Nonprofit Cybersecurity Incident Report by Matthew Eshleman

Emerging Trends, Practical Advice

8TH EDITION: 2026

CommunityIT Innovators®
Where Technology Meets Mission

Table of Contents

CommunityIT Innovators®

ABOUT THE AUTHOR

Matthew Eshleman

Chief Technology Officer
Community IT

As the Chief Technology Officer at Community IT, Matthew Eshleman leads the team responsible for strategic planning, research, and implementation of the technology platforms used by nonprofit organization clients to be secure and productive. With a deep background in network infrastructure, he understands how nonprofit tech works and interoperates both in the office and in the cloud. With extensive experience serving nonprofits, Matt also understands nonprofit culture and constraints and has a history of implementing cost-effective and secure solutions at the enterprise level.

Matt has over 23 years of expertise in cybersecurity, IT support, team leadership, software selection and research, and client support. Matt is a frequent speaker on cybersecurity topics for nonprofits and has presented at the Technology Association of Grantmakers, Jitasa, Nonprofit Learning Lab, NTEN events, the Inside NGO conference, Nonprofit Risk Management Summit and Credit Builders Alliance Symposium, LGBT MAP Finance Conference, and Tech Forward Conference. He is also the session designer and trainer for TechSoup's Digital Security course, and our resident Cybersecurity expert.

Matt holds dual degrees in Computer Science and Computer Information Systems from Eastern Mennonite University, and an MBA from the Carey School of Business at Johns Hopkins University.

Matt Eshleman is available as a speaker on cybersecurity topics affecting nonprofits, including cyber insurance compliance, staff training, and incident response.

CommunityIT Innovators®

Thanks for downloading Community IT's 8th Annual Nonprofit Cybersecurity Incident Report. Started in 2018 to provide data driven insights into the real threats facing small to mid-sized nonprofit organizations, this report has matured into an annual discipline for me to see what trends have emerged and which tools are effective to combat the threats that organizations face.

This report draws on data from the calendar year of 2025 and begins to show the impact of AI on nonprofit security. Emails look more realistic and plausible, clever new scams are emerging such as fake invoicing, and we saw a spike in malware and viruses that is probably fueled by AI coding new variants. We also see a continued increase in brute force attacks meant to overwhelm organizational defenses, likely also driven by the ease with which such attacks can be coded and run with AI tools.

We saw an increase in advanced persistent threat attacks from well financed actors for partisan or political reasons. That said, the vast majority of cybercrime is still financial in nature, not partisan. The good news is fundamental cybersecurity practices are effective against both.

Data for nonprofit-specific cybersecurity threats is lacking, and marketing by cybersecurity firms tend to be jargon-filled and product centric. Our goal with this report is to inform our sector. Nonprofits should not be overwhelmed and bullied into purchasing solutions that are overly complicated, expensive, or misaligned with the actual threats facing their organizations. This year we do see evidence that your tools matter. In this report, we lay out the trends that we see, explain jargon and cybersecurity concepts, and provide a path forward.

We provide a quick checklist of important cybersecurity fundamentals at the close of the report, and links to further resources throughout for a deeper dive.

I hope that the data and reporting that we share here helps you understand and better face the cyber threats facing nonprofit organizations.

- Matthew Eshleman, Chief Technology Officer

CommunityIT Innovators®

Introduction

This report draws on data from 2025, and this year's numbers tell a story with a few clear chapters: AI is reshaping the threat landscape in meaningful ways, email-based attacks continue to climb, and virus and malware activity spiked noticeably. At the same time, wire fraud incidents dropped again, suggesting that training and stronger financial controls are doing their job.

Virus and malicious endpoint activity increased sharply – from 13 incidents in 2024 to 57 in 2025. AI is a factor here: it's enabling new attack methods both from outside organizations and, in some cases, self-inflicted risks from AI-generated tools and scripts that staff are running themselves.

Advanced Persistent Threat incidents – targeted attacks by state-sponsored actors – also increased, from 3 to 6. While concern about politically motivated targeting is understandably high right now, the data shows that the vast majority of cyberattacks on nonprofits remain financially motivated.

The good news: foundational cybersecurity practices remain effective against both financial and partisan threats.

CommunityIT Innovators®

What are we seeing?

AI is changing the game – for attackers. Emails look more realistic and plausible than ever. Scams are more creative and more convincing, including fake invoices, fake DMCA takedown notices, HR impersonation scams, and calendar invite attacks that bypass your inbox entirely. AI is helping threat actors code new malware variants and run brute force attacks at scale.

Account compromise is holding steady – but our visibility is improving. Better alerting and monitoring tools are catching more suspected account compromises. This is a sign that investments in security tools are paying off in awareness, even as threats persist.

Wire fraud continues to decline. Wire fraud dropped from 3 incidents in 2024 to 1 in 2025. In each case where wire fraud occurs, a compromised internal account is involved – reinforcing the importance of both staff training and secure financial transaction processes.

Ungoverned AI use is a growing risk. Nonprofit staff are using free and ungoverned AI tools across organizations, often without policy guardrails. This creates real data leakiness risks – sensitive organizational data being exposed to external systems without oversight.

CommunityIT Innovators®

What's next?

Nonprofit organizations continue to face a high risk of cyberattack, and AI is raising the stakes on both sides of the equation. Threat actors are using AI to launch more convincing, more creative, and more frequent attacks. At the same time, new tools and training are offering stronger protections – if organizations invest in them.

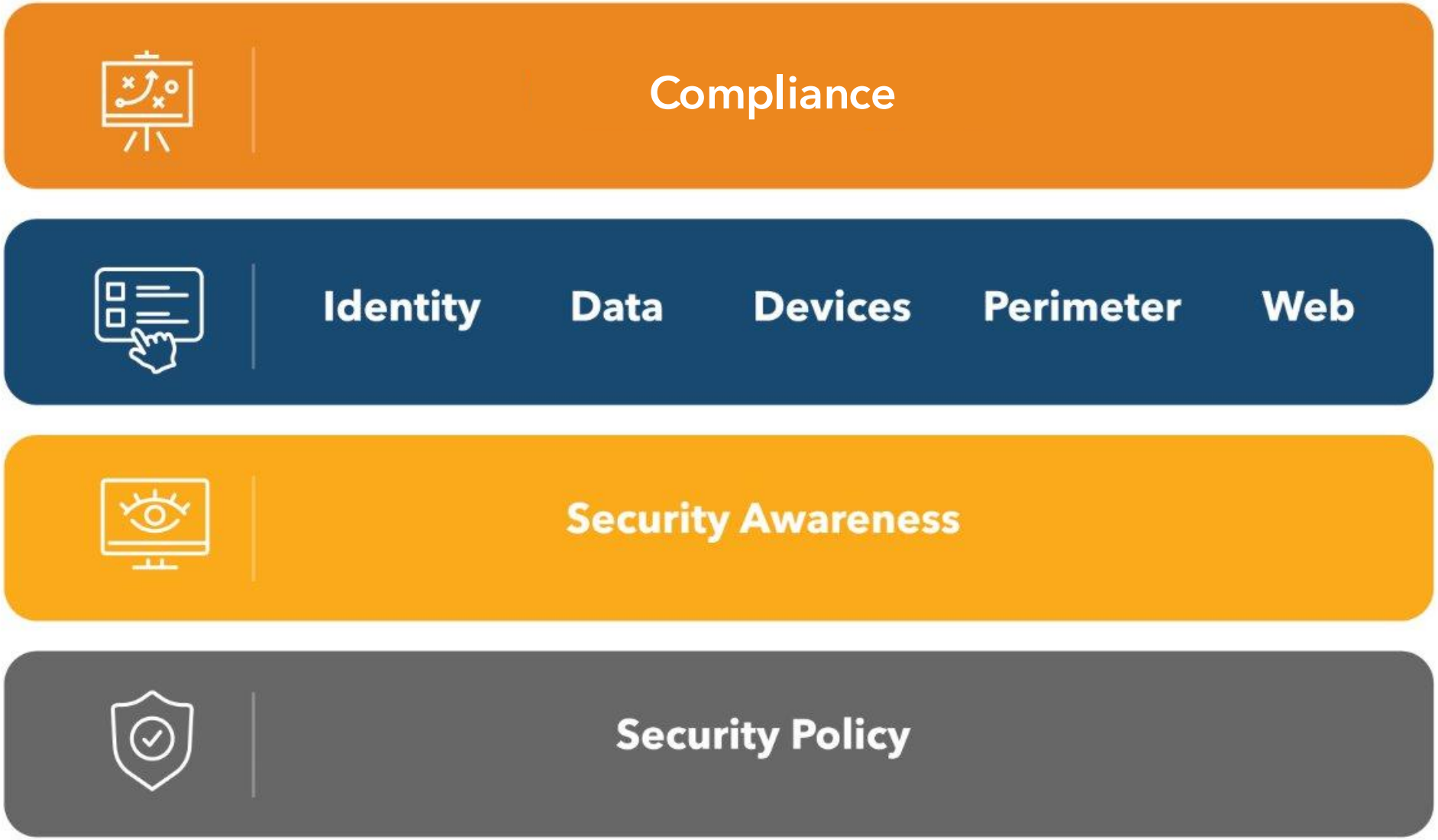
Vulnerable staff need training and protection that extends beyond work systems – online, personally, and from the reputational risks of partisan targeting and doxxing.

Foundational controls remain your best defense: security awareness training, phish-resistant MFA, strong data and AI use policies, and clear incident response plans. These basics hold up against new threats as well as old ones.

Learning Objectives in this Report

- Learn the cybersecurity landscape for nonprofits: what are general best practices?
- Learn cybersecurity lingo, definitions, and trending scams.
- Understand the initial impact of AI on cybersecurity: in assisting hackers, creating more risks, and creating more possible protections.
- Learn how to protect ourselves and our nonprofits in 2026.

CommunityIT Innovators®


Compliance
Identity
Data
Devices
Perimeter
Web
Security Awareness
Security Policy

Community IT Innovators Cybersecurity Framework for Nonprofits

This graphic is in our free Cybersecurity Readiness for Nonprofits Playbook download. That download goes into more detail and action items as well as how you can manage cybersecurity at your nonprofit. https://communityit.com/cybersecurity-readiness-for-nonprofits-playbook/

The lowest layer represents foundational cybersecurity concepts including **rooting your cybersecurity processes in policy** to provide guidance for technical solutions. On top of that we recommend a layer of **security awareness training** so that you have staff are educated and engaged about the very real risks that they face and can serve as your front line of protection.

We can't emphasize enough how important **training** is. Most of the attacks we see in this small to midsize nonprofit space, in organizations between 15 to 300 staff, are **initiated by something as benign as clicking on a link in an email** or being tricked into updating some payment information or buying gift cards, and new scams and cons too.

Moving up a layer we have a range of **technical solutions** that monitor and protect and recover when something does happen. That includes tools to automatically protect **identity, data, device management, perimeter protection, and website security.**

The top layer is **compliance**. You can have policies, awareness, and technical tools protecting you, but if you don't have a leader insisting on compliance, and reporting mechanisms to ensure your policies are being followed, you may as well not have the policies. In addition, cyber insurance, nonprofit auditors, and funders are increasingly interested in proof of compliance with cybersecurity best practices and policies.

This graphic continues to provide a good framework for us to talk about building effective cybersecurity protection plans at the organizations that we support, and you can also use this model to think about where to invest and what to focus on.

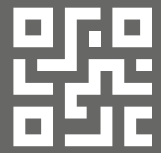
CommunityIT Innovators®

Definitions

- Threat Actor
- Advanced Persistent Threat
- Credentials/Compromised Accounts
- Malware
- Virus
- Brute Force Attacks
- Wire Fraud
- Ransomware

- Smishing
- Spear phishing
- Spoofing

- MFA Push Bombing/Fatigue attack
- AiTM Attacker-in-the-Middle attack
- QR Code Malware
  - Malware Browser Pop-up



- Pastejacking
  - Doxxing

CommunityIT Innovators®

Definitions:

Threat Actor: The entity perpetrating the attack: an individual, cybercriminal network, or corporate rival.
When a state sponsored adversary, usually called **Advanced Persistent Threat**.

Credentials, or Identity, is your username and password. A **Compromised Account** is one where a hacker can control your email and send authentic-seeming emails that seem to come from you, or from a new account the hacker has created and controls in your system.
Being able to link a staff member with social media accounts, personal emails, or reused passwords that are already on the dark web allows hackers multiple options for further crimes, or to sell that compromised Personally Identifying Information (PII) such as ID, credit card numbers, etc.

Malware/Virus Malicious software designed to damage, disrupt, or gain unauthorized access to your systems. A virus is a type of malware that spreads when infected files are opened or shared.

Brute Force Attacks An automated attack that rapidly guesses passwords until one works. Strong, unique passwords and MFA are your best defenses.

Wire Fraud: a federal financial crime that occurs over the Internet or by electronic means. If you're a victim of this, it's something you should report to the FBI, whether a payment was made and money lost or not.

Ransomware: A type of malware that encrypts your files, making them inaccessible until you pay the attacker – typically in cryptocurrency – for the decryption key.

Smishing or text-based phishing. SMS text protocols combined with phishing gives us smishing. Messages range from obvious, for example "click on this link to authorize this package," to AI-driven or real conversations with hackers that lure you into sharing your identity.

Spear phishing: A targeted email scam where the sender appears to be someone you know or trust, and asks you to click a link, share credentials, or take a financial action. The sender knows details about you or your organization.

CommunityIT Innovators®

Definitions:

Spoofing: a fraudulent email that uses deception to appear to be from another sender. This might be by using small typos, or by disguising the email header to appear to show a legitimate sender. Hovering over the email will reveal the fraudulent sender's email and metadata. A spoofed email does not indicate an email compromise. Spoofing is easy to do and easy to detect.

Multi Factor Authentication (MFA): using a second factor to confirm identity, usually a text message code or an authenticator app. Can be a physical key. MFA that requires an employee to use their personal device such as a smartphone should be covered under Acceptable Use Policies. Employees using personal emails or devices to provide a backup or recovery authentication to organization accounts should be protecting those personal emails against phishing and re-used passwords, and those personal devices against insecure connections.

MFA Push Bombing/Fatigue Attack: multiple requests for MFA validation that wear the user down until, despite knowing that they are not themselves trying to log in, they assume the requests are important and approve one. This opens the victim up to an Attacker in the Middle AitM attack where their MFA token can be stolen.

QR code: A code that your phone can read as a URL. QR codes are everywhere and very useful links on menus or signs, but threat actors are using them to get you to click on links embedded on false websites.

Malware browser pop-up: A social engineering attack where a popup window opens claiming you have a virus or your computer's being encrypted and you need to call the help number and not close the tab. The message creates a sense of panic. Close the tab and it'll go away. If you are unsure how to close the tab safely, contact your IT provider. Do NOT call the number on the popup.

Pastejacking: A social engineering attack where the victim is fooled into entering malicious code in order to open a document.

Doxxing: Personal or online attacks in which personal data such as home address, family members, or employer, is revealed in order to intimidate or silence someone. We are seeing more personal attacks against nonprofit staff or spokespeople who hold a different world view than the attacker. If you or your staff is facing this intimidation, we have resources on our site to help you stay safer.

CommunityIT Innovators®

Current Cybersecurity Landscape

- Cyber criminals see their work as a job not a hobby.
- Most organizations are primarily under threat for financial scams. Most hackers just want your money.
- Partisan attacks are increasing including online doxxing/personal attacks.
- AI presents an opportunity for threat actors in new scams and more convincing scams and vulnerabilities

CommunityIT Innovators®

Landscape: Hacker Approach

- AI is making attacks are more convincing.
- AI is also helping create creative new scams.
- Viruses and malware are rising. AI is helping.
- Compromise/spoofing/phishing increasing.
- Increase in HR scams and longer cons.
- Increase in creative ways to get users to click on something – calendar, malicious code in images or on websites, etc.

Landscape: Operational Trends

- Account compromise is holding steady.
- Cyberliability insurance and auditing requirements are driving stronger IT risk assessments and cybersecurity controls.
- MFA compromises flat; major Attacker-in-the-Middle actor taken down. Passkeys becoming standard.
- Anti-phishing training becoming standard practice.
- Recognition of ungoverned account risks; better offboarding and data retention policies trending up.

Selected Resources:

- https://communityit.com/cybersecurity/
- https://communityit.com/blog-mission-aligned-ai-adoption-model-for-nonprofits/
- https://communityit.com/template-acceptable-use-of-ai-tools-in-the-nonprofit-workplace/
- https://communityit.com/webinar-how-to-use-ai-tools-safely-at-nonprofits/
- https://communityit.com/blog-3-basic-cybersecurity-essentials-for-nonprofits/
- https://communityit.com/podcast-cybersecurity-viruses-phish-resistant-mfa/
- https://communityit.com/webinar-cybersecurity-tabletop-exercise-for-nonprofits/
- https://communityit.com/podcast-anti-doxxing-and-nonprofit-staff-safety/

- https://communityit.com/download-cybersecurity-readiness-for-nonprofits-playbook/

CommunityIT Innovators®

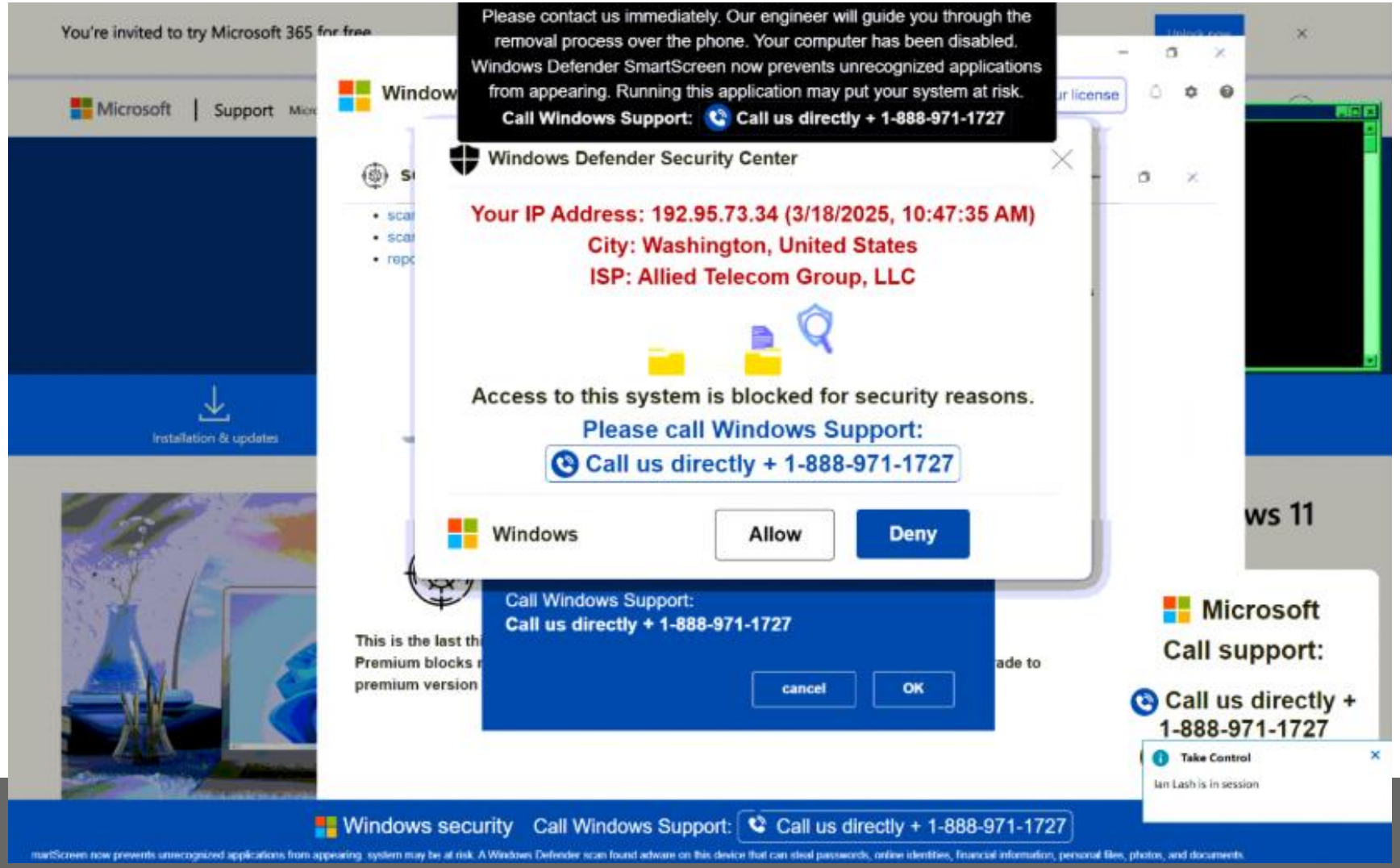
New Cybersecurity Attacks in 2025

- Increase in viruses and malware
- Fake invoices
- AI manipulated or AI generated digital scams
- Fake DCMA violation notices
- HR scams that trade on the organization's identity
- Calendar invite scams that bypass your inbox

A common tactic is to use fear, "legal authority," urgency.
Or a convincingly mundane request.

CommunityIT Innovators®

Malware Pop-up Scam



Impersonation

Subject: Received? As of today, we are yet to receive ACH payment. Just checking, did the attachments come through on your end? For compliance reasons, please do not CC anyone when replying to this email. Thank you. Jimmy Ratliff **CEO/Founder Jimmy Ratliff**

Fake Invoice

Simpson Thacher Bartlett LLP
425 Lexington Ave Ste 15
New York, NY 10017

Invoice #: 981992001
Created: April 08, 2025
Terms: Due Upon Receipt
Account ID: ALE293000-122

Bill to:
Stimson Center
United states

Attn: **Brian Finlay**

INVOICE

Item	Price
Stimson Center - Feasibility assessments, Creation and Deployment of a new marketing strategy	$37,500.00
Executive Development and Professional Services for (Brian Finlay)	$19,000.00
Initial setup and onboarding - stimson.org	$23,501.00
SIN 874-1 **Stimson Center** - Holistic Approach - Customized Solutions - Project Management - Assessment and Measurement - Principle-Centered Organizational Change - Method Optimization	$18,900.00
Comprehensive Reports and Analytics Sr. Consultant I Sr. Consultant II	$999.00
	Total: $99,900.00
	Discount 10%: $9,990.00
	Balance Due: $89,910.00
Payment Information	

Bank Name: Citibank, N.A
Bank Address: 111 Wall Street New York, NY 10043
Beneficiary: Simpson Thacher Bartlett LLP
ACH/Wire Routing #: 031100209

Comprehensive Reports and Analytics Sr. Consultant I Sr. Consultant II	$999.00
	Total: $99,900.00
	Discount 10%: $9,990.00
	Balance Due: $89,910.00
Payment Information	

Bank Name: Citibank, N.A
Bank Address: 111 Wall Street New York, NY 10043
Beneficiary: Simpson Thacher Bartlett LLP
ACH/Wire Routing #: 031100209

SWIFT Code #: CITIUS33
Account #: 7058763000161421O
Payment Method #: EFT only

Note: Please make the payment by the due date to avoid any late fees.

CommunityIT Innovators®

Fake DMCA Takedown Notice

Page Name:
South Asian Voices

Facebook ID:
170510573143983

Detection Date:
July 18 2025
Violation Details:
You have uploaded, shared, or distributed audio and video content owned by

Wondrous Works

without proper authorization. This constitutes an infringement of reproduction, distribution, and public transmission rights under the intellectual property laws of

America

.
Evidence Documents
We have compiled objective evidence and details regarding the violations.

You can view and verify through the following link:

Download Evidence PDF

Required Actions:
To avoid legal liability, you are required to undertake the following actions within

.
Evidence Documents
We have compiled objective evidence and details regarding the violations.

You can view and verify through the following link:

Download Evidence PDF

Required Actions:
To avoid legal liability, you are required to undertake the following actions within

7 days

from the receipt of this notice:

- Remove all infringing content from the relevant Facebook page.
- Provide a written statement confirming that you will not repeat such actions in the future.
- Send confirmation of these actions to us via the contact information below.

CommunityIT Innovators®

Fake HR Notice

Subject: File "Salary Bonus / DD Deductions.xls" has been shared with you.

You have been invited you to view a file
HR Dept shared this with you 7 days ago. If you missed it, here's a quick reminder.

DOC
Salary Bonus / DD Deductions.xls

This invite will only work for you and people with existing access.

Open
Share

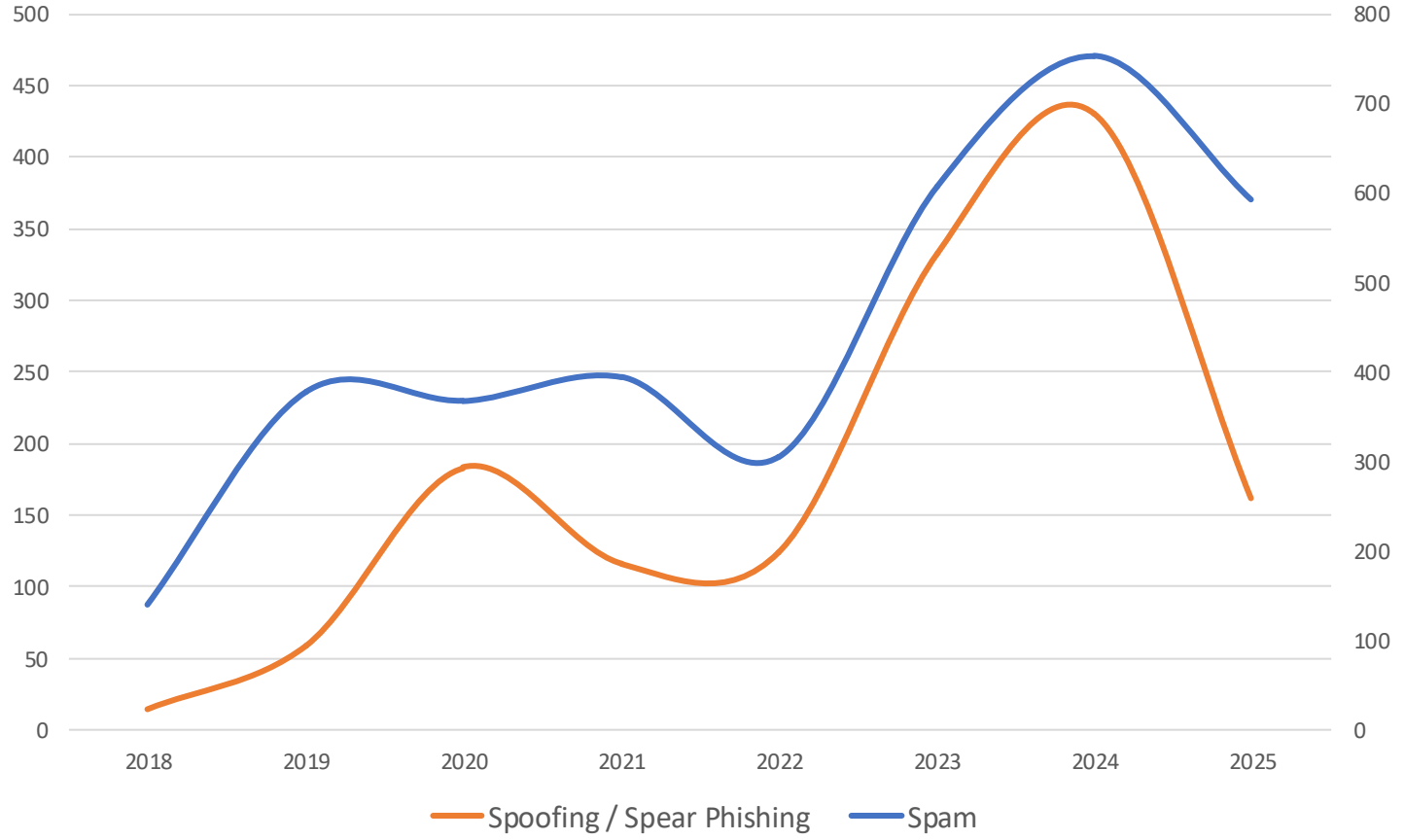
Privacy Statement

Incident Report: YoY Changes

Incident Type	2018	2019	2020	2021	2022	2023	2024	2025	YoY
Spam	140	378	368	394	305	608	753	592	-21%
Spoofing / Spear Phishing	14	59	183	116	124	333	430	162	-62%
Malware	54	50	95	45	156	76	59	101	71%
Virus	1	3	7	7	4	12	13	57	338%
Ransomware	0	0	1	2	0	0	0	0	
Account Compromise (Confirmed)	20	15	32	32	17	44	32	32	0%
Account Compromise (Suspected)				88	254	391	472	648	37%
Advanced Persistent Threat	1	1	4	9	12	8	3	6	100%
Wire fraud	3	3	0	3	8	6	3	1	-67%
Brute Force Attacks			43	64	60	177	273	203	-26%
Supply Chain	0	0	0	0	0	0	0	0	
Total	233	509	690	696	940	1655	2038	1802	76%

CommunityIT Innovators®

Incident Report: BEC & Spam



CommunityIT Innovators®

Incident Report: Trends in 2025

- Your tools are important.
- Malicious endpoint and virus activity increased.
- Most attacks are still financial not partisan.
- Insecure AI use creates new risks.

- Provide staff training
- Create clear policies for data and AI in general
- Maintaining baseline, foundational defenses helps against new threats too

Protect Your Organization

- Review or establish governance policies on:
  - IT Acceptable Use
  - Incident Response
  - AI Acceptable Use
  - Disaster Response Plan
  - Data Retention Policy
- Implement security awareness training
- Update and upgrade MFA
- Third party email filtering
- Cloud identity protection
- Patching/timely security updates

CommunityIT Innovators®

Cybersecurity Basics Checklist

All nonprofits should have the following cybersecurity policies and practices:

- An executive-level ownership of cybersecurity as a business function
- A written IT Acceptable Use Policy (maintained with your HR department). Other policies as necessary: Data policy, AI use policy, Disaster Recovery Plan, etc.
- Periodic and frequent security awareness training
- Required multi-factor authentication (MFA), upgraded to use physical keys to prevent AitM for sensitive roles such as CFO, Executive Director, HR Manager
- Password management
- Spam filtering
- Spear phishing protection
- Operating system and third-party updates and patches management
- Antivirus
- Scheduled backups, with periodic testing of ability to restore from backup
- Cyber Insurance. Contact your current policy writer to inquire about your coverage.
- If working with an MSP (Managed Service Provider), clear lines of communication about cybersecurity. This free Guide to Vetting a Managed IT Service Provider provides helpful tips. https://communityit.com/the-nonprofit-guide-to-vetting-a-managed-it-service-provider/

CommunityIT Innovators®

Community IT Cyber Offerings

- Free initial assessment and discussion
- Free online resources
- In-Depth Cybersecurity Assessment
- Managed Cybersecurity Services
- Managed Cybersecurity Training for Staff

https://communityit.com/cybersecurity/

CommunityIT Innovators®

Book time with Matthew Eshleman:

https://meetings.hubspot.com/meshleman

CommunityIT Innovators®

ABOUT US

Advancing mission through the effective use of technology.

100% employee-owned

Channel Partners™

MSP501

2025 WINNER

CommunityIT Innovators®

Mission:

Create value for the nonprofit sector through well-managed IT

Values:

- **Trust**: treat people with respect and fairness
- **Knowledge**: empower staff, clients, and sector to understand and use technology effectively
- **Service**: we seek to be helpful with our talents
- **Balance**: the health of our communities is vital to our well-being; work is only a part of our lives

Thank You

CommunityIT Innovators®

100% EMPLOYEE OWNED

25 KNOWLEDGE • BALANCE • SERVICE • TRUST

https://communityit.com

As advocates for using technology to work smarter, we're practicing what we recommend. This report was drafted with the assistance of AI, and was reviewed, edited, and finalized by a human editor to ensure accuracy.