Journal of
Modern Medical Information Science

Summer 2025. Vol 11. Issue 2

# Letter to Editor

## Cybersecurity models for preventing attacks on health information systems

⁎ **Ameneh Marzban**[1]

1. Department of Health in Disasters and Emergencies, School of Health Management and Information Sciences, Iran University of Medical Sciences, Tehran, Iran.

Use your device to scan and read the article online

**Citation:** Marzban A. Cybersecurity models for preventing attacks on health information systems. Journal of Modern Medical Information Science. 2025; 11(2):125-130. [In Persian]

10.48312/jmis.11.2.965.1

**Article Info:**
Received: 30 Mar 2025
Accepted: 15 Sep 2025
Available Online: 20 Sep 2025

**Key Words:**
Cybersecurity, Cyberattacks, Health Information Systems, Prevention Models, Patient Data.

## Dear Editor

In the digital age, health information systems are considered one of the critical infrastructures for delivering healthcare services and preserving patient data [1]. However, the growing number of cyberattacks on these systems poses a serious threat to information security and patient privacy. Failure to implement appropriate countermeasures can lead to the exposure of sensitive patient data, disruption of healthcare services, and significant financial losses for healthcare institutions [2]. This letter not only reviews real-world cyberattacks but also provides a comparative analysis of major cybersecurity prevention models, with particular attention to their practical applicability in developing countries such as Iran.

Real-World Examples of Cyberattacks in Healthcare Systems

According to security reports, ransomware attacks, breaches of patient databases, and phishing campaigns have caused substantial damage to healthcare centers in recent years:

Ransomware Attack on Hospital Systems: In 2017, the WannaCry cyberattack caused widespread disruption across the UK's National Health Service (NHS), preventing doctors from accessing patient records and resulting in the cancellation of thousands of appointments [3].

Patient Database Breach in the U.S.: In 2021, hackers accessed the data of over 3.5 million patients at a major healthcare center, leaking sensitive information including medical records and financial data [2].

Phishing Attacks on Healthcare Institutions: In recent years, phishing campaigns targeting healthcare staff have led to the exposure of critical patient information and the infiltration of malware into medical networks [4].

*** Corresponding Author:**
Ameneh Marzban
Address: Iran University of Medical Sciences, Tehran, Iran.
E-mail: amenemarzban@yahoo.com

These examples demonstrate that neglecting cybersecurity can have severe consequences for the healthcare sector. Therefore, evaluating prevention models is essential.

Comparison of Cyberattack Prevention Models

To reduce the vulnerability of health information systems, the following models are recommended:

Implementation of Multi-Layered Security Systems: Utilizing smart firewalls, data encryption, and intrusion detection systems (IDS) helps identify and prevent attacks. However, their high implementation and maintenance costs, along with infrastructure requirements, may limit their feasibility in many developing healthcare systems [5].

In contrast, staff training and awareness programs aim to reduce human error by educating employees about phishing attacks and secure behaviors. Compared with purely technical solutions, this model is more cost-effective and highly feasible in developing countries, including Iran, where financial and technical resources may be limited [6].

Active monitoring using artificial intelligence and machine learning algorithms enables real-time detection and rapid response to cyberattacks. Although highly effective in large and well-resourced healthcare organizations, the need for advanced technical expertise and investment restricts its immediate applicability in low-resource settings [2].

Regular data backup and secure storage represent one of the most fundamental yet effective prevention strategies, particularly in mitigating the impact of ransomware attacks. Due to its relatively low cost and ease of implementation, this model is among the most practical options for healthcare institutions in developing countries [4].

Finally, penetration testing and periodic security assessments help identify system vulnerabilities before they can be exploited by attackers. When implemented selectively and periodically, this approach can effectively bridge technical and managerial perspectives on cybersecurity [6].

Implementation Challenges and Improvement Strategies

Challenges:

High Costs: Implementing advanced security systems requires significant investment in modern technologies [3]. Lack of Cybersecurity Expertise: Many healthcare centers lack specialized cybersecurity teams, increasing their vulnerability [1]. Resistance to Change: Some organizations resist structural changes and updates to security systems [2].

Improvement Strategies:

Investing in Human Resource Development: Providing specialized training to enhance cybersecurity knowledge among healthcare personnel [1].

Adopting Cost-Effective Technologies: Developing more economical solutions to protect data and reduce expenses [2].

Promoting a Culture of Cybersecurity: Raising awareness and encouraging acceptance of changes among staff and healthcare administrators [4].

Cybersecurity in health information systems is no longer merely a technical concern but a strategic priority for healthcare system resilience. Real-world cyberattacks highlight the severity of these threats and the urgent need for action.

Hospital administrators in developing countries are strongly encouraged to prioritize low-cost, high-impact interventions- such as continuous staff training, regular data backup, and baseline multi-layered security measures.

At the policy level, the development of national cybersecurity guidelines tailored to resource-limited settings, along with support for future research on the cost-effectiveness of hybrid prevention models, is recommended to enhance the sustainability and resilience of healthcare systems.

# نامه به سردبیر

## مدل‌های پیشگیری از حملات سایبری در سیستم‌های اطلاعاتی سلامت

* آمنه مرزبان[۱]

۱. گروه سلامت در بلایا و فوریت‌ها، دانشکده مدیریت و اطلاع‌رسانی پزشکی، دانشگاه علوم پزشکی ایران، تهران، ایران.

Use your device to scan and read the article online

**Citation:** Marzban A. Cybersecurity models for preventing attacks on health information systems. Journal of Modern Medical Information Science. 2025; 11(2):125-130. [In Persian]

doi 10.48312/jmis.11.2.965.1

اطلاعات مقاله :

تاریخ دریافت: ۱۱ فروردین ۱۴۰۴

تاریخ پذیرش: ۲۵ شهریور ۱۴۰۴

تاریخ انتشار: ۳۰ شهریور ۱۴۰۴

کلیدواژه‌ها :

امنیت سایبری، حملات سایبری، سیستم اطلاعات سلامت، مدل‌های پیشگیری، داده‌های بیماران.

### سردبیر محترم

در عصر دیجیتال، سیستم‌های اطلاعات سلامت به‌عنوان یکی از زیرساخت‌های حیاتی در ارائه خدمات درمانی و حفظ داده‌های بیماران شناخته می‌شوند [۱]. بااین‌حال، افزایش روزافزون حملات سایبری به این سیستم‌ها تهدیدی جدی برای امنیت اطلاعات، حریم خصوصی بیماران و تداوم ارائه خدمات سلامت ایجاد کرده است، عدم اتخاذ تدابیر پیشگیرانه مناسب می‌تواند منجر به افشای اطلاعات حساس بیماران، اختلال در فرآیندهای درمانی و تحمیل زیان‌های مالی قابل‌توجه به مؤسسات بهداشتی و درمانی شود [۲]. این نامه با اشاره به نمونه‌هایی از حملات سایبری واقعی و با تمرکز تحلیلی بر مقایسه مدل‌های پیشگیری، تلاش می‌کند راهکارهایی عملی برای کاهش آسیب‌پذیری سیستم‌های اطلاعات سلامت، به‌ویژه در کشورهای درحال‌توسعه مانند ایران، ارائه دهد. نمونه‌هایی از حملات سایبری واقعی در سیستم‌های سلامت به شرح ذیل است:

بر اساس گزارش‌های امنیتی، حملات باج افزاری، نفوذ به پایگاه داده‌های بیماران و حملات Phishing ازجمله حملاتی هستند که طی سال‌های اخیر خسارات بزرگی به مراکز درمانی وارد کرده‌اند.

حمله باج افزاری به سیستم‌های بیمارستانی: در سال ۲۰۱۷، حمله سایبری WannaCry موجب اختلال گسترده در سیستم‌های بهداشتی بریتانیا شد، دسترسی پزشکان به پرونده‌های بیماران را مختل کرد و منجر به لغو هزاران نوبت درمانی شد [۳].

*نویسنده مسئول:
دکتر آمنه مرزبان
نشانی: دانشگاه علوم پزشکی ایران، تهران، ایران.
پست الکترونیک: amenemarzban@yahoo.com

نفوذ به پایگاه داده بیماران در آمریکا: در سال ۲۰۲۱، هکرها به اطلاعات بیش از ۳/۵ میلیون بیمار در یک مرکز درمانی بزرگ دسترسی پیدا کردند و داده‌های حساس شامل سوابق پزشکی و اطلاعات مالی را منتشر کردند [۲].

حملات Phishing در مؤسسات بهداشتی: طی سال‌های اخیر، حملات Phishing که کارکنان درمانی را هدف قرار داده‌اند، منجر به افشای اطلاعات حیاتی بیماران و ورود بدافزارها به شبکه‌های درمانی شده‌اند [۴].

این نمونه‌ها نشان می‌دهند که عدم توجه به امنیت سایبری می‌تواند خسارات جدی برای بخش سلامت به همراه داشته باشد، ازاین‌رو، بررسی مدل‌های پیشگیری ضرورت دارد.

برای کاهش آسیب‌پذیری سیستم‌های اطلاعات سلامت، مدل‌های مختلفی پیشنهادشده‌اند که هرکدام مزایا و محدودیت‌های خاص خود رادارند.

پیاده‌سازی سیستم‌های چندلایه امنیتی: استفاده از فایروال‌های هوشمند، رمزنگاری داده‌ها و سیستم‌های تشخیص نفوذ به شناسایی و جلوگیری از حملات کمک می‌کند، بااین‌حال، هزینه‌های بالا و نیاز به زیرساخت پیشرفته، اجرای کامل این مدل را در بسیاری از کشورهای درحال‌توسعه با چالش مواجه می‌سازد [۵]. در مقابل، آموزش کارکنان و کاهش خطاهای انسانی از طریق دوره‌های آموزشی هدفمند، رویکردی کم‌هزینه‌تر و درعین‌حال مؤثر در مقابله با حملات Phishing و مهندسی اجتماعی محسوب می‌شود، این مدل به دلیل اتکای کمتر به فناوری‌های پیچیده، برای کشورهایی مانند ایران عملی‌تر و قابل‌اجراتر است [۶].

مدل پایش فعال با استفاده از هوش مصنوعی و الگوریتم‌های یادگیری ماشین، امکان شناسایی حملات در لحظه وقوع را فراهم می‌کند، اگرچه این رویکرد در مراکز درمانی بزرگ بسیار کارآمد است، اما نیاز به تخصص فنی بالا و منابع مالی قابل‌توجه، کاربرد آن را در محیط‌های کم منبع محدود می‌کند[۲].

تهیه نسخه‌های پشتیبان منظم و ذخیره امن اطلاعات، یکی از پایه‌ای‌ترین و درعین‌حال مؤثرترین مدل‌های پیشگیری است که نقش مهمی در بازیابی اطلاعات پس از حملات باج افزاری ایفا می‌کند، این مدل به دلیل هزینه نسبتاً پایین، یکی از مناسب‌ترین گزینه‌ها برای مراکز درمانی در کشورهای درحال‌توسعه به شمار می‌رود [۴].

درنهایت، انجام تست‌های نفوذ و ارزیابی‌های امنیتی دوره‌ای، با شناسایی آسیب‌پذیری‌ها پیش از سوءاستفاده مهاجمان، به افزایش تاب‌آوری سیستم‌ها کمک می‌کند، اجرای هدفمند و دوره‌ای این مدل می‌تواند پیوند مؤثری میان رویکردهای فنی و مدیریتی ایجاد کند [۶].

برخی چالش‌های پیاده‌سازی مدل‌های پیشگیری به شرح ذیل است:

هزینه‌های بالا: اجرای سیستم‌های امنیتی پیشرفته نیازمند سرمایه‌گذاری قابل‌توجه در فناوری‌های نوین است [۳].

کمبود تخصص در امنیت سایبری: بسیاری از مراکز درمانی فاقد تیم‌های تخصصی امنیت سایبری هستند که موجب افزایش آسیب‌پذیری آن‌ها می‌شود [۱].

مقاومت در برابر تغییرات: برخی سازمان‌ها در برابر تغییرات ساختاری و به‌روزرسانی سیستم‌های امنیتی مقاومت نشان می‌دهند [۲].

راهکارهای بهبود چالش‌های ذکرشده به شرح ذیل است:

سرمایه‌گذاری در توسعه منابع انسانی: آموزش تخصصی نیروی کار برای افزایش دانش امنیت سایبری در سیستم‌های سلامت [۱].

به‌کارگیری فنّاوری‌های ارزان‌تر و کارآمدتر: توسعه راهکارهای اقتصادی‌تر برای حفاظت از داده‌ها و کاهش هزینه‌ها [۲].

ترویج فرهنگ امنیت سایبری: افزایش آگاهی و پذیرش

تغییرات در میان کارکنان و مدیران مؤسسات بهداشتی [۴].

امنیت سایبری در سیستم‌های اطلاعات سلامت نه‌تنها یک ضرورت فنی، بلکه یک اولویت راهبردی برای پایداری نظام سلامت است. شواهد حاصل از حملات سایبری واقعی نشان می‌دهد که تهدیدات این حوزه جدی و رو به افزایش هستند. توصیه می‌شود مدیران بیمارستانی، به‌ویژه در کشورهای درحال‌توسعه، بر اجرای مدل‌های کم‌هزینه و پربازده مانند آموزش مستمر کارکنان، پشتیبان منظم از داده‌ها و حداقل الزامات امنیت چندلایه تمرکز کنند. در سطح کلان، تدوین دستورالعمل‌های ملی متناسب با محدودیت‌های منابع و حمایت از پژوهش‌های آینده در زمینه ارزیابی اثربخشی اقتصادی مدل‌های ترکیبی امنیت سایبری می‌تواند نقش مهمی در ارتقای تاب‌آوری مراکز درمانی ایفا کند.

## ملاحظات اخلاقی:

### مشارکت نویسندگان

همه نویسندگان به‌طور مساوی در این تحقیق مشارکت داشته‌اند.

### تعارض منافع

هیچ گونه تضاد منافعی از سوی نویسندگان گزارش نشده است.

### تشکر و قدردانی

از معاونت تحقیقات و فناوری دانشگاه علوم پزشکی ایران به خاطر فراهم کردن امکان دسترسی به پایگاه‌های اطلاعاتی علمی، سپاسگزارم.

## References

1. Al-Qarni EA. Cybersecurity in healthcare: A review of recent attacks and mitigation strategies. IJACSA. 2023; 14(5):135-140. DOI: 10.14569/IJACSA.2023.0140513
2. Angel D. Protection of medical information systems against cyber attacks: A graph theoretical approach. Wirel Pers Commun. 2022; 126(4):3455-64. DOI: 10.1007/s11277-022-09873-x PMID: 35756173
3. Kilincer IF, Ertam F, Sengur A, Tan RS, Acharya UR. Automated detection of cybersecurity attacks in healthcare systems with recursive feature elimination and multilayer perceptron optimization. Biocybern Biomed Eng. 2023; 43(1):30-41. DOI: 10.1016/j.bbe.2022.11.005
4. Patel AU, Williams CL, Hart SN, Garcia CA, Durant TJS, Cornish TC, et al. Cybersecurity and information assurance for the clinical laboratory. J Appl Lab Med. 2023; 8(1):145-61. DOI: 10.1093/jalm/jfac119 PMID: 36610432
5. Rahim MJ, Rahim MI, Afroz A, Akinola O. Cybersecurity threats in healthcare it: Challenges, risks, and mitigation strategies. JAIGS ISSN: 3006-4023. 2024; 6(1):438-62. Link
6. Soni P, Pradhan J, Pal AK, Islam SH. Cybersecurity attack-resilience authentication mechanism for intelligent healthcare system. IEEE Transactions on Industrial Informatics. 2022; 19(1):830-40. DOI: 10.1109/TII.2022.3179429