pada situs palsu. Bentuk umum phishing meliputi email phishing, spear phishing, whaling, dan smishing. Pencurian kredensial terjadi ketika penyerang memperoleh username dan password korban untuk mengakses sistem elektronik secara tidak sah[7].

Kerangka Regulasi BSSN

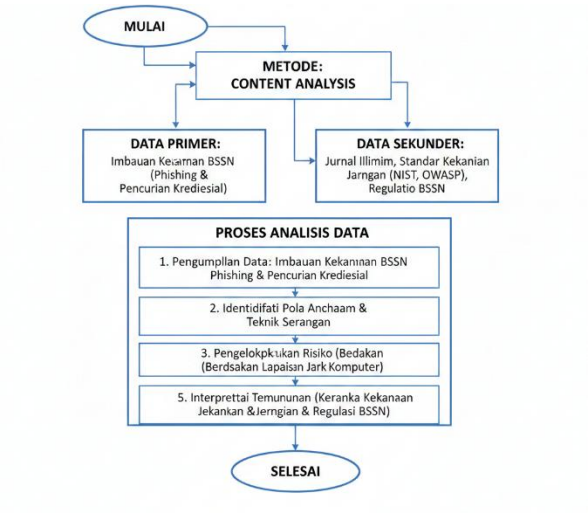
BSSN menetapkan beberapa regulasi terkait keamanan informasi, seperti PERKA BSSN No. 4 Tahun 2021 tentang Kategori Sistem Elektronik dan PERKA BSSN No. 8 Tahun 2020 tentang Tata Kelola Keamanan Informasi. Imbauan keamanan BSSN berfungsi sebagai panduan tambahan untuk meningkatkan kesiapsiagaan masyarakat terhadap ancaman siber[8].

Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode content analysis, di mana data primer berasal dari imbauan keamanan (security advisory) BSSN yang berkaitan dengan phishing dan pencurian kredensial, sedangkan data sekunder diperoleh dari jurnal ilmiah, dokumen standar keamanan jaringan, publikasi NIST, OWASP, serta regulasi BSSN. Proses analisis dilakukan melalui beberapa tahap, yaitu mengumpulkan seluruh imbauan keamanan BSSN terkait phishing dan pencurian kredensial, mengidentifikasi pola ancaman serta teknik serangan yang digunakan, mengelompokkan risiko berdasarkan lapisan jaringan komputer yang terdampak, menganalisis langkah mitigasi yang disampaikan oleh BSSN, dan akhirnya menginterpretasikan temuan tersebut berdasarkan kerangka keamanan jaringan serta ketentuan yang tercantum dalam regulasi BSSN.

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika

[E-ISSN 2656-0321]
[Vol 20 No 1]
[Januari 2026]




Gambar 1. Alur Metodologi Penelitian

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 20 No 1]
[Januari 2026]

## 3. Hasil dan Pembahasan

### 3.1 Pola Phishing Berdasarkan Imbauan BSSN

Hasil analisis menunjukkan bahwa mayoritas imbauan phishing yang dikeluarkan oleh Badan Siber dan Sandi Negara (BSSN) menyoroti berbagai modus serangan yang memanfaatkan kanal komunikasi digital yang umum digunakan masyarakat. Modus yang paling dominan meliputi penyebaran pesan WhatsApp palsu yang mengatasnamakan instansi resmi, email penipuan yang menyerupai lembaga pemerintah, tautan login palsu yang dirancang menyerupai situs resmi, permintaan One Time Password (OTP) palsu, serta penggunaan formulir daring palsu yang disebarkan melalui pesan spam. Pola ini menunjukkan bahwa pelaku phishing cenderung mengeksploitasi tingkat kepercayaan masyarakat terhadap institusi negara dan layanan digital yang sering diakses dalam aktivitas sehari-hari.

Lebih lanjut, BSSN menegaskan bahwa serangan phishing tidak hanya mengandalkan teknik rekayasa sosial (social engineering) untuk memanipulasi korban secara psikologis, tetapi juga secara sistematis diarahkan pada pencurian kredensial (credential harvesting). Kredensial yang dicuri tersebut kemudian dimanfaatkan untuk memperoleh akses tidak sah ke akun pemerintahan, layanan publik berbasis digital, serta data pribadi pengguna. Hal ini menunjukkan adanya pergeseran dari phishing sederhana yang bersifat informatif menuju phishing yang lebih kompleks dan terstruktur, dengan tujuan eksploitasi data dan penyalahgunaan identitas digital.

Dalam konteks hasil analisis, temuan ini mengindikasikan bahwa pola phishing yang diamati memiliki karakteristik adaptif terhadap perkembangan teknologi dan kebiasaan pengguna. Penggunaan platform populer seperti WhatsApp dan email resmi menunjukkan bahwa pelaku phishing berupaya meningkatkan tingkat keberhasilan serangan dengan menyesuaikan medium serangan pada saluran komunikasi yang dianggap paling kredibel oleh korban. Selain itu, pemalsuan tampilan situs dan formulir daring memperlihatkan peningkatan kualitas teknis serangan, sehingga semakin sulit dibedakan dari layanan resmi.

Dari sisi pembahasan, imbauan BSSN mencerminkan urgensi peningkatan literasi keamanan siber di kalangan masyarakat dan aparatur pemerintahan. Serangan phishing yang menargetkan kredensial akun pemerintahan dan layanan publik berpotensi menimbulkan dampak serius, seperti kebocoran data sensitif, gangguan layanan, serta penyalahgunaan akses oleh pihak yang tidak bertanggung jawab. Oleh karena itu, pola phishing yang diidentifikasi melalui imbauan BSSN dapat dijadikan dasar untuk merumuskan strategi mitigasi yang lebih efektif, baik melalui peningkatan kesadaran pengguna, penguatan sistem autentikasi, maupun penerapan kebijakan keamanan informasi yang lebih ketat.

Secara keseluruhan, hasil analisis ini menunjukkan bahwa pola phishing di Indonesia, sebagaimana tercermin dalam imbauan BSSN, bersifat dinamis dan terus berkembang. Hal ini menuntut pendekatan penanggulangan yang tidak hanya reaktif terhadap insiden, tetapi juga proaktif melalui edukasi, sosialisasi, dan penguatan sistem keamanan siber secara berkelanjutan.

### 3.2 Risiko Jaringan yang Relevan

Berdasarkan analisis, risiko jaringan yang terkait dengan serangan phishing meliputi beberapa kategori utama. Pada lapisan komunikasi, ancaman yang sering muncul mencakup man-in-the-middle attack, SSL stripping, dan session hijacking yang memungkinkan penyerang mencegat atau memanipulasi data selama proses transmisi. Pada layanan DNS dan web, serangan umum terdiri dari DNS spoofing, typosquatting, fake login page, serta HTTP fallback attack yang mengarahkan pengguna ke situs palsu untuk mencuri kredensial. Sementara itu, risiko berbasis server dan protokol meliputi penggunaan email gateway tanpa konfigurasi keamanan seperti SPF, DMARC, dan DKIM, kerentanan web server terhadap serangan XSS, serta kurangnya penerapan enkripsi end-to-end. Seluruh risiko tersebut konsisten dengan pola serangan yang dijelaskan dalam berbagai security advisory BSSN, khususnya yang berkaitan dengan phishing dan pencurian kredensial.

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 20 No 1]
[Januari 2026]

Tabel 1. Pemetaan Risiko Jaringan Terkait Serangan Phising

| Lapisan Jaringan | Jenis Risiko | Vektor Serangan | Dampak Potensial |
|---|---|---|---|
| Lapisan Komunikasi | Man-in-the-middle (MitM) | Intersepsi trafik jaringan, ARP spoofing, rogue access point | Kebocoran data sensitif, manipulasi konten, pengambilalihan sesi pengguna |
| Lapisan Komunikasi | SSL Stripping | Downgrade koneksi HTTPS ke HTTP | Transmisi kredensial tanpa enkripsi, hilangnya kerahasiaan data |
| Lapisan Komunikasi | Session Hijacking | Pencurian cookie sesi, kelemahan manajemen sesi | Pengambilalihan akun dan akses tidak sah |
| Layanan DNS & Web | DNS Spoofing | Manipulasi resolusi DNS | Pengalihan pengguna ke situs phishing |
| Layanan DNS & Web | Typosquatting | Domain mirip situs resmi | Penipuan pengguna dan pencurian kredensial |
| Layanan DNS & Web | Fake Login Page | Replikasi antarmuka situs asli | Pengumpulan username dan kata sandi |
| Layanan DNS & Web | HTTP Fallback Attack | Tidak diterapkannya HSTS | Akses ke situs tidak aman dan eksploitasi data |
| Server & Protokol | Email Spoofing | Tidak adanya SPF, DKIM, DMARC | Penyebaran email phishing yang sulit dideteksi |
| Server & Protokol | Cross-Site Scripting (XSS) | Validasi input yang lemah | Penyisipan skrip berbahaya, redireksi ke situs phishing |
| Server & Protokol | Kurangnya Enkripsi End-to-End | Konfigurasi keamanan yang tidak memadai | Kebocoran data selama transmisi |

3.3 Relevansi Ancaman dengan Kerangka BSSN

Berdasarkan PERKA BSSN, ancaman phishing memberikan dampak langsung terhadap keamanan Sistem Elektronik, terutama pada SE kategori tinggi yang mengelola data sensitif dan sangat bergantung pada integritas serta kerahasiaan informasi. Selain itu, phishing juga berpengaruh pada penerapan Tata Kelola Keamanan Informasi, khususnya pada aspek kontrol akses, manajemen risiko, dan peningkatan kesadaran keamanan di lingkungan pengguna. BSSN menegaskan bahwa upaya mitigasi phishing tidak hanya bergantung pada pengamanan teknis seperti penggunaan autentikasi berlapis dan enkripsi, tetapi juga sangat dipengaruhi oleh edukasi pengguna agar mampu mengenali modus penipuan dan tidak mudah terjebak dalam rekayasa sosial yang menjadi inti dari serangan phishing.

Tabel 2. Pemetaan Relevansi Ancaman Terkait Serangan Phising

| Aspek Kerangka BSSN | Area Pengamanan | Relevansi Ancaman Phishing | Implikasi terhadap Sistem Elektronik |
|---|---|---|---|
| Keamanan Sistem Elektronik | Kerahasiaan Informasi | Pencurian kredensial dan data sensitif | Kebocoran data dan pelanggaran privasi |

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 20 No 1]
[Januari 2026]

| Aspek Kerangka BSSN | Area Pengamanan | Relevansi Ancaman Phishing | Implikasi terhadap Sistem Elektronik |
|---|---|---|---|
| Keamanan Sistem Elektronik | Integritas Informasi | Manipulasi akun dan sesi pengguna | Perubahan data tanpa otorisasi |
| Keamanan Sistem Elektronik | Ketersediaan Layanan | Penyalahgunaan akun untuk serangan lanjutan | Gangguan operasional sistem |
| Tata Kelola Keamanan Informasi | Kontrol Akses | Autentikasi lemah dieksploitasi phishing | Akses tidak sah ke sistem |
| Tata Kelola Keamanan Informasi | Manajemen Risiko | Phishing sebagai risiko siber prioritas | Perlunya penilaian dan mitigasi berkelanjutan |
| Tata Kelola Keamanan Informasi | Kesadaran Keamanan | Pengguna sebagai target utama phishing | Kebutuhan pelatihan dan edukasi rutin |
| Faktor Manusia | Rekayasa Sosial | Eksploitasi kepercayaan pengguna | Meningkatnya probabilitas keberhasilan serangan |

### 3.4 Rekomendasi Mitigasi

Penelitian ini menunjukkan bahwa imbauan keamanan BSSN tentang phishing dan pencurian kredensial memuat pola ancaman yang berhubungan erat dengan kelemahan pada jaringan komputer, terutama pada lapisan komunikasi, DNS, dan autentikasi. Serangan phishing semakin canggih dan memanfaatkan kombinasi rekayasa sosial dengan teknik teknis seperti MITM, DNS spoofing, dan SSL stripping. Berdasarkan kerangka BSSN, ancaman ini dapat memengaruhi keamanan sistem elektronik, terutama yang mengelola data sensitif. Implementasi pengamanan berlapis, penguatan protokol jaringan, serta edukasi pengguna merupakan langkah mitigasi yang direkomendasikan.

Tabel 3. Pemetaan Rekomendasi Mitigasi terhadap Risiko Jaringan Phishing

| Lapisan Jaringan | Risiko Utama | Rekomendasi Mitigasi | Tujuan Mitigasi |
|---|---|---|---|
| Lapisan Komunikasi | MitM, SSL Stripping | TLS terbaru, HSTS, enkripsi end-to-end | Menjaga kerahasiaan dan integritas data |
| Lapisan Komunikasi | Session Hijacking | Secure cookie, HttpOnly, IDS/IPS | Mencegah pengambilalihan sesi |
| DNS & Web | DNS Spoofing | DNSSEC, validasi resolusi DNS | Menjamin keaslian domain tujuan |
| DNS & Web | Fake Login Page | WAF, certificate pinning | Mencegah pengalihan ke situs palsu |
| Server & Email | Email Spoofing | SPF, DKIM, DMARC | Mengurangi penyebaran email phishing |
| Autentikasi | Pencurian Kredensial | MFA, kebijakan kata sandi kuat | Mengurangi dampak kebocoran kredensial |
| Faktor Manusia | Rekayasa Sosial | Edukasi pengguna, simulasi phishing | Meningkatkan kesada |

## 4 Kesimpulan

Penelitian ini menunjukkan bahwa imbauan keamanan BSSN tentang phishing dan pencurian kredensial memuat pola ancaman yang berhubungan erat dengan kelemahan pada jaringan komputer,

terutama pada lapisan komunikasi, DNS, dan autentikasi. Serangan phishing semakin canggih dan memanfaatkan kombinasi rekayasa sosial dengan teknik teknis seperti MITM, DNS spoofing, dan SSL stripping. Berdasarkan kerangka BSSN, ancaman ini dapat memengaruhi keamanan sistem elektronik, terutama yang mengelola data sensitif. Implementasi pengamanan berlapis, penguatan protokol jaringan, serta edukasi pengguna merupakan langkah mitigasi yang direkomendasikan.

**Daftar Pustaka**

[1] R. Yudhiyati, A. Putritama, and D. Rahmawati, "What small businesses in developing country [1] Y. S. Nugroho et al., "Think of cybersecurity risks in the digital age: Indonesian case," J. Information, Communication & Ethics in Society, vol. 19, no. 4, pp. 446–462, 2021, doi: 10.1108/JICES-03-2021-0035.

[2] J. Aljabri et al., "Hybrid stacked autoencoder with dwarf mongoose optimization for phishing attack detection in internet of things environment," Alexandria Engineering Journal, vol. 106, pp. 164–171, 2024, doi: 10.1016/j.aej.2024.06.070.

[3] P. López-Aguilar, "Phishing vulnerability and personality traits: Insights from a systematic review," Computers in Human Behavior Reports, vol. 20, p. 100784, 2025, doi: 10.1016/j.chbr.2025.100784.

[4] C. K. Kotabaru, "Waspada smishing baru: Modus penipuan tol elektronik," 2025.

[5] J. Selatan, "Lanskap keamanan siber Indonesia 2024," no. 70, 2024.

[6] L. Tang and Q. H. Mahmoud, "A survey of machine learning-based solutions for phishing website detection," pp. 672–694, 2021.

[7] B. Naqvi et al., "Mitigation strategies against phishing attacks: A systematic literature review," Computers & Security, vol. 132, p. 103387, 2023, doi: 10.1016/j.cose.2023.103387.

[8] Badan Siber dan Sandi Negara, "Peraturan BSSN tentang pengamanan sistem elektronik," 2021.

[9] Badan Siber dan Sandi Negara, "Strategi Keamanan Siber Nasional," Jakarta: BSSN, 2020.

[10] Badan Siber dan Sandi Negara, "Indeks Keamanan Informasi (Indeks KAMI)," Jakarta: BSSN, 2022.

[11] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," NIST CSF, 2018.

[12] National Institute of Standards and Technology, "Digital Identity Guidelines," NIST SP 800-63, 2017.

[13] International Organization for Standardization, "ISO/IEC 27001: Information Security Management Systems," Geneva: ISO, 2022.

[14] A. Herzberg and A. Gbara, "Security and identification indicators for browsers against spoofing and phishing attacks," ACM Transactions on Internet Technology, vol. 8, no. 4, 2008.

[15] M. Jakobsson and S. Myers, Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft, Hoboken, NJ: Wiley, 2007.think of cybersecurity risks in the digital age: Indonesian case," *J. Information, Commun. Ethics Soc.*, vol. 19, no. 4, pp. 446–462, 2021, doi: 10.1108/JICES-03-2021-0035.