Nonprofit Cybersecurity Incident Report by Matthew Eshleman

Emerging Trends, Practical Advice

7TH EDITION: 2025

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 7th 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 2024, and doesn't completely capture growing online harassment and threats, which have already spiked higher in early 2025. These attacks aren't focused on the traditional cybercrime motivations of the past 7 years. They are personal attacks on individuals who work at organizations with a mission that's not aligned with the threat actor's world view.

Another development in 2025 is a decreased ability to rely on data and advice from Federal institutions like the FBI and CISA, which face serious funding cuts to cybercrime prevention and community outreach.

While there is good data around cybersecurity incidents published widely, including Microsoft's Digital Defense Report, focused data on the SMB and nonprofit-specific space is lacking. Additionally, 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. 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

2024 Incidents Summary

After multiple years of increases in the number of security incidents reported across multiple categories, in 2024 we are starting to see a slowdown in the rate of reported cybersecurity incidents.

The rate of incidents reported is still alarming, with almost 500 cases of suspected account compromises occurring. However, the number of confirmed account compromises dropped by 27% compared to 2024.

Wire fraud incidents also went down in 2024. While the impacted organizations suffer, in aggregate we are seeing better training and more formal financial transaction processes put in place to prevent these fraudulent transactions.

In each case of wire fraud, the organization also experienced an internal compromised account, which was used in the commission of the wire fraud crime. We continue to urge nonprofits to implement strong security awareness training both for protecting staff inboxes and protecting secure financial processes.

CommunityIT Innovators®

What are we seeing?

More organizations are investing in security awareness training. For multiple reasons - board involvement, cybersecurity policy requirements, audit mandates or just recognizing that training is important - the number of clients engaged in training grew by almost 20% in 2024 with 10 new organizations adopting a formal security awareness training program.

Improved MFA? While “regular” MFA is still too far from being universally adopted at nonprofits, we have started to enroll finance, executive, and operations staff in roles targeted for spear phishing into stronger MFA methods. Those methods include physical security keys using the FIDO standard and built-in stronger authentication methods such as Microsoft Hello on Windows systems and Secure Enclave in macOS.

Improved tools? New email security tools and requirements are better protecting inboxes. We are seeing better performance of the tools as evidenced by fewer relative reported phishing messages and falling numbers of compromised accounts from 2023.

CommunityIT Innovators®

What's next?

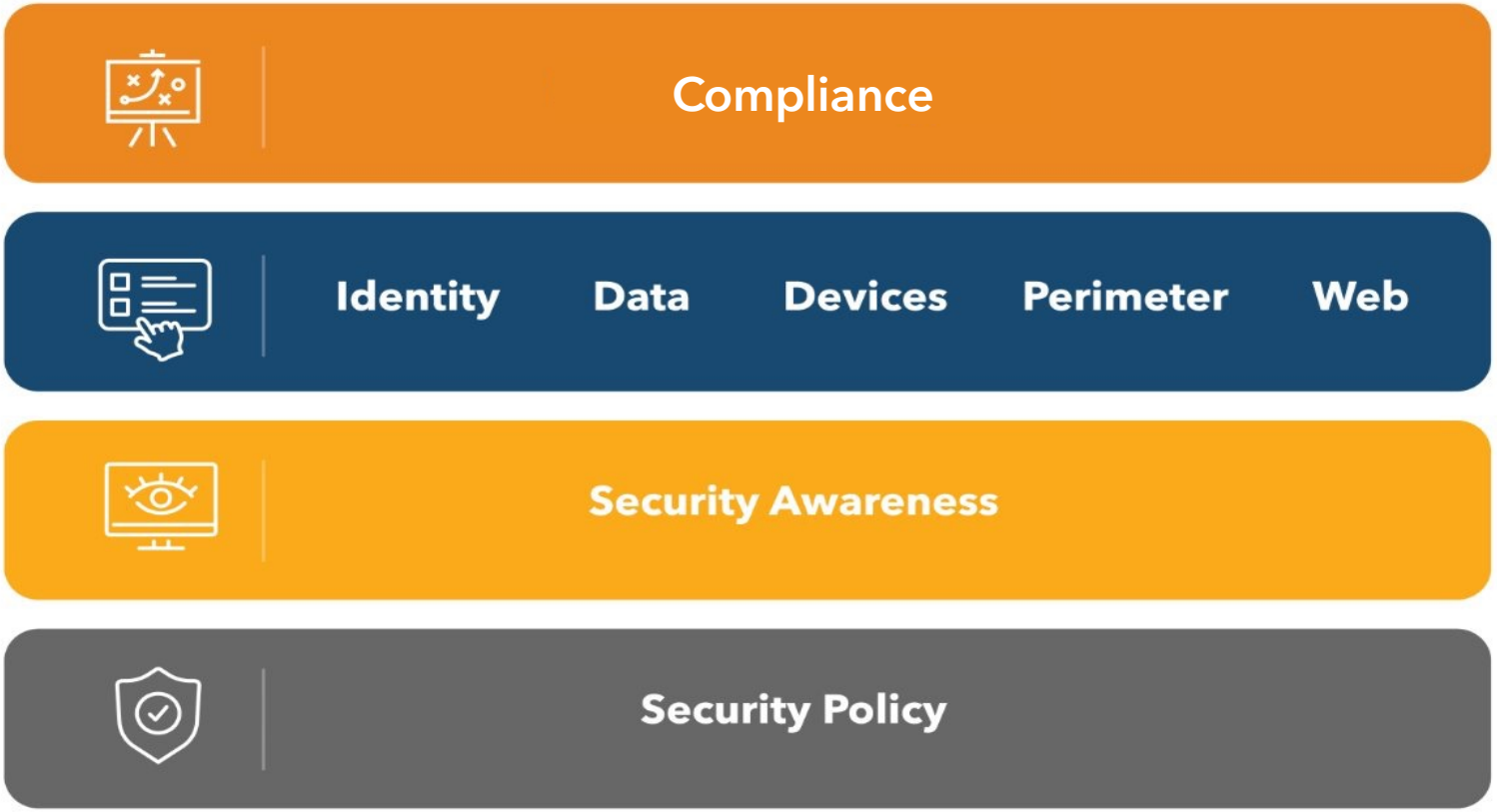
Nonprofit organizations continue to be at a high risk for cyberattacks of all types. While threats like ransomware are not as common, email attacks are a guarantee, and attacks targeting an individual's digital identity are an almost certainty as well.

Foundational controls such as an Acceptable Use Policy, formal security awareness training, phish-resistant MFA and cloud identity protection do provide meaningful protection against the most likely attacks that organizations will face. Our updated cybersecurity playbook covers this in greater detail.

Learning Objectives in this Report

- Learn our basic approach to cybersecurity
- Learn the trends in attacks and organization protections we saw in 2024
- Understand evolving security best practices
- Learn the role of governance policies and training in protecting your nonprofit from common scams

CommunityIT Innovators®



Community IT Innovators Cybersecurity Framework for Nonprofits
https://communityit.com/cybersecurity-readiness-for-nonprofits-playbook/

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
- Multi-factor Authentication (MFA)
  - MFA Push Bombing/Fatigue attack
- Credentials/Compromised Accounts
- Smishing
- Spear phishing
- Spoofing
- Ransomware
- Wire Fraud

- 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**.

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.

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.

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: scam using email impersonation to extract funds, passwords, etc., through deception. The identity of the sender is obfuscated or hidden, or appears to be a known sender, but on closer inspection includes a misspelling or unusual email. The sender knows something about you and your organization. Typically, this email includes a "call to action" like clicking on a link or buying gift cards, etc. Could also be an email that includes a link to access a document that requires a password, such as an invitation to an event or a link in an itinerary.

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.

Ransomware: A specific kind of virus that encrypts files rendering them inaccessible. A virus could encrypt all files on a computer with a key that the attacker holds. After the files are encrypted, they are unreadable. The ransomware will typically include instructions for how to contact the threat actor to pay for the files to be decrypted. That typically is done through cryptocurrency.

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 or not a payment was made, and money lost.

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 safe.

CommunityIT Innovators®

Current Cybersecurity Landscape

- Chaotic environment presents an opportunity for threat actors
- Cyber criminals see their work as a job not a hobby
- Insurance, compliance and funder mandates are driving cybersecurity adoption
- Centralized resources from FBI, CISA and Industry Partners may be eroding
- Attacks are going beyond work into personal accounts and devices

CommunityIT Innovators®

Landscape: Hacker Approach

- Generic, automated attacks, viruses, malware are routinely blocked; nonprofits remain at greater risk from targeted scams and criminal cons for $$
- Compromise/spoofing/phishing still the most common initiation of an attack
- New MFA protections aim to guard against Attacker-in-the-Middle (AitM) attacks
- Hackers take advantage of chaotic environment

Landscape: Operation Trends

- Cyberliability insurance is driving regular audits and stronger controls; SAS145 auditing requirements now include IT risk assessments.
- Artificial Intelligence (AI) is enabling new scams and new protections.
- Training offers best protection from wire fraud, phishing, doxxing, other scams
- Data policies, AI policies, and Incident Response Plans are essential to organization operation

CommunityIT Innovators®

Selected Resources:

https://communityit.com/blog-data-retention-policy-best-practices-in-uncertain-times/

https://communityit.com/blog-free-resources-for-building-it-policy-at-nonprofits/

https://communityit.com/podcast-anti-doxxing-and-nonprofit-staff-safety/

https://communityit.com/podcast-new-nonprofit-auditing-requirements-sas145/

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

https://communityit.com/template-acceptable-use-of-ai-tools-in-the-nonprofit-workplace/

https://communityit.com/webinar-cybersecurity-awareness-training-tips/

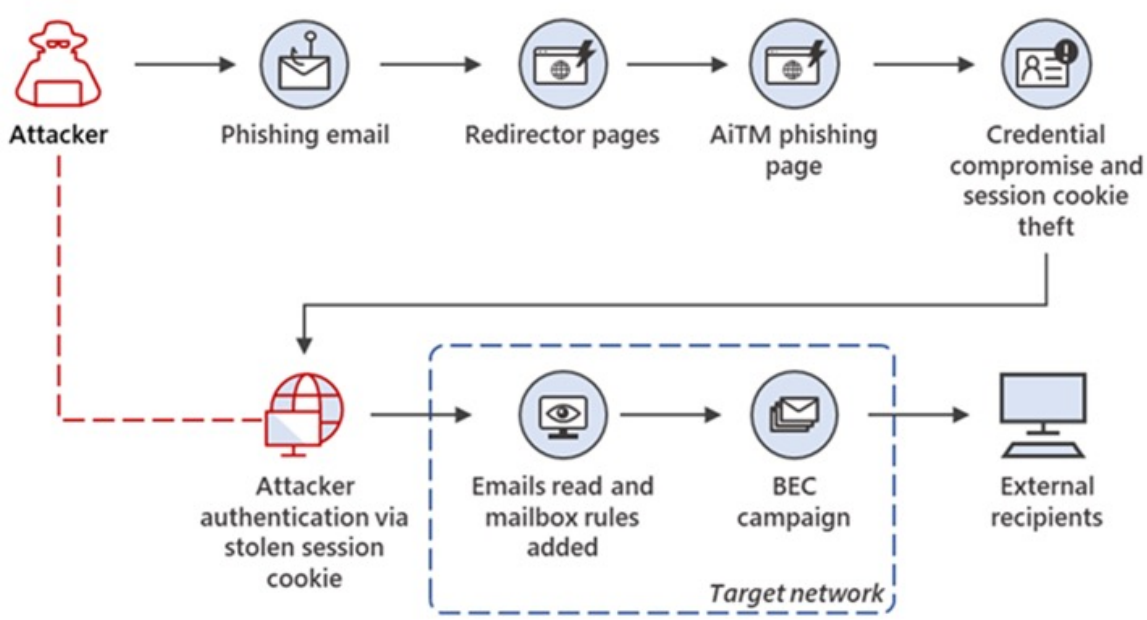
CommunityIT Innovators®

New Cybersecurity Attacks

- AI-powered phishing attacks
- AitM attacks circumvent MFA; New MFA tools
- Pastejacking
- Malicious App registration
- ShadowIT
  - Policies are ignored/not known or understood. Particularly AI.
  - Tools are purchased/adopted without IT dept input or cybersecurity protections. Particularly AI.
  - Data map and retention policies are more important.
  - Not offboarding accounts leaves security risks.

CommunityIT Innovators®

Attacker-in-the-Middle



https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

CommunityIT Innovators®

Attacker-in-the-Middle Attack Anatomy

The victim clicks on a phishing email that redirects briefly to a proxy page. **The proxy is in between your account and Office 365.**

Everything that you are going to see after the proxy looks like your official log in page, because it is your official log in page. There's just a brief moment where you can see the proxy page as you pass through it. From that point on, anything that you, the targeted user, fills in can be stolen by the threat actor.

The hacker will steal the session cookie that allows the user to authenticate, and they'll log in as the user within the timeframe that session cookie is valid. It's all automated. The hacker will then add their own Multi-Factor Authentication (MFA) method to be MFA compliant whenever they want to log in, and then they will lurk. Your network administrator may not be aware that an unauthorized additional user is present, because the hacker used the accurate MFA session token to begin the attack; administration logs will show an authorized user.

Typically, they'll work to build up into a financial attack, monitor your emails, and build an attack from there. It all starts with that malicious phishing message, clicking on a link, taking the victim through a proxy where their MFA session can be stolen.

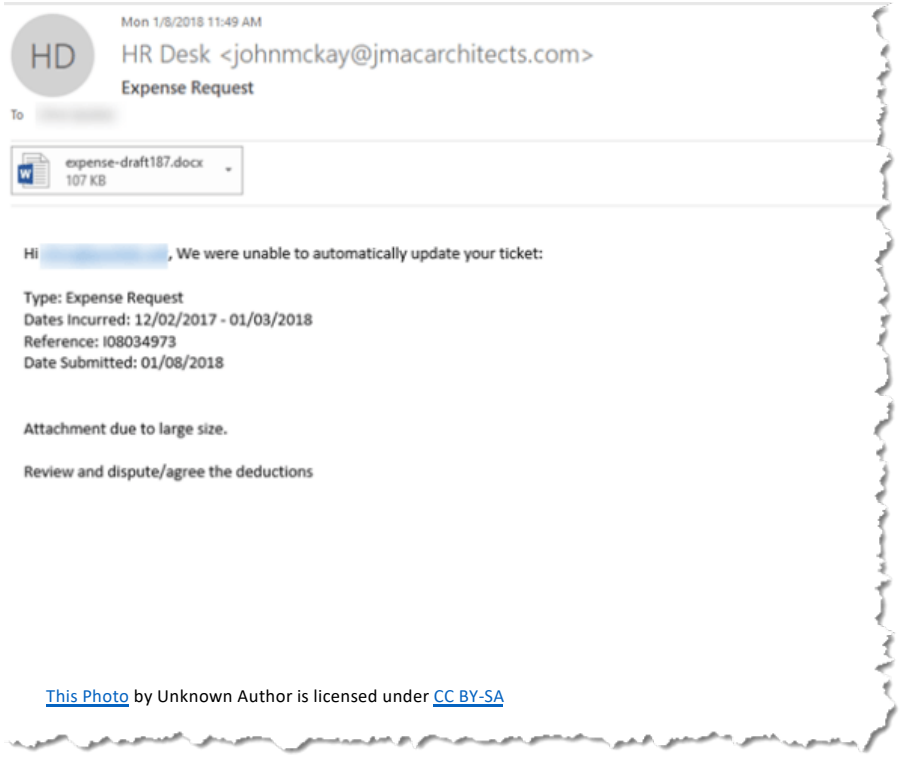
To prevent an AitM attack, you need to be very vigilant when using a link that requires MFA.
MFA is still recommended and still protects you.

For additional protection, particularly for high-risk roles such as Development, Accounts, CFO, or ED, your organization can update your MFA method to **require a physical key** like FIDO or UbiKey as your second factor. When using a physical key, the threat actor (who is remote) will not have the ability to log in to your session, because they won't have the session cookie from the physical key.

Finally, **if you see something suspicious, report it.** You may not be aware that you have been the victim of an AitM attack, but if you cultivate a healthy suspicion about scams and cons and notice anything unusual, your report will help your IT provider discover the compromised account.

CommunityIT Innovators®

Pastejacking



In a pastejacking attack, the attacker uses social engineering to convince the victim to assist in the attack against them. An email with a document is sent, and when the document cannot be opened, follow up instructions are sent to “help” the victim open the document.

The victim will be given instructions and code to paste into the “run” dialog box or will be asked to launch Windows PowerShell Terminal and paste code in to be able to open the document.

The code helpfully given by the email correspondent is of course malicious and will give the attacker access to the victim’s computer and accounts.

You should be extremely suspicious of any document that you can’t open without this extra “help.” A legitimate document will not require you to jump through these hoops, nor would a legitimate colleague ask you to take these steps for them.

Incident Report: Incident Count

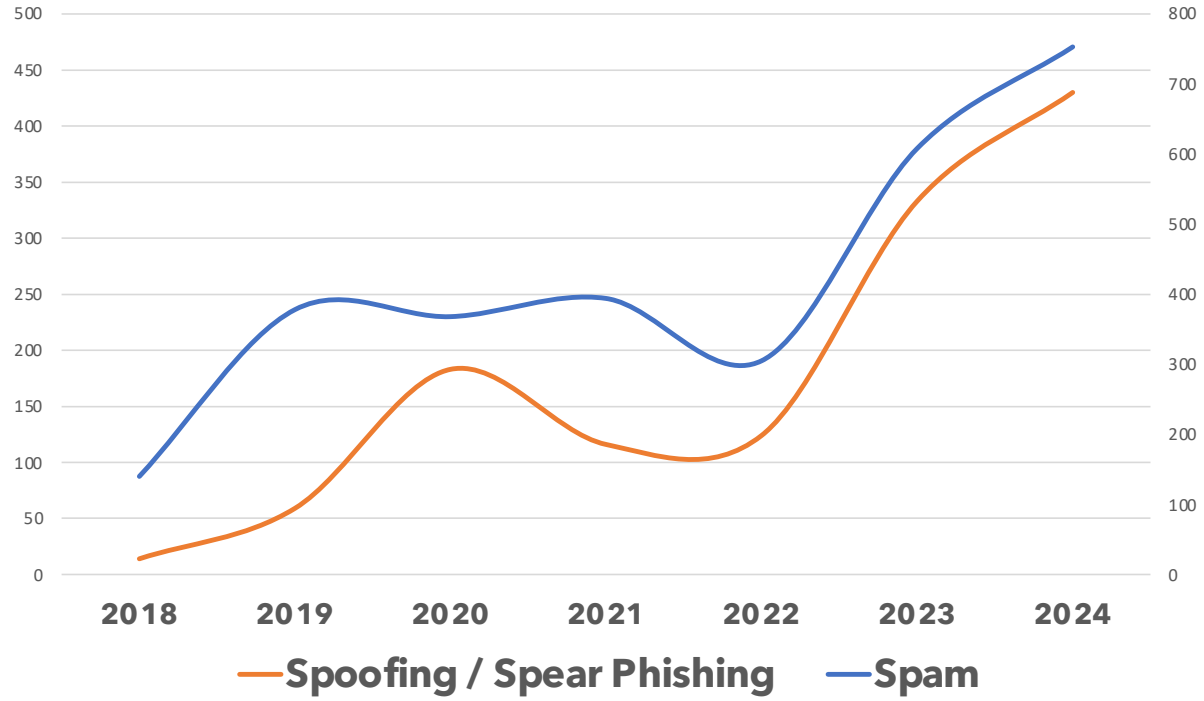
HIGH RISK THREATS	
Brute Force Attacks	273
Compromised Account (confirmed)	32
Advanced Persistent Threat	3
Wire Fraud	3
Ransomware	0
Medium Risk Threats	
Compromised Account (suspected)	472
Business Email Compromise (or spoofing)	430
Virus	13
Low Risk Threats	
Spam	753
Malware	59
Grand Total	2038

Incident Report: YoY Changes

Type	2018	2019	2020	2021	2022	2023	2024	YoY
Spam	140	378	368	394	305	**608**	**753**	**+ 24%**
Spoofing / Spear Phishing	14	59	183	116	124	**333**	**430**	**+ 29%**
Malware	54	50	95	45	156	**76**	**59**	**- 22%**
Virus	1	3	7	7	4	**12**	**13**	**+ 8%**
Ransomware	0	0	1	2	0	**0**	**0**	**0%**
Account Compromise (Confirmed)	20	15	32	32	17	**44**	**32**	**- 27%**
Account Compromise (Suspected)				88	254	**391**	**472**	**+ 21%**
Advanced Persistent Threat	1	1	4	9	12	**8**	**3**	**- 63%**
Wire fraud	3	3	0	3	8	**6**	**3**	**- 50%**
Brute Force Attacks			43	64	60	**177**	**273**	**+ 54%**
Supply Chain	0	0	0	0	0	**0**	**0**	
Total	233	509	690	696	940	**1655**	**2038**	**+ 76%**

CommunityIT Innovators®

Incident Report: BEC & Spam



CommunityIT Innovators®

Incident Report: Trends in 2025

- Maybe the peak is over?
- Email based attacks continue to increase
- Account compromises finally recede
- Staff aware of wire fraud attempts

- New tools are in place that require additional monitoring capacity
- More proactive cybersecurity solutions
- Protection needs to expand beyond the boundaries of “work”

CommunityIT Innovators®

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

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
- NIST Security Survey
- In-Depth Cybersecurity Assessment
- Managed Cybersecurity Services
- Managed Cybersecurity Training for Staff

https://communityit.com/cybersecurity/

CommunityIT Innovators®

ABOUT US

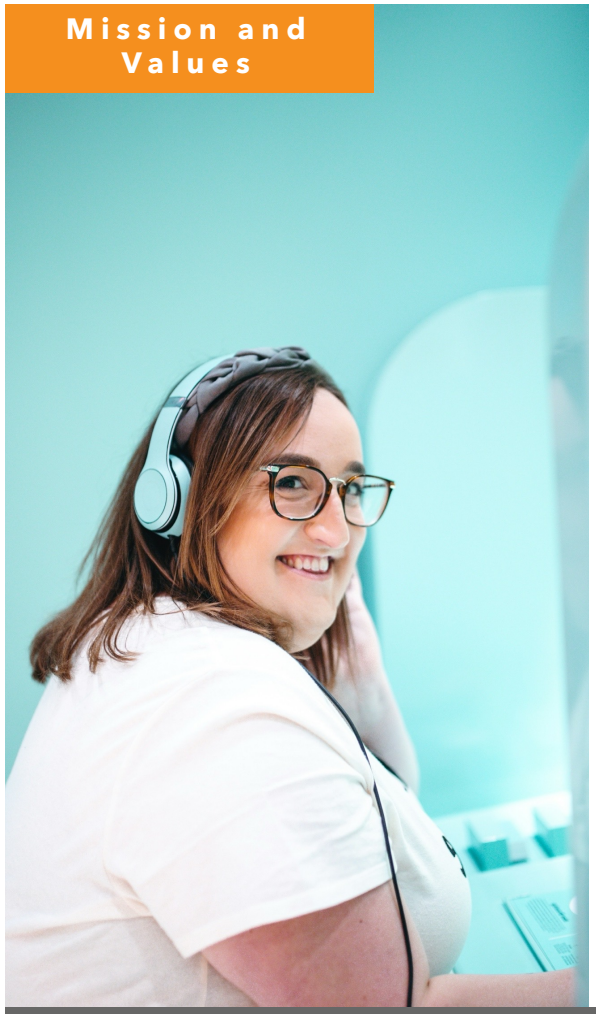
Advancing mission through the effective use of technology.

100% employee-owned

Channel Futures
Leading Channel Partners Forward
MSP 501
2024 WINNER

CommunityIT Innovators®

Mission and Values



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®

Where Technology Meets Mission

Book time with Matthew Eshleman:
https://meetings.hubspot.com/meshleman
www.communityit.com
https://www.linkedin.com/in/eshleman/