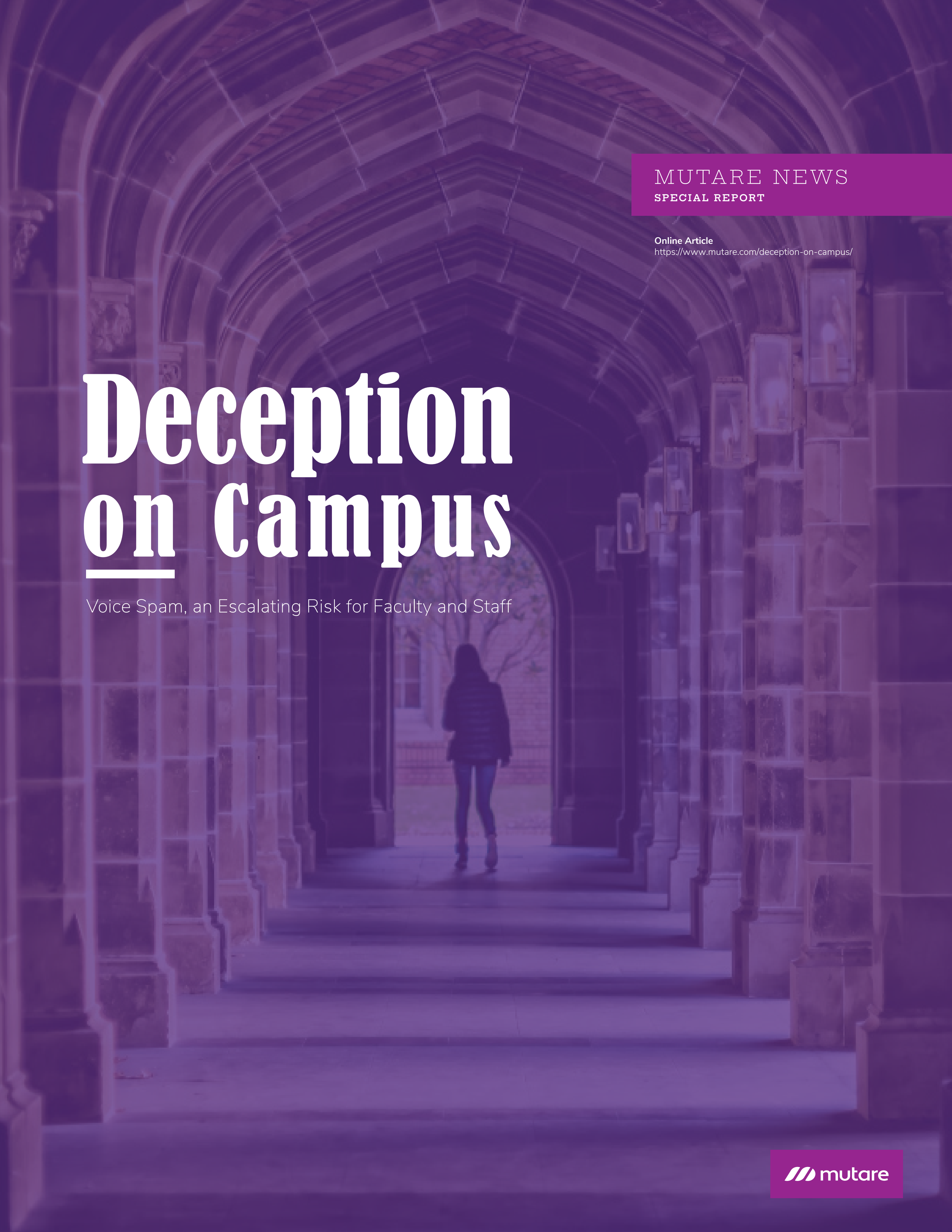


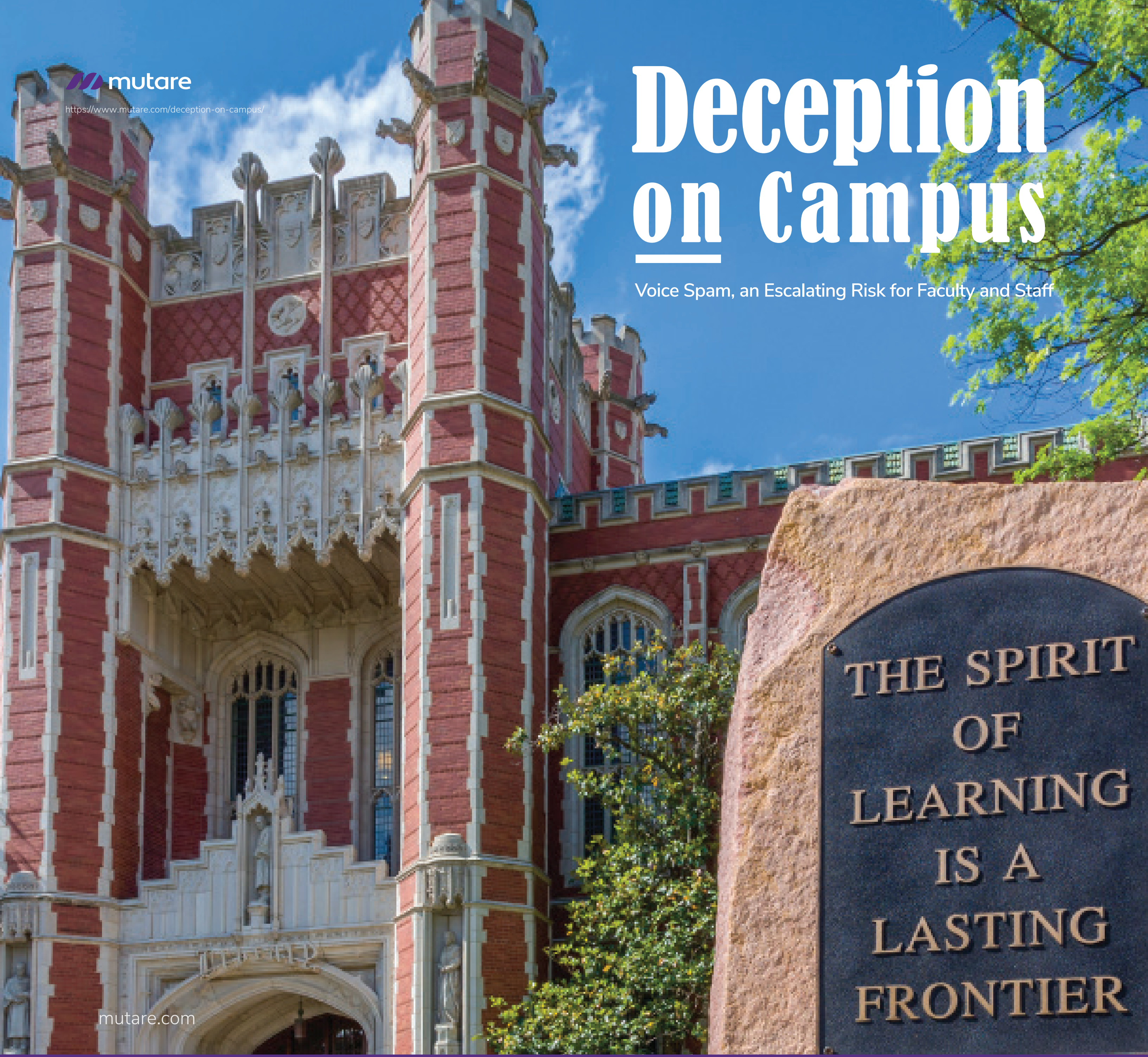
MUTARE NEWS
SPECIAL REPORT

Online Article
https://www.mutare.com/deception-on-campus/

Deception on Campus

Voice Spam, an Escalating Risk for Faculty and Staff

mutare



mutare

https://www.mutare.com/deception-on-campus/

Deception on Campus

Voice Spam, an Escalating Risk for Faculty and Staff

mutare.com

Executive Summary

When colleges and universities reopen their doors for on-campus learning this fall, it's not just students who will be happy to greet their educators. A new, increasingly virulent strain of voice spammers, robocallers and criminal scammers has been taking shape over the course of the pandemic and, according to data gathered by Mutare, Inc., is poised to take advantage of a particularly attractive target - institutions of higher education.

Table of Contents

Introduction

When colleges and universities reopen their doors for on-campus learning this fall, it's not just students who will be happy to greet their educators. A new, increasingly virulent strain of voice spammers, robocallers and criminal scammers has been taking shape over the course of the pandemic and, according to data gathered by Mutare, Inc., is poised to take advantage of a particularly attractive target - institutions of higher education.

Contact Information for faculty and staff is readily available on most university websites.

Key Facts for Higher Education

A	Higher Ed experiences a greater than average percentage of Spam Calls and Robocalls.
B	Students are a ripe target for scammers due to their lack of experience and deference to authority.
C	International faculty and students on US campuses are particularly vulnerable to nefarious phone scammers.
D	Contact Information for faculty and staff is readily available on most university websites.
E	Individuals in authority, with public profiles are an easy target for bad actors.
F	Many University IT & Security staff are not aware that tools are available to stop voice spam.

Let’s First Level-Set about Voice Spam

The term “Voice Spam” is often used as a general reference encompassing different forms of unsolicited phone calls. These phone calls can be placed by live humans or by using a recorded message delivered en masse through auto-dialing technologies—better known as robocalls. Originally used for purposes like telemarketing or political messaging, over the years robocalls have crossed the line from benign annoyance to severe disruption and criminal threat as bad actors have seized on Voice over Internet Protocol (VoIP) technology to deliver mass numbers of unwelcome and often illegal calls from hidden identities.

Variations of Illicit voice spam Includes:

Social Engineering Calls

The goal of these callers is to gather sensitive, financial, or information technology (IT) Intelligence from the call recipient. The caller may also be Intent on stealing some bit of information to fuel a larger data attack. For instance, social engineering calls may seek information about an organization's reporting structure, names and phone numbers or email addresses of key personnel, or information about computer systems or other data. These calls are very difficult to detect and usually go unreported.

Voice Phishing (Vishing)

Bad actors may use social engineering techniques, combined with a fraudulent caller ID (see "Spoof Calls") to present as a trusted source In order to lure their target into providing information for criminal purposes. Such techniques tend to be targeted—including sophisticated attacks on individual staff members.

Robocall Scam Attacks

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.

Spoof Calls

Call “spoofing” is the act of changing the caller ID to a number other than the actual caller’s number. While sometimes used for legitimate purpose to protect the caller’s identity, bad actors are using the practice to trick call recipients into thinking the call is trusted because it is from a familiar area code ("neighbor spoofing") or a familiar business name or number ("enterprise spoofing"). Caller ID spoofing is often used in tandem with social engineering techniques to further trick the recipient into complying with the caller’s request for information.

Colleges and Universities are Unique Targets

Institutions of higher education experience a larger than average percentage of unwanted calls entering their internal phone networks.

According to Mutare's VTA data, nearly 15% of all calls directed at college faculty and staff are unwanted, with some institutions experiencing numbers as high as 32%.

The impact in terms of lost time and productivity is significant. When projected over a year's time, Mutare calculates an average cost per institution tops $1 million annually!

However, there is additional impact beyond lost time due to chronic disruptions or unnecessary voicemail management. Statistically, 83% of those calls are using spoofed phone numbers, a common technique used by spammers attempting to hide the true source of their call. What's more, 40% are identified as actual scams. Staff and faculty are not just losing time due to unwanted calls. They are also facing victimization from fraud.

While students make particularly attractive targets for phone scammers intent on taking advantage of their lack of experience and deference to authority, university faculty and staff members working behind their institution's PBX phone systems are no less insulated from the disruption and outright threat posed by robocalls, spammers, scammers and other malicious callers penetrating those networks. International visiting faculty members are particularly vulnerable, as noted on Yale University's Office of International Students and Scholars website. With English as a second language and lack of familiarity with cultural and governmental norms, these individuals are now being exposed as likely targets for attacks from vishers posing as officials from, for instance, the Departments of Homeland Security or Immigration Services.

The problem is further exacerbated by the fact that contact information for faculty and staff is often readily available through online directories. When combining that with other easily harvested personal information and a spoofed phone number, experienced vishers are able to make convincing calls posing as a trusted source in order to bilk their targets out of money or personal information.

But the problem extends beyond anonymous vishers looking to profit. Academics are also easy targets for malicious calls from extremist groups intent on intimidating those in positions of authority and with public profiles. New York's Columbia University and affiliate Barnard College experienced this first hand late December 2019 when a high-profile murder case involving a student unleashed an onslaught of threatening robocalls to faculty and staff from a white supremacist group.

15%
of all calls are
Unwanted

$1M
lost productivity

40%
of Unwanted Calls are
Scams

83% of those calls are using spoofed phone numbers

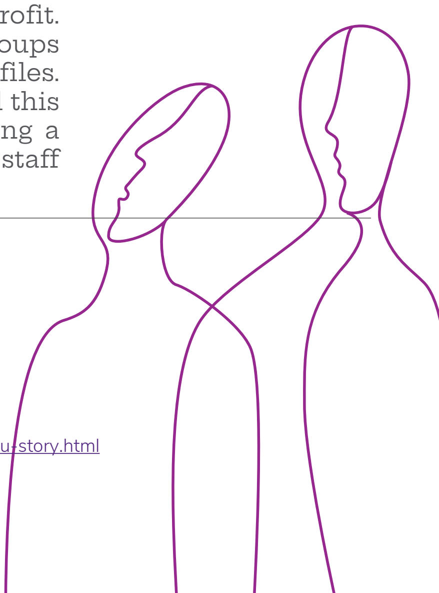
https://firstorion.com/wp-content/uploads/2019/07/First-Orion-Scam-Trends-Report_Summer-2019.pdf

Yale University's Office of International Students and Scholars website

https://oiss.yale.edu/taxes-legal/scams-fraud

an onslaught of threatening robocalls to faculty and staff

https://www.nydailynews.com/new-york/ny-columbia-white-supremacists-20191226-afvhdhtflba67kdph7zo5anmnu-story.html



What Some Institutions are Saying...

A quick web search of the term “phone scam” with any college or university name reveals that these Institutions do, indeed, recognize spam and robocalls as a real problem. Most have added a page on their sites dedicated to driving awareness in their campus communities about vishing, scams, and other nuisance calls.

For example:

“Beware of Scams Targeting Students, Employees” headlined an alert from Colorado State University’s police.

“Vishing....Many of us have received these types of calls recently. Like many other organizations, the University of Miami has been affected by this deceptive practice when our campus numbers are spoofed. You may have received a call from what looks to be a legitimate number, only to find that it is a scam,” the University of Miami posted on its IT web page.

“Harvard University has had numerous reports of employees receiving nuisance calls, however these calls are widespread affecting Harvard, other universities, companies, residential landlines and cellphones,” reads a Harvard University alert.

Colleges and universities have also Increasingly reported Incidences of scammers using spoofed numbers connected to the Institution to scam students and families, not only harming those Individuals but potentially damaging the Institution's reputation in the process. In one example, a Penn State news alert warned that scammers had spoofed the number for campus police in order to demand money and threaten jail time to those who did not comply.

And yet, the only help most can offer up are tips on how to recognize scam calls and how to report them. As stated on the “Nuisance/Malicious Telephone Call Guidelines” page on the University of Michigan IT site, “Annoying, nuisance, spam, and robocalls cannot currently be blocked.”

That is, until now.

Colorado State University

https://source.colostate.edu/beware-of-scams-targeting-students-employees/

University of Miami

https://www.it.miami.edu/about-umit/it-news/phishing/vishing/index.html

Harvard University

https://phone.harvard.edu/news/nuisance-calls-spam-robo-calls

College Call Spoofing Scams Target Students and Institutions

https://calleridreputation.com/blog/college-call-spoofing-scams-target-students-and-institutions/

The Pennsylvania State University

https://news.psu.edu/story/590924/2019/10/01/campus-life/scammers-spoof-penn-state-police-phone-number

University of Michigan

https://its.umich.edu/communication/telephone/policies/nuisance-malicious-telephone-call-guidelines

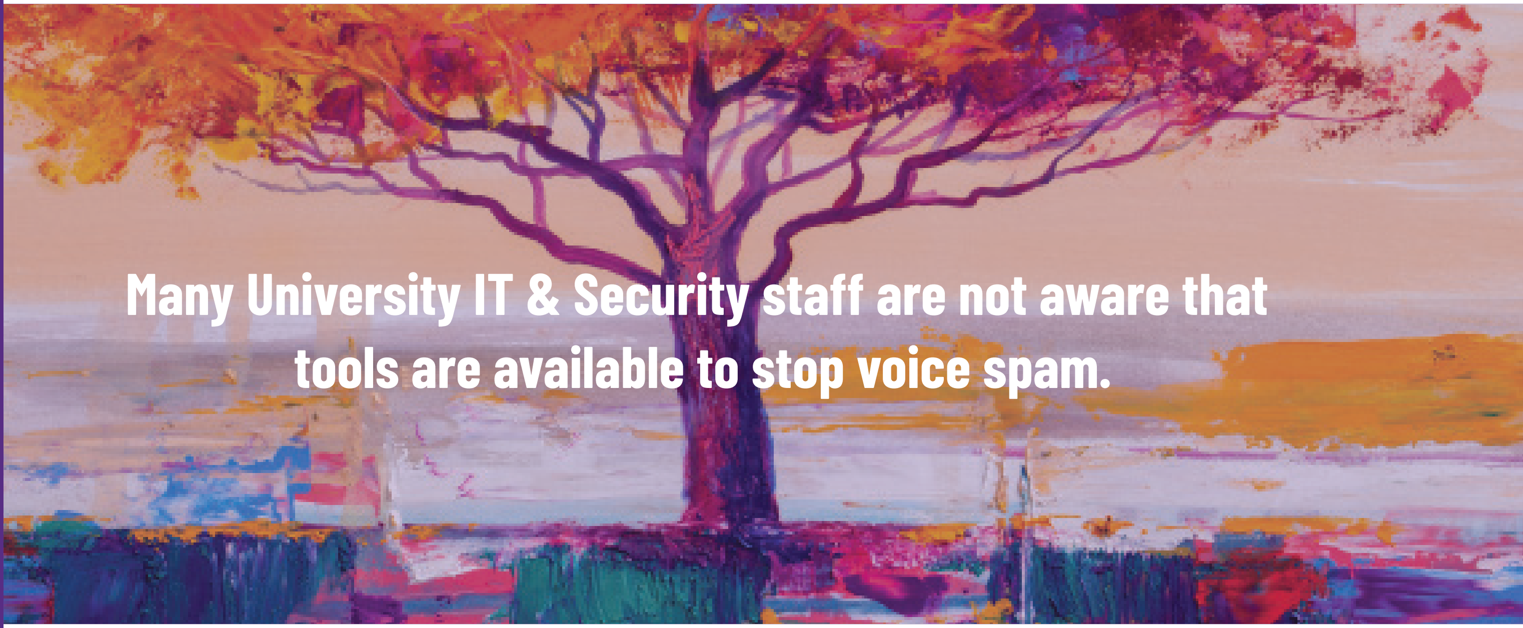
Enterprise Voice Spam Filter Outsmarts the Spammers

As the developer of the nation's first truly effective spam filtering solution for enterprise voice networks, Mutare, Inc., knows a thing or two about the forces driving today's unrelenting tsunami of spam and robocalls. Not only has Mutare's Voice Spam Filter blocked millions of unwanted calls for its enterprise customers but, in the process, has provided those organizations with valuable insights about the content of their voice traffic and efficiency of their voice networks through the application's built-in analytics and reporting tools.

Mutare's Voice Spam Filter is the only enterprise solution of its kind to effectively identify and block the vast majority of voice spam in its many forms, from robocalls to spoofers, vishers, spammers and scammers. It employs a massive nationwide database of known spammer and robocall IDs along with a spectrum of integrated analytic tools to identify and block suspected calls at the network edge, 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 proprietary "spoof detection" system and unique Voice CAPTCHA feature that adds a second layer of screening for suspect calls. Organizations can add their own allow lists, block lists and rules to further customize the management of incoming calls and block any nuisance or malicious callers specifically targeting their institutions.

Added Benefit – Network Performance Assessment

While blocking unwanted calls, Mutare's Voice Spam Filter also captures and organizes all incoming call data for analytics and reporting purposes and, in the process, can reveal anomalies in call patterns that warrant further investigation by IT systems administrators. "We have had a number of customers tell us how much they appreciate the added benefit of ongoing voice traffic monitoring and the visual data display on the admin dashboard," says Mutare Regional Manager Erik Jacoby. "Network errors or inefficient call distributions are just some examples of correctable issues that we have uncovered. It's a nice additional benefit, even for prospects who simply want us to run a proof-of-concept Voice Traffic Analysis for them. It's easy to make the case for full implementation once they see the depth of our spam detection and voice traffic analysis capabilities."


Many University IT & Security staff are not aware that tools are available to stop voice spam.

Our Bastions of Open Discourse and Thought Development Must Be Protected

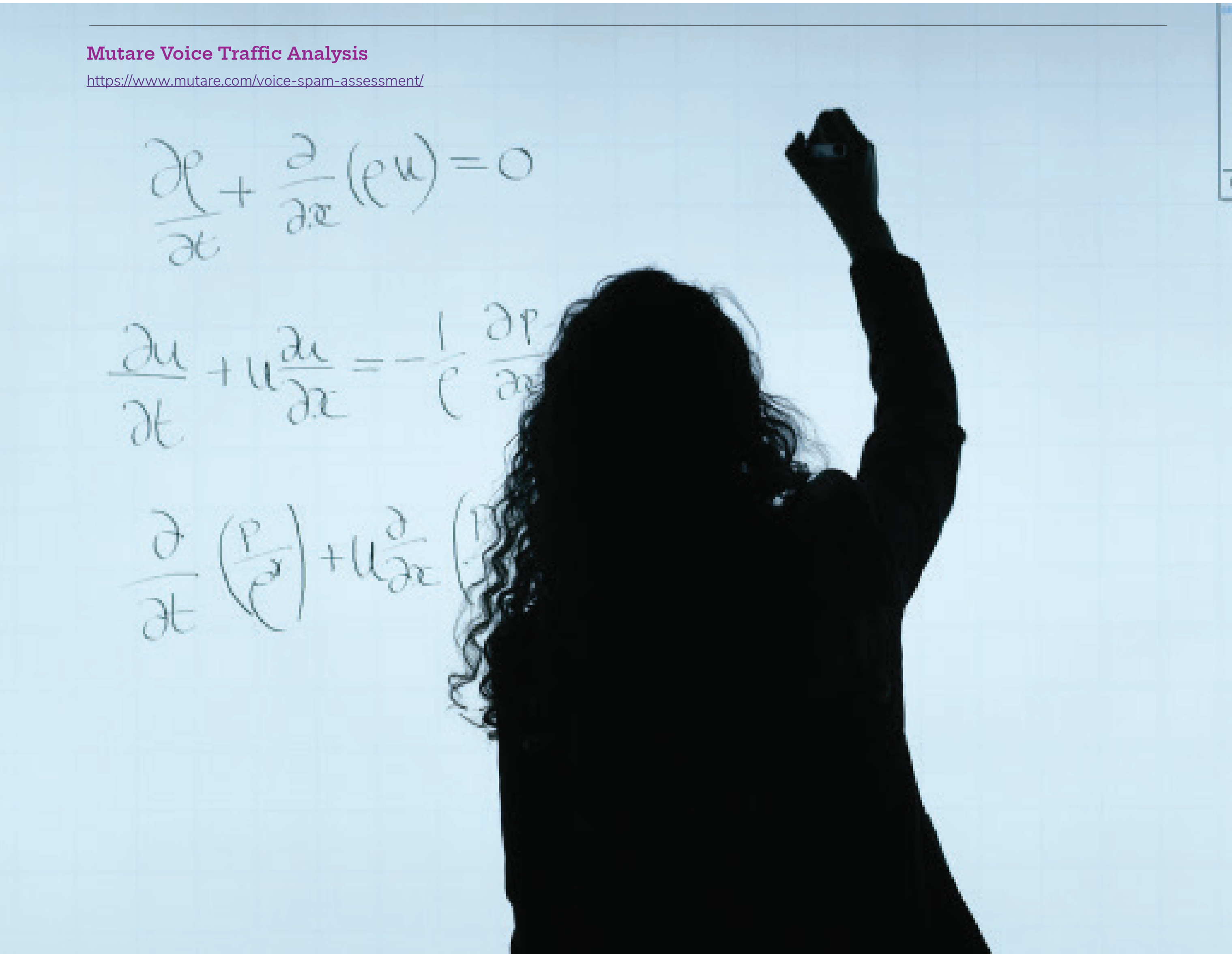
While executing their vital responsibility to educate the next generation of workers and scholars, Institutions of higher education and those they employ are, themselves, Invaluable repositories of accumulated knowledge that serves to advance that mission for generations to come. It Is a paradox, then, that the university environment and the intellectual property contained within deserves the highest degree of protection while, at the same time, depends on open avenues of discourse and unrestricted access to fulfill Its commitments to Its students and the society they will enter. Combine that with the susceptibility of an Inexperienced and transitory student population, the presence of a more vulnerable faculty and staff, and ready access to personal and contact Information, and It Is easy to see why anonymous scammers leveraging easily manipulated voice communication pathways have set their sights on these Institutions. Fortunately, Mutare's deep experience with voice communication solutions development and commitment to protecting the Integrity of voice networks and the Institutions that depend them has led to a real solution.

Find Out
if Your Organization
is Being Impacted by Voice Spam

Over the past year, Mutare has extended, as a service, the use of its proprietary voice traffic filtering and analysis technology to produce a fully detailed Voice Traffic Analysis report for organizations interested in gaining a better understanding of the make-up of their voice traffic and the impact of voice spam intrusions. In the process, the company has divined some interesting, industry-specific patterns and Insights. Specifically, not only do Institutions of Higher Learning have a larger than average number of robocalls and spam calls entering their networks, but they are uniquely vulnerable to the more dangerous variations that bring real harm to their communities.

Regardless of organization, those struggling with voice spam know there is power in knowledge.

To learn more about the power of Mutare's Voice Spam Filter or to request a Voice Traffic Analysis for your organization, visit https://www.mutare.com/voice-spam-filter.


$\frac{\partial \rho}{\partial t} + \frac{\partial}{\partial x}(\rho u) = 0$
$\frac{\partial u}{\partial t} + u\frac{\partial u}{\partial x} = -\frac{1}{\rho}\frac{\partial p}{\partial x}$

Mutare Voice Traffic Analysis

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

Deception on Campus

Voice Spam, an Escalating Risk for Faculty and Staff

Online Article
https://www.mutare.com/deception-on-campus/

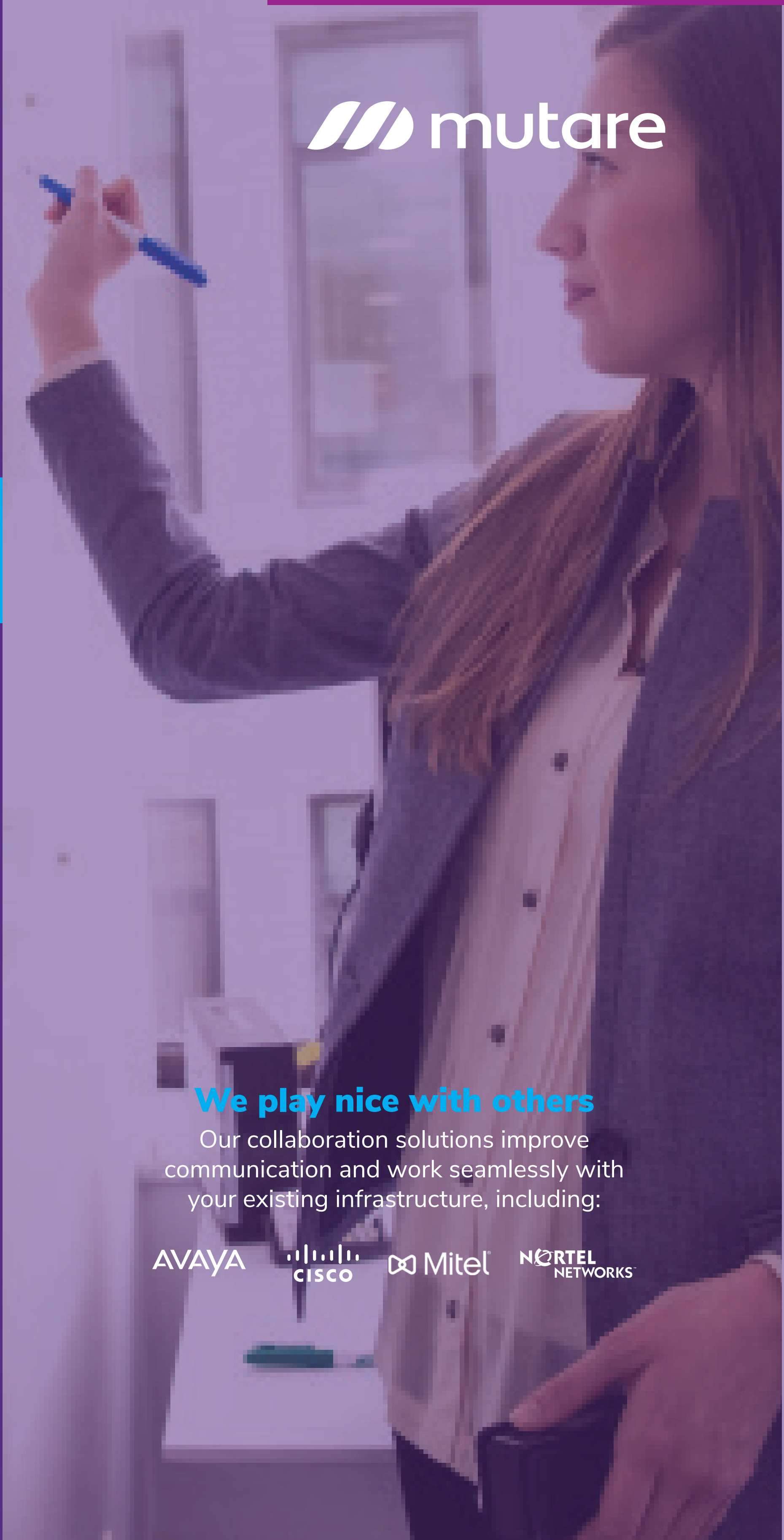
FREE Assessment
Find out how Voice Spam is
impacting your institution
https://www.mutare.com/voice-spam-assessment/

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/



MUTARE NEWS
SPECIAL REPORT

mutare

We play nice with others

Our collaboration solutions improve communication and work seamlessly with your existing infrastructure, including:

AVAYA CISCO Mitel NORTEL NETWORKS