MUTARE NEWS
SPECIAL REPORT

Online Article
https://www.mutare.com/healthcare-communications-in-crisis/

Healthcare: Communications in Crisis

Hospitals are battling malicious robocalls, voice spam & vishing

mutare

mutare

https://www.mutare.com/healthcare-communications-in-crisis/

Healthcare:
Communications in Crisis

Hospitals are battling malicious robocalls, voice spam & vishing

Healthcare Organizations are Uniquely Vulnerable

According to a Federal Communications Commission (FCC) report filed by the American Hospital Association (AHA), what makes robocalls to hospitals uniquely damaging "is the impact they can have on the public health and safety of patients and the community." Hospitals can fall victim to a variety of unlawful calling schemes, ranging from telephone denial-of-service, TDoS, attacks (often part of an extortion scheme where the perpetrator hijacks critical lines with a flood of simultaneous calls until their demands are met) to targeted social engineering vishing schemes (where the perpetrator uses available information about an employee and, through impersonation, tricks them into divulging protected information) to general disruptive robocall campaigns.

Table of Contents

Introduction

Every month, billions of robocalls are placed to American consumers, a substantial portion of which are unlawful. While voice spam and robocalls are an all-too familiar irritation for anyone with a phone, they are also exacting a significant financial toll on business in the form of lost productivity, reduced network performance and cybersecurity breaches.

This is especially painful for healthcare, an industry highly dependent on phone communications but whose phone networks have become an increasingly attractive target for criminal behavior, particularly as the stress of the COVID-19 pandemic is stretching staff and resources to the limit.

Robocall 'crackdown': F'TC blocks more than a billion illegal calls, but problem festers
https://www.usatoday.com/story/money/2019/06/25/ftc-robocall-crackdown/1548714001/

Officials Warn of Phone Scams Targeting Hospitals and Patients
https://therecord.media/officials-warn-of-phone-scams-targeting-hospitals-and-patients/

The Unique Vulnerability of Healthcare Organizations

According to a Federal Communications Commission (FCC) report filed by the American Hospital Association (AHA), what makes robocalls to hospitals uniquely damaging "is the impact they can have on the public health and safety of patients and the community." Hospitals can fall victim to a variety of unlawful calling schemes, ranging from telephone denial-of-service (TDoS) attacks (often part of an extortion scheme where the perpetrator hijacks critical lines with a flood of simultaneous calls until their demands are met) to targeted social engineering vishing schemes (where the perpetrator uses available information about an employee and, through impersonation, tricks them into divulging protected information) to general disruptive robocall campaigns.

These and other malicious calling activities "can disrupt hospitals' critical communications and render hospitals unable to place or receive telephone calls. They threaten patients' privacy, facilitate unauthorized access to prescription drugs, and divert hospital resources."

What's more, if a criminal intrusion results in the exposure of protected health information, the penalty is severe; The average fine for a single HIPAA breach is $1.5M

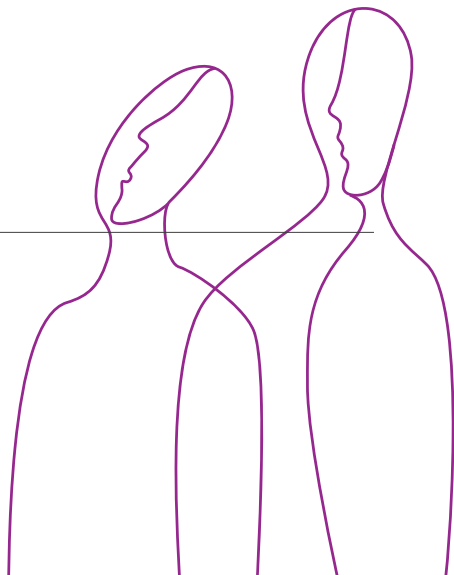
HOSPITAL ROBOCALL PROTECTION GROUP (HRPG)
https://www.aha.org/system/files/media/file/2020/12/hrpg-report-final.pdf

Is TRACED Act the Solution?

For this reason, in June of 2020 and at the direction of Congress, the FCC created the Hospital Robocall Protection Group (HRPG) to serve as a federal advisory committee in concert with the Telephone Robocall Abuse Criminal Enforcement and Deterrence Act of 2019 (TRACED Act). The HRPG's objective: "To serve as a resource to all stakeholders involved in preventing the receipt of unlawful robocalls by hospitals and patients and mitigating their effect."

When the TRACED Act was passed in 2019, it was seen as a step in the right direction to curb the rising tide of robocalls. While criminalizing rogue robocall activity, the Act also mandates that carriers implement an attestation protocol (STIR/SHAKEN) used to confirm the legitimacy of the call source. However, the TRACED Act is far from a perfect solution. It will be years before all carriers will have the infrastructure necessary to support STIR/SHAKEN; the attestation process simply tags suspicious calls but allows them to ring through; bad actors can still launch malicious call campaigns through unregulated overseas carriers; and the filtering process can be easily circumvented by those already committed to criminal intent. What's more, the Act focuses on carriers and was designed for consumer protection but has little to offer the enterprise networks that empower businesses.

In other words, businesses, and hospitals in particular, should not depend solely on government regulators to solve their robocall, vishing and voice spam problems.



TRACED Act, STIR/SHAKEN
Will Businesses See Benefits of Anti-Phone Spam Measures?
https://www.mutare.com/traced-act-stir-shaken/

Best Practices Defined

The HRPG recognizes this fact, stating, "Efforts by any single entity or group will not prevent robocalls to hospitals. Therefore, collective efforts and coordination between hospitals, government agencies, and voice service providers are critical to the success of unlawful robocall prevention and mitigation efforts."

On December 14, 2020, the HRPG presented a report to the FCC outlining Best Practices for voice service providers, hospitals, and federal and state governments to follow in order to prevent unlawful and damaging robocalls from disrupting hospital communications.

The 28-page document includes three advisory sections:

1. How Voice Service Providers Can Better Combat Unlawful Robocalls Made to Hospitals
2. How Hospitals Can Better Protect Themselves from Unlawful Robocalls
3. How the Federal and State Government Can Help Combat Unlawful Robocalls

A repeated theme is the call for additional, hospital-specific practices, systems and technologies that can be used to augment TRACED Act detection methods in the battle against unwanted robocalls.

Specifically, the report notes "Perimeter defense and network monitoring are critical strategies to protect hospital networks from unlawful robocalls. Not unlike security perimeter defense, tools exist to identify unlawful traffic and stop it before infiltrating the network."

Hospital Robocall Protection Group Issues Best Practices
https://www.fcc.gov/document/hospital-robocall-protection-group-issues-best-practices

The Do No Harm Solution to Robocall Eradication

One such tool, Mutare's Voice Spam Filter, stands out, offering a unique combination of features that provide one of the industry's most powerful voice spam, voice spoof and robocall detection and blocking systems combined with a "do no harm" construct that adds a second layer of vetting for suspect calls. Hospitals, wary of any system that might inadvertently block a legitimate patient call, would find the Mutare Voice Spam Filter a particularly reassuring fit.

Mutare's Voice Spam Filter integrates several methods to identify voice spam and robocalls before they enter the hospital's voice network, filtering them against a massive, continuously updated database of known illegitimate robocall perpetrators combined with organization-specific allow list and block list. IT administrators have access to a set of secure web tools used to control how the system handles known voice spam or suspect calls (Allow, Drop, Route to another phone, or Route to the included voice CAPTCHA system for additional screening). It also includes a Rules Manager tool which applies specific actions, as determined by the administrator, to numbers or partial numbers (such as allow any call from regional area codes, send to CAPTCHA any call with an overseas country code).

While calls with spoofed phone numbers may elude less sophisticated voice spam detection systems, Mutare's Voice Spam Filter also includes its own, unique voice spoof detection technology, built on a platform that combines advanced call pattern recognition, heuristics and machine learning to spot robocalls from suspect caller IDs. This feature is particularly effective in detecting and diverting auto-dialer "voice spam storms" before they overtake voice networks. It also addresses the HRPG recommendation to "analyze, identify, and monitor traffic on (voice) networks for patterns consistent with unlawful robocalls."

Not only does the Mutare Voice Spam Filter monitor all network filtering activity in real time; its robust reporting capabilities capture all identifying data related to the caller and called party along with filtering actions applied to each call, then delivers it in visual (Web) as well as downloadable (CSV) reports that satisfy regulatory requirements and support FCC case investigations.

Utilizing its Voice Spam Filter engine, Mutare offers a free voice traffic analysis (VTA) as well as a paid proof of concept trial to any organization wanting to better understand the make-up of its voice traffic, including what proportion of that traffic is actually unwanted spam and the level of savings that could be realized if those unwanted calls were eliminated.

According to Mutare's Chief Technology Officer, Roger Northrop, most company voice networks are experiencing an average of 12% unwanted call activity, "Though we have seen it as high as 80%," he says. Of the healthcare organizations analyzed, Mutare's VTA projected annual costs in lost productivity ranging from $74,000 to well over $2,400,000 depending on the size of the organization. "Add to that the potential damages when callers with criminal intent successfully sabotage voice channels or extract protected information from vulnerable employee targets, and the additional loss could be catastrophic," he says.

For healthcare, the threat of such intrusions is particularly concerning.

"I cannot imagine a more challenging year for our healthcare systems than 2020," says Chuck French, Mutare's Chief Growth Officer. "We are eternally grateful to the providers who are continuing to deal with the unprecedented stress of COVID-19 patient care. It's truly unconscionable that, at the same time, voice scam and robocall activity directed at hospitals is on the rise, further stressing resources and threatening staff and patient safety alike."

For more than 35 years, Mutare has been developing communications solutions that help customers solve real-world and often complex problems. "Dealing with unwanted voice traffic is a battle that will not be won without insight and tools that can continuously adapt to the ever-changing nature of the opponent," says French. "Our passion for helping organizations safely defeat the scourge of illegitimate spam and robocalls is the driving force behind our enterprise Voice Spam Filter solution. We are proud that so many organizations trust, and are benefiting from, our technology. But knowing that it is now providing much-needed relief and protection for our friends in the healthcare industry – that is especially gratifying."

For more information about Mutare's Voice Spam Filter and to register for a Voice Traffic Analysis, contact a Mutare representative or visit https://www.mutare.com/voice-spam-filter/

Learn More: Mutare Voice Spam Filter

https://www.mutare.com/voice-spam-filter/

TERMS & DEFINITIONS

Telephone Denial of Service attack (TDoS)
An intentional attack to disrupt telephone/voice service communications of an organization by flooding the network with multiple simultaneous calls. It may include a spoofed number, and also can be part of an extortion scheme where a call recipient is asked for money or information as ransom with the threat of such an attack.

Target social engineering calls
The goal is to gather sensitive, financial, or information technology (IT) information. The goal may also be to steal some bit of information to be used in a larger data attack. For instance, social engineering calls may seek information about the hospital organization, names and phone numbers of key personnel, email addresses, and information about computer systems, among other data. These calls are very difficult to detect and usually go unreported.

Voice Phishing, also known as vishing
Bad actors may use social engineering techniques to try to steal information and credentials from hospital workers in order to, for example, obtain prescription drugs fraudulently. Such attacks tend to be targeted—including sophisticated attacks targeting individual staff members—and rely on caller ID spoofing to hide the caller's identity in favor of impersonating a more trusted one.

General unlawful robocall campaigns
General unlawful robocall campaigns rely on automatic dialing to blast mass numbers of prerecorded scam calls to as many potential victims as possible. The calls, which frequently originate from outside the United States, often seek to defraud recipients by, for example, claiming to be from a government agency or legitimate business and suggest that the recipient must take some immediate action to avoid a financial penalty or to be eligible for a benefit. In addition to being fraudulent, such calls also very often violate various criminal laws governing calling parties, such as the federal Telephone Consumer Protection Act (TCPA) and the Truth in Caller ID Act, the Federal Trade Commission's (FTC) Telemarketing Sales Rule (TSR), and similar state laws. While general unlawful robocalls may not specifically target hospitals, they can tie up hospital lines and resources. In addition, patients and staff at hospitals, like any other recipient of the call, can fall victim of robocall scams.

Nuisance and disruptive robocalls
Some robocalls are placed to consumers who wish to receive them (medical appointment reminders, fraud alerts from banks, etc.). Many calls are also made to consumers attempting to sell some product, service, or information. With appropriate consent, as governed by relevant federal and state laws, such calls may not be unlawful, but they are very often unwanted. These calls can irritate patients and reduce hospital personnel productivity and can consume hospital voice system resources.

Healthcare:
Communications in Crisis
Hospitals are battling malicious robocalls, voice spam & vishing

MUTARE NEWS
SPECIAL REPORT

Online Article
https://www.mutare.com/healthcare-communications-in-crisis/

Headquarters
Mutare, Inc.
2325 Hicks Road
Rolling Meadows, Illinois 60008

Support
855.782.3890
help@mutare.com

Sales
847.496.9000
sales@mutare.com

https://www.mutare.com/