Top 10 Healthcare Cybersecurity Tips

Using Digital Identity to Detect Cybercriminals

LexisNexis® RISK SOLUTIONS | Healthcare

Why Digital Identity Intelligence Matters for Healthcare Cybersecurity

Healthcare organizations are increasingly reliant on digital channels to support patient access, engagement and self-service. Your patients expect convenient digital experiences, from portal logins and online scheduling to digital registration and account management. As those digital touchpoints grow, so do the opportunities for cybercriminals to target sensitive information and exploit weaknesses.

In 2025, more than 139 million individuals were impacted by a healthcare data breach.[1] A LexisNexis® Risk Solutions healthcare industry analysis also identified more than **13.8 million healthcare interactions associated with confirmed fraud elsewhere in the Digital Identity Network**, highlighting the challenge of evaluating trust decisions using healthcare data alone.[2]

As digital engagement continues to expand, you face increasing pressure to balance security, a positive patient experience and operational efficiency. At the same time, determining whether a digital interaction should be trusted is becoming more challenging, particularly when important context may exist beyond the visibility of your own organization.

Emerging threats are contributing to this challenge. Deepfakes, synthetic identities, credential stuffing attacks and AI-enabled fraud techniques are making it more difficult to distinguish trusted users from bad actors. Many of these threats are designed to appear legitimate, increasing the need for a more contextual approach to evaluating risk.

For hospitals and hospital systems the challenge is balancing security with patient experience. you need to identify risk early while ensuring patients can access digital services without unnecessary barriers.Relying too heavily on static authentication requirements can create friction, reduce engagement and increase support costs without effectively stopping modern threats.

A stronger approach focuses on digital identity. By evaluating activity in context and comparing it to broader patterns, you can make more informed trust decisions, better distinguish trusted users from potential attackers and help protect access to sensitive health information.

Use the following strategies to detect bots, prevent identity fraud and reduce risk with digital identity intelligence.

TIP 1

Apply Real-Time Risk Scoring with Digital Identity Intelligence

Healthcare digital access points are high-value targets. Patient portals, online registration tools and account recovery workflows can all be targeted by attackers using stolen credentials, automation and other techniques that imitate legitimate patients.

A risk-based approach evaluates activity in real time and assigns a risk score to each interaction. This helps you distinguish between activity that appears consistent with trusted patients and activity that may warrant additional scrutiny.

When risk scoring is applied effectively:

- Trusted patients can move through digital experiences with minimal interruption.
- Potentially risky activity can be identified earlier.
- Security and fraud teams can focus attention on the interactions that matter most.

KEY ACTION:

Adopt a risk-based approach that evaluates each interaction in context.

Additional insight into identity, device and network signals can help you identify potentially risky activity, focus investigative resources and make more informed trust decisions.

TIP 2

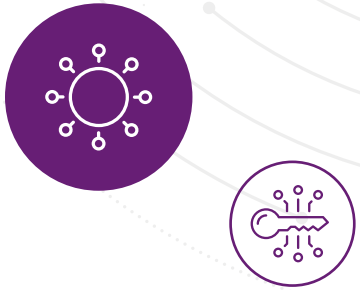
Unify Security Signals With Digital Identity

Many healthcare organizations rely on multiple tools that operate independently. As a result, you may not have a complete view of risk across devices, users and environments.

Attackers take advantage of these gaps. Activity that appears low risk in one system may look very different when viewed alongside signals from other systems.

A unified identity intelligence approach provides better visibility by connecting signals across:

- Devices
- Networks
- Digital interactions
- Known threat activity



KEY ACTION:

Integrate digital identity, device and threat intelligence into a unified view.

This can help you improve detection accuracy, reduce operational complexity and respond to threats faster.

TIP 3

Recognize Trusted Patients Faster

Security measures often create friction for the wrong users. Legitimate users are asked to reauthenticate again and again, while attackers using stolen credentials may initially appear valid.

Improving recognition of trusted users helps you reduce unnecessary friction and supports stronger engagement.

Industry research shows digital trust plays a significant role in user behavior. Consumer concerns about identity theft and stolen payment data remain high, increasing pressure on you to build trust while protecting digital interactions.[3]

KEY ACTION:

Focus on consistently recognizing returning users based on consistent patterns of activity.

This helps you create smoother digital experiences for your patients while maintaining strong protection against impersonation, account takeover and identity fraud.

TIP 4

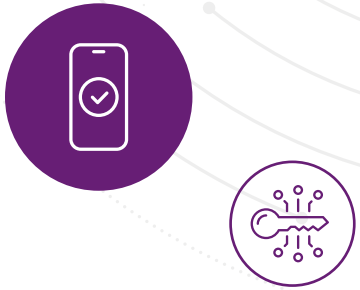
Strengthen Trust with Device Intelligence

Every interaction leaves behind a digital footprint. Devices, browsers and network attributes provide important signals that help determine whether activity is consistent with a known user.

Device intelligence can identify:

- Previously seen or trusted devices
- Suspicious configurations or anomalies
- Devices linked to known fraudulent activity
- Inconsistencies between device, location and account activity

When evaluated in context, these signals can help you detect risk while minimizing unnecessary friction for trusted users



KEY ACTION:

Use device intelligence as an early layer of defense.

Combine it with broader digital identity intelligence to help you identify inconsistencies that may indicate potential identity fraud, account takeover or unauthorized access.

TIP 5

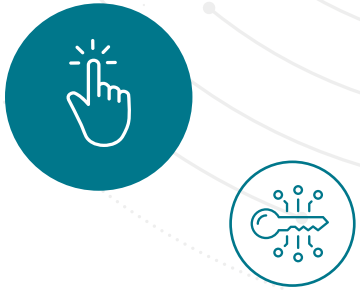
Leverage Behavioral Intelligence as Part of a Broader Trust Strategy

Behavioral patterns can help your healthcare organization understand whether digital activity appears consistent or unusual. This may include timing, frequency, navigation patterns, session activity or changes in how a user interacts with an account.

Behavioral indicators can provide useful context when evaluating digital interactions. While no single signal tells the whole story, patterns that appear unusual may become more meaningful when evaluated alongside device, network and digital identity intelligence.

When behavioral indicators are evaluated in context, you can:

- Gain additional insight into digital interactions.
- Identify potentially suspicious activity may be identified earlier.
- Make more informed trust decisions using a broader set of signals.



KEY ACTION:

Use behavioral indicators as part of your broader digital identity intelligence.

Evaluate behavior alongside device, network and identity intelligence to help you identify potentially suspicious activity earlier and make more informed trust decisions.

TIP 6

Detect Malware Loaders and Hidden Threat Activity

Cybercriminals continue to use malware to gain access to systems, control sessions and collect sensitive information. Loader malware plays a critical role in these attacks by delivering additional payloads such as ransomware, backdoors or data theft tools.

Recent threat research shows loader malware continues to evolve. Zscaler ThreatLabz identified TransferLoader in 2025 and reported that it had been used to deliver Morpheus ransomware. The malware includes downloader, backdoor and loader components and uses anti-analysis techniques to evade detection.[4]

These threats can be difficult for you to detect. They may operate silently in the background while attackers move deeper into a session or environment, increasing the risk of unauthorized access, fraud or other malicious activity.

KEY ACTION:

Use tools that can detect indicators of compromise across your devices, sessions and networks.

Look for suspicious execution patterns, abnormal behavior, session inconsistencies and connections to known threat infrastructure.

Prioritize malware detection techniques that operate in the background and do not depend on users to recognize or report malicious activity.

TIP 7

Move Beyond Signature-Based Detection

Signature-based defenses remain useful, but they are not enough on their own. Attackers constantly modify malware, rotate infrastructure and adapt tactics to avoid known detection patterns.

This is especially important as AI-enabled attacks become more dynamic. A threat may not match a known signature, but it can still show abnormal behavior. A session may begin normally, then shift in ways that suggest automation, manipulation or compromise.

Static checks are limited because they confirm what is already known. To identify evolving threats, you need additional risk signals that can help detect suspicious behavior, unusual patterns or unexpected changes as they occur.

KEY ACTION:

Use behavioral analysis and advanced page fingerprinting to distinguish between trusted activity, automation and signs of compromise.

Rather than relying only on known signatures, evaluate whether activity fits the expected profile of a trusted digital interaction.

TIP 8

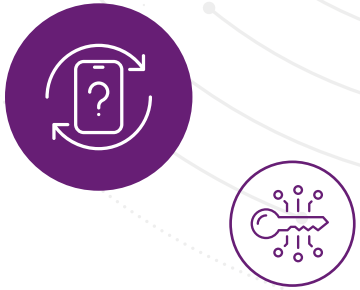
Identify Risky Devices, Suspicious Infrastructure and Automated Activity

Bot attacks continue to grow across the digital ecosystem. According to the LexisNexis® Risk Solutions "Evolving Threats Beneath the Surface,"[5] automated bot attacks increased by **59% in 2025** as attackers increasingly relied on automation and more sophisticated techniques.

Automated attacks are not limited to account takeover and credential abuse. The same ecosystem of malicious infrastructure is often associated with broader threats, including attempts to disrupt digital services through distributed denial-of-service (DDoS) attacks. For healthcare organizations, disruptions to patient portals, scheduling systems and other digital access channels can affect both operations and patient experience.

Bot activity can take several forms. Some attacks are fast and high volume. Others are low and slow, designed to stay below traditional detection thresholds. Attackers may use botnets, proxies, compromised devices or rotating IP addresses to test credentials, create accounts or take over existing accounts.

Risky devices and IP addresses become more meaningful when they are evaluated across a broader intelligence network. A device that appears new to one organization may have a history elsewhere. An IP address may be linked to suspicious behavior across multiple environments, giving you additional context to make more informed trust decisions.



KEY ACTION:

Monitor for risky devices and IP addresses which have been involved in attacking other websites, or which are accessing multiple accounts from the same device.

Leverage shared digital identity intelligence to help you identify infrastructure, devices and behaviors that may already be associated with risk elsewhere. Broader visibility can help you identify coordinated activity sooner and support more informed trust decisions.

TIP 9

Identify Spoofed Devices and Hidden Locations

Cybercriminals often try to hide who they are and where they are operating from. They may use proxies, VPNs, emulators, device spoofing or other techniques to disguise their true environment.

Legitimate users may use privacy tools, too. That means the presence of a proxy or location mismatch should not automatically determine risk. The key is context.

A hidden location becomes more concerning when paired with indicators such as unusual velocity, unfamiliar devices, recent credential changes or access attempts across multiple accounts. Looking at these signals in context can help you make more informed trust decisions and focus attention on the interactions that warrant additional scrutiny.

KEY ACTION:

Evaluate suspicious configurations as part of a broader risk profile.

Look for inconsistencies between device, network, location and known account activity. When multiple indicators point to elevated risk, apply additional controls.

TIP 10

Use Shared Digital Identity Intelligence

Fraudsters do not operate in isolation. They reuse credentials, devices, phone numbers, email addresses, infrastructure and attack methods across organizations and industries.

That makes shared intelligence essential. A signal that looks new inside one organization may be part of a broader pattern already seen elsewhere. A global digital identity network can help reveal connections between activity, devices, identities and known threat behavior.

Credential stuffing attacks often appear as a series of routine login attempts. Viewed individually, they may not trigger concern. Viewed collectively, they can reveal a coordinated effort to test stolen credentials across multiple accounts and digital services. Access to broader intelligence can help you identify these patterns earlier and make more informed trust decisions.

KEY ACTION:

Move beyond organization-specific visibility by incorporating digital identity intelligence derived from a broader network of digital interactions.

Insights from billions of analyzed transactions can help you identify patterns, devices, identities and behaviors that may not be apparent from internal data alone. A broader view of digital activity can improve risk assessment, strengthen fraud detection and support more informed trust decisions across account creation and account recovery interactions.

CONCLUSION:

Stop More Cybercriminals Without Slowing Trusted Users

Cybersecurity has become a digital identity challenge. Attackers are using automation, AI-enabled tools, malware and stolen credentials to appear legitimate. They move quickly. They adapt. And they exploit gaps between disconnected systems.

To keep pace, you need a smarter way to determine trust in real time.

Digital identity intelligence helps make that possible. By connecting device, network, behavioral and threat signals, you can identify risk earlier and respond with more precision. You can reduce unnecessary friction for trusted users while identifying suspicious activity that may require additional scrutiny, review or intervention.

LexisNexis® ThreatMetrix® helps organizations apply this approach across digital interactions. By using intelligence from the Digital Identity Network®, AI and machine learning, ThreatMetrix® supports real-time, risk-based decisions that help detect bots, identity fraud, account takeover and emerging cyber threats.

You do not have to choose between stronger security and a better user experience. With the right digital identity strategy, you can make more confident trust decisions, reduce fraud risk and help protect digital access for patients and other trusted users.

Ready to strengthen cybersecurity with digital identity intelligence?

Learn how ThreatMetrix can help you detect cybercriminals, reduce unnecessary friction and make more confident risk decisions in real time.

End Notes

1. The HIPAA Journal, “Largest Healthcare Data Breaches of 2025.” https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2025/
2. LexisNexis® Risk Solutions, Independent analysis of healthcare-specific data within the Digital Identity Network.
3. Digital Trust Institute, “A World Increasingly Dependent on Trust https://www.digitaltrust.institute/why-digital-trust-matters
4. Zscaler, “Technical Analysis of TransferLoader.” https://www.zscaler.com/blogs/security-research/technical-analysis-transferloader
5. LexisNexis® Risk Solutions, “Evolving Threats Beneath the Surface” report. https://risk.lexisnexis.com/-/media/files/financial%20services/research/lexisnexis-risk-solutions-cybercrime-report-2026.pdf

About LexisNexis® Risk Solutions

LexisNexis® Risk Solutions provides customers with information-based analytics and decision tools that combine public and industry-specific content with advanced technology and algorithms to assist them in evaluating and predicting risk and enhancing operational efficiency. Headquartered in metro Atlanta, Georgia, the company has offices throughout the world, serves customers in more than 190 countries and territories and is part of RELX. For more information, please visit LexisNexis Risk Solutions.

LexisNexis® RISK SOLUTIONS | Healthcare