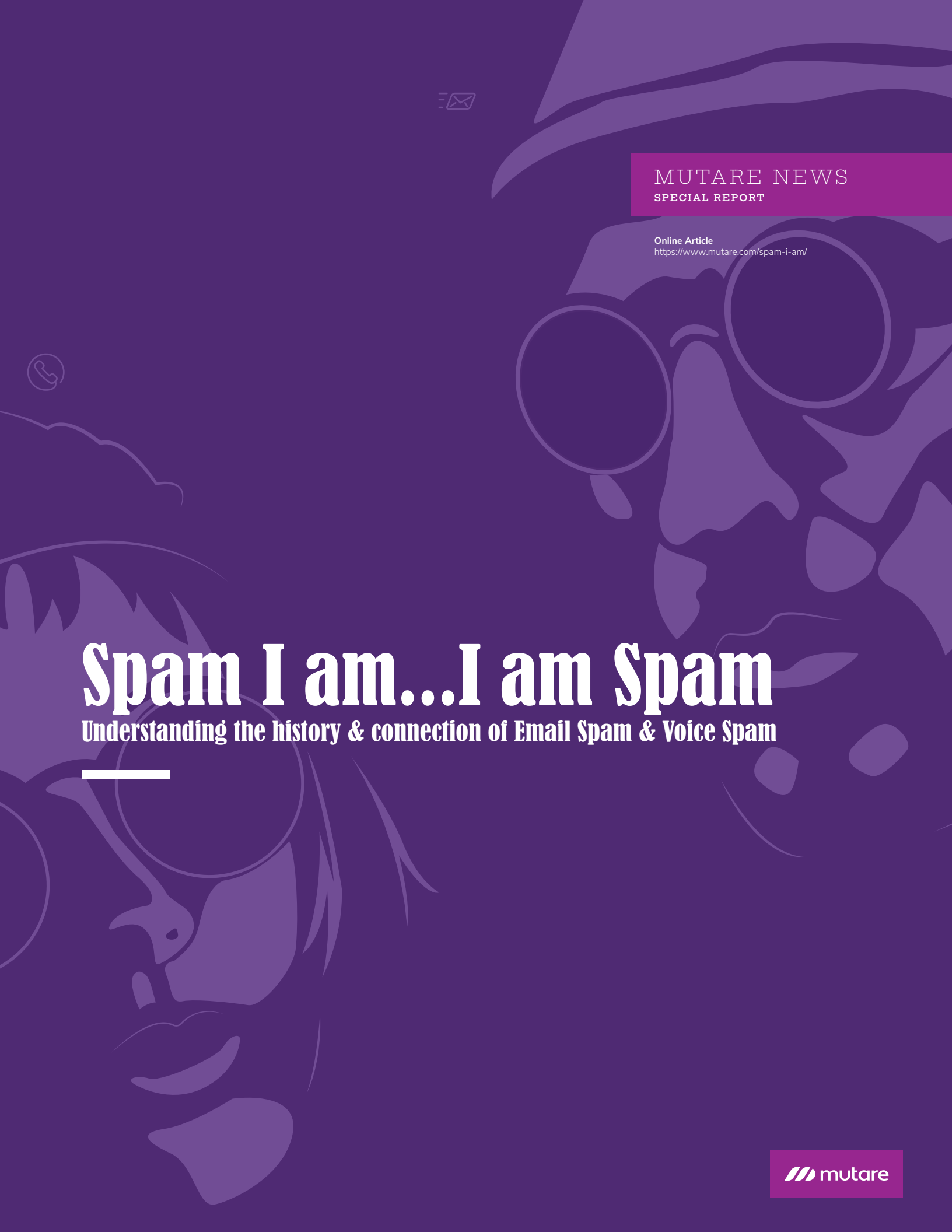


MUTARE NEWS

SPECIAL REPORT

Online Article
https://www.mutare.com/spam-i-am/

Spam I am...I am Spam

Understanding the history & connection of Email Spam & Voice Spam

mutare

mutare

https://www.mutare.com/spam-i-am/

Spam I am... I am Spam

Understanding the history & connection of Email Spam & Voice Spam

mutare.com

Executive Summary

The story of how digital junk mail came to be called “spam” is a quick tale of human foibles and pop culture colliding with technology-fueled opportunism. This article examines the roots of spam intrusion onto the “Information Superhighway,” starting with early, clumsy attempts at automated mass-marketing that laid the groundwork for today’s highly sophisticated bot operations. It also examines the process of, and reasons for, the apparent shift of digital spam and related scam activity from email to voice, due largely to the relative lack of adequate defense structures protecting voice networks but also fueled by the increased vulnerabilities of a decentralized, at-home workforce.

Company risk managers should take heed, note what organizations with specific expertise in enterprise voice networks are advising, and learn what measures they can take now to protect their networks and employees from the increasingly disruptive and dangerous intrusion of robocalls, vishers, and scammers.

Table of Contents

2 Executive Summary
3 Introduction
4 The First Digital Spam
5 Driving the Information Highway
6 From Spammers to Spitters
Why Voice Spam? It’s Cheap, Easy and Effective
7 Tip to Voice Spam Driven by Effectiveness
8 Targeting At-Home-Workforce Employees
9 Putting a Filter Between Spammers and Enterprise Networks

Introduction

First hitting the market in the late 30's, Hormel's iconic canned lunchmeat has been both beloved and maligned by generations of consumers. The name alone is enigmatic – possibly a contraction for Shoulder Pork and hAM or SPiced hAM, but also the acronym used by British troops when this Special Processed American Meat was served as rations during World War II.

How "spam" became a metaphor for junk mail is also a matter of debate but could very well have arisen from a single incident that later inspired, through the combination of mischief, computer geek humor and pop culture, the incarnation of "spam" as a favored term for digital abuse.

"Spam, spam, spam, spam, spam, Spam, spam, spam, spam. Lovely spam! Wonderful spam!"

--- 1970 "Spam" sketch from Monty Python's Flying Circus

Monty Python's Flying Circus: Spam, Spam, Spam...
https://www.dailymotion.com/video/x9fly1

Derivation of the SPAM Name
https://www.templetons.com/brad/spamterm.html

CREDIT: EVERETT COLLECTION

The First Digital Spam... those damn Marketing folks!

In 1978, Gary Thuerk, an enterprising marketer for one of the nation's leading manufacturers of computer equipment, Digital Equipment Corporation (DEC), recognized the potential for reaching a large, targeted audience using the Advanced Research Project Agency Network (ARPANET). As a precursor to today's Internet, the APRANET was created by the Department of Defense and used primarily by military/government officials, academics, and scientific researchers to share information between computers connected through phone lines. The platform included rudimentary email capabilities. As a new and fairly closed system, use of the ARPANET and its email component was loosely regulated through an unwritten code of "netiquette," trusted enough that users' online addresses were freely published in a directory for other subscribers to access.

With the help of an assistant, Thuerk constructed and sent a digital message promoting a series of new product open houses for his company, manually addressing it to all 400 West Coast APRANET subscribers. While the effort was well-intended, the execution, as well as the response, was not as hoped. Not only did the long list of addresses spill chaotically into the body of the email and obscure the message, but the effort was greeted by an immediate angry backlash from recipients and a rebuke from APRANET administrators for breaking appropriate use rules.

While this may go down as the first recorded incident of digital "spam," the term was not widely adopted until the early 90's following the capitalization of the Internet and its widespread use among consumers.

Online user groups were commonplace by then and often populated by self-described "computer geeks" who enjoyed interacting electronically but also testing the limits of the technology. When file upload capabilities were added to some chat platforms, users intent on mischief began flooding the system with long strings of repetitive data, one of the favorites being the words to the "spam" song from an iconic 1970 Monty Python sketch. The term stuck and was soon a permanent part of the IT lexicon.

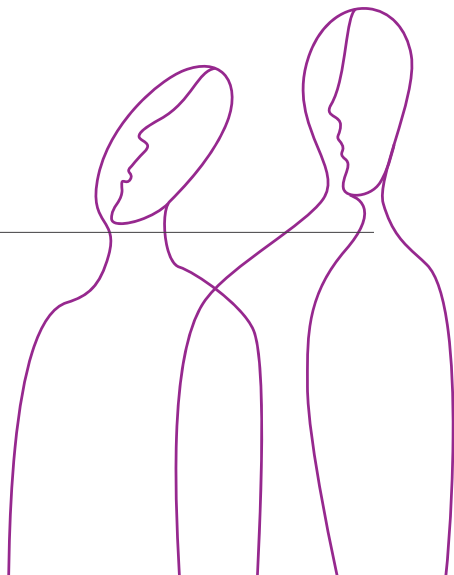
Gary Thuerk, the father of spam
https://www.computerworld.com/article/2539767/unsung-innovators--gary-thuerk--the-father-of-spam.html

The ARPANET (short for Advanced Research Projects Agency Network)
https://en.wikipedia.org/wiki/ARPANET

Driving the Information Highway

While such early "spam" was mostly benign, the first large-scale commercial spam attack was launched in 1994 by two lawyer partners, Lawrence Canter and Martha Siegel, shortly after the National Science Foundation lifted the unofficial ban on commercial speech on the Internet. Their ad targeted the susceptible immigrant community, promising legal assistance for enrollment in the nation's green card lottery. Utilizing the services of a mercenary coder, they churned out a digital ad promoting their services and delivered it overnight to nearly 6,000 discussion groups on the Usenet. The effort incited an immediate firestorm of outrage. It also reportedly netted the couple a windfall of new business, prompted the launch of their own "spam for hire" business, and led to their authorship of a popular self-help book, How to Make a Fortune on the Information Superhighway: Everyone's Guerrilla Guide to Marketing on the Internet and Other On-line Services.

By most accounts, the notorious "Green Card Spam" incident is credited as the watershed event ushering in an explosion of spam traffic onto that Information Superhighway. According to the Internet Society's published "History of Spam," by 2003, the amount of spam email had surpassed legitimate emails, and by 2010, an estimated 88% of all email traffic was defined as spam. Clearly the lure to "Make a Fortune on the Information Highway" was a strong one.



Laurence Canter and Martha Siegel: Green Card Spam
https://en.wikipedia.org/wiki/Laurence_Canter_and_Martha_Siegel

The History of Spam
https://www.internetsociety.org/wp-content/uploads/2017/08/History20of20Spam.pdf

From Spammers to Spitters

While concern was growing over the integrity of email in the wake of the new spam barrage, another form of digital spam – unsolicited voice calling - was stealthily taking root. Like junk email, voice spam is an unwanted byproduct of Internet technology. Its rise was mostly facilitated by the digitalization of voice data combined with the development of Voice Over Internet Protocol (VoIP) and multi-media Session Initiation Protocol (SIP) connectivity. While enabling high quality, low cost, global phone calling and the integration of voice into unified messaging applications, SIP also opened the gates to opportunists, mass marketers and scammers looking to exploit the more personalized medium of voice to reach their targets.

These intrusions, dubbed SPIT (Spam over Internet Telephony) in 2004, share much in common with their email counterpart per perpetrators and intent, but with several significant distinctions, beginning with the disturbance factor.

Email spam does not ring. It arrives at the email server where it can be evaluated and possibly identified as unwanted spam before the user ever accesses it. Even then, it will rest in the user's inbox until the recipient chooses to open it (or dismisses it outright based on the sender or subject line). Voice spam, on the other hand, creates an immediate disruption. Once the call session is initiated, it is too late for a system to analyze the content of the call, and so it simply rings through. Minus any form of external filtering other than generic caller ID, a voice spam call is virtually indistinguishable from any other call. And while consumers may choose to ignore calls from unknown sources, business users should not, which means voice spam has a significantly greater impact in terms of work disruption for the business user compared with email spam.

.

additionally, email spammers must rely on well-defined purchased lists of addresses, in contrast to the finite, sequential nature of phone numbers which gives phone spammers a greater chance of hitting a live target through random dialing.

That, combined with auto-dial technology, pre-recorded messages, virtually unlimited, low-cost VoIP bandwidth, a spoofed caller ID and the ability to use large, low-cost overseas call centers to field any call that gets a response, created the "robocall" phenomenon and a growing threat to voice network integrity.

Why Voice Spam? It's Cheap, Easy and Effective

The relative ease of accessibility to robocall technology has also produced a reverse trajectory for spam activity vs. email. The percentage of email identified as spam peaked in 2008 at 92.6%, but since then, that percentage has dropped precipitously and, as of 2019, had fallen to under 29%. Conversely, voice spam is on a sharp rise. In a Federal Communications Commission report from First Orion, more than half the calls placed in 2019 were spam, more than doubling that number from the previous year. While the pandemic of 2020 put a temporary hold on robocall activity, it is showing signs of a strong revival as businesses reopen.

SPIT (Spam over Internet Telephony)

https://www.webopedia.com/DidYouKnow/Internet/spam_spit_spim.asp

The percentage of email identified as spam

https://www.statista.com/statistics/420400/spam-email-traffic-share-annual/

Tip to Voice Spam Driven by Effectiveness

Many other factors are at play with the apparent rise of phone spam/scam activity over email, but all are driven by the likelihood of success for the perpetrator.

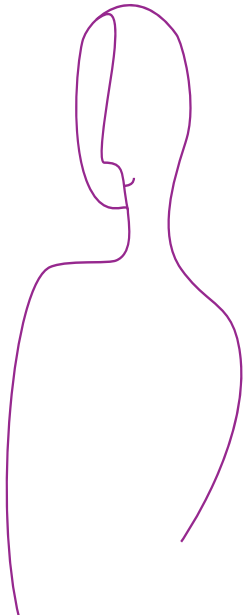
For one thing, consumers have become more discerning about email and tell-tale signs of an email scam. Additionally, email servers have become more sophisticated in their spam-spotting capabilities based on analysis of sender history, ip domain reputation, and message content, so messages are flagged at the server level and simply routed out of sight into the recipient's junk folder.

Voice spammers/scammers, on the other hand, have been especially adroit at exploiting not only the innate advantages of the medium, but also the psychological vulnerabilities of their targets.

For example, voice calls are more direct. Unless sent to voicemail, they establish an immediate, unfiltered connect between the caller and the called party and so demand immediate attention. While Caller ID is normally displayed, it can be easily "spoofed" to look like a familiar number or organization, so detecting the actual source of the call is impossible for the called party. And, unlike email, there is no "content" that can be examined prior to call delivery, so the nature and intent of the caller is not exposed until the connection is already made.

In other words, for all the benefits of Internet telephony come significant shortcomings that have provided an easy pathway for spammers, scammers and spoofers to, at best, disrupt phone network and recipients and, at worst, execute their criminal activity. Note that the Federal Communications Commission (FCC) is attempting to provide some protections against nuisance robocalls through enforcement of the TRACED Act, but the system so far has many hurdles to cross to be at all effective.

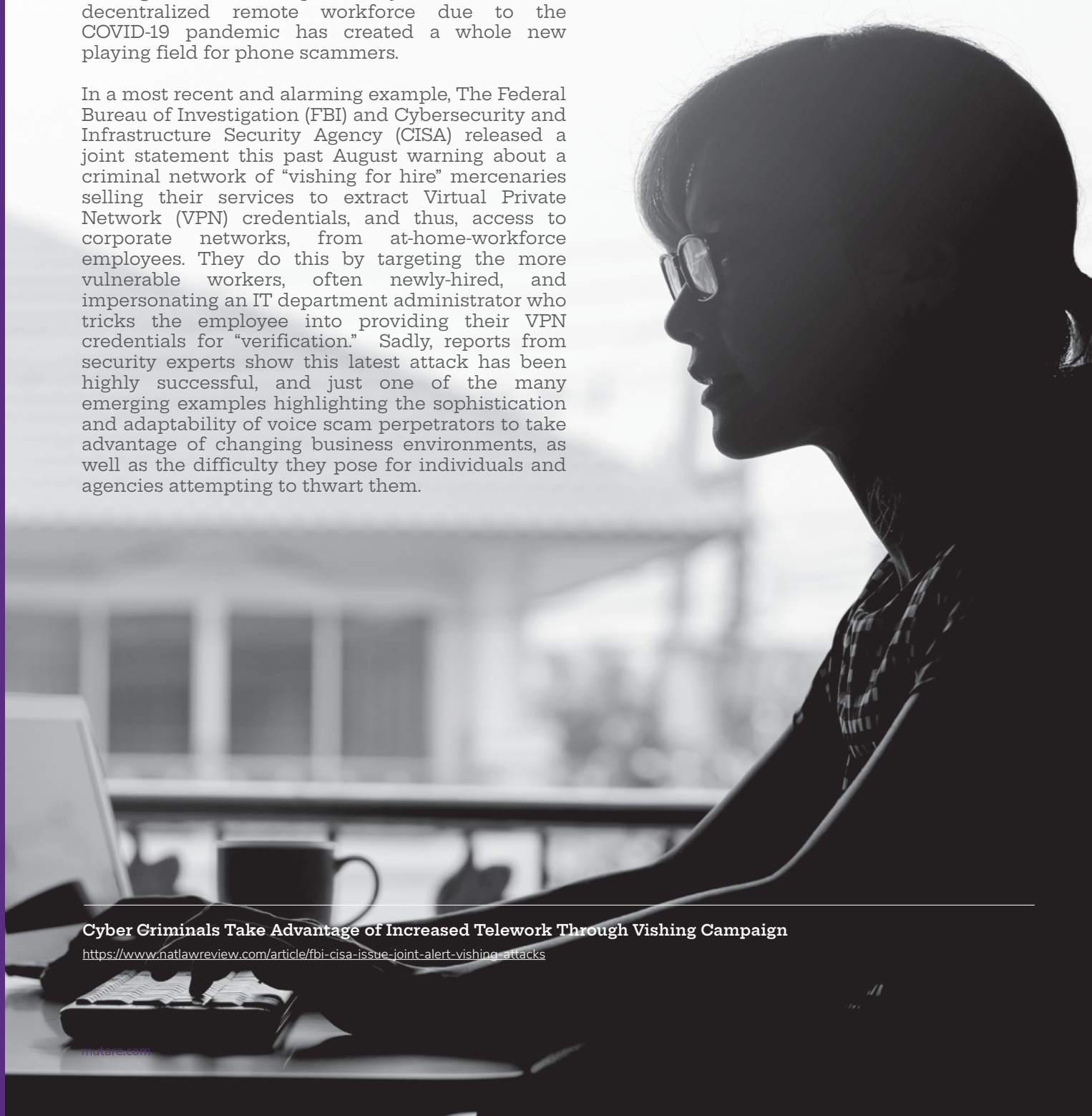
The psychological advantage of phone call vs. email has also attracted highly skilled scammers to the medium, using the persuasive power of voice and social engineering techniques to defraud their victims. These particularly malicious, but too-often successful Vishing (Voice Phishing) attacks are directed at specific vulnerable individuals, and usually employ spoofed caller IDs and personal information gained through other hacking attacks to manipulate the call recipient into a false sense of trust in order to extract from them sensitive or protected information.



Targeting At-Home-Workforce Employees

While there have been a number of high-profile vishing cases over the past few years, the rise of a decentralized remote workforce due to the COVID-19 pandemic has created a whole new playing field for phone scammers.

In a most recent and alarming example, The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) released a joint statement this past August warning about a criminal network of "vishing for hire" mercenaries selling their services to extract Virtual Private Network (VPN) credentials, and thus, access to corporate networks, from at-home-workforce employees. They do this by targeting the more vulnerable workers, often newly-hired, and impersonating an IT department administrator who tricks the employee into providing their VPN credentials for "verification." Sadly, reports from security experts show this latest attack has been highly successful, and just one of the many emerging examples highlighting the sophistication and adaptability of voice scam perpetrators to take advantage of changing business environments, as well as the difficulty they pose for individuals and agencies attempting to thwart them.



Cyber Criminals Take Advantage of Increased Telework Through Vishing Campaign
https://www.natlawreview.com/article/fbi-cisa-issue-joint-alert-vishing-attacks

Putting a Filter Between Spammers and Enterprise Networks

While some level of spam filtering/suspect call identification is becoming a common feature for cellular phone carriers, business-centric enterprise phone networks are still left relatively unprotected from the potential damage of voice spam, robocalls and vishing attacks. Employee cyber-security training, including an emphasis on how to recognize scam and vishing calls, should be an essential element for any enterprise risk management program. Equally important, businesses IT should strongly consider an investment in a robust, enterprise-grade spam filtering solution for their voice networks, like that offered through Mutare, Inc.

Vaporize it.

mutare.com/vaporize

Mutare's Voice Spam Filter solution is designed specifically to protect enterprise voice networks. It employs a nationwide database of known spammer IDs along with a spectrum of integrated analytic tools to identify and block suspected spam, scam, vishing, spoof, and robocalls before they enter the enterprise voice network, so call recipients are protected from both the call disruption and potential fraud. The solution gives administrators full control over how their system responds to suspected incoming spam, including a built-in "spoof detection" system and unique Voice CAPTCHA feature that can be turned on as a further failsafe measure. There is no other enterprise application that matches the capabilities of the Mutare Voice Spam Filter.

It's clear, as long as spammers and scammers have easy access to tools that connect us to each other, they will continue to find new ways to pursue new victims, and businesses are increasingly at risk. Arming your voice network with tools that outsmart even the most savvy spammer is key, and it's well-worth the time to investigate how tools like Mutare Voice Spam Filter creates the foundation for a truly impenetrable defense strategy.

Spam I am... I am Spam

Understanding the history & connection of Email Spam & Voice Spam

MUTARE NEWS
SPECIAL REPORT

mutare

Online Article
https://www.mutare.com/spam-i-am/

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/