Executive Incident Report: Ohio Multi-County Phishing Attack (May–June 2025)

16 JUNE 2025

Suspected Wi-Fi Compromise at Land Records Modernization Conference, Quest Conference Center (Westerville, OH)

Executive Summary

A coordinated "multi-county phishing attack" has targeted multiple Ohio county governments in late May and early June 2025, exploiting trusted inter-county relationships to spread malicious emails. The attack was first observed by Geauga County in late May, shortly after the **Land Records Modernization Conference** (held May 20, 2025 at Quest Conference Center in Westerville, OH) – an event attended by officials from many counties. It is suspected that attackers may have **compromised user credentials via the conference's Wi-Fi or malicious QR codes**, enabling them to send phishing emails from legitimate county and organization accounts. These phishing emails were cleverly disguised as routine financial documents or invoices and appeared to come from known, trusted senders in other counties and associations. This tactic bypassed ordinary email trust filters and user suspicion, since the messages originated from **real government or organization email domains that had been compromised**.

Over a three-week period, the campaign expanded quickly across county lines. By leveraging **compromised accounts and distribution lists** – notably the County Engineers Association of Ohio (CEAO) contact list – the attackers propagated phishing emails to numerous counties. In each case, the sender's domain belonged to an Ohio county or a county-related organization, making the phishing attempts appear legitimate. Geauga County's cybersecurity team (DARC) moved quickly and aggressively to contain the threat: they **identified the phishing emails early, blocked communication with the compromised domains, and isolated affected devices**. As a result, **Geauga County sustained no internal breach** and only minimal disruptions, even as less-prepared peer counties fell victim to the attack.

This report provides a detailed narrative of the incident timeline, an analysis of how the attack was possibly executed (through conference Wi-Fi/QR code exploits), Geauga County's defensive actions, and the subsequent measures taken. It also outlines **policy changes** (such as prohibiting use of unsecured public Wi-Fi on county devices) and **forward-looking recommendations** to prevent similar incidents. Also, it announces the formation of a new **statewide IT intelligence-sharing group** led by Geauga County to improve collective defense against cyber threats. The content is intended for executive leadership, with clear non-technical explanations of technical issues and a focus on actionable insights.

Finally, and most importantly, the heart of Geauga's response has been its people. The recently formed Department of Advanced Research and Cybersecurity (DARC) team has quickly established itself as a leader and exemplar in cybersecurity response among Ohio counties. Under the leadership of DARC Director Zach McLeod, the team—which includes Advanced Security Specialist Rob Bushman, IT Physical Security Analyst Joe Birli, and Security Technician Josh Holtz—has been working tirelessly around the clock. Leveraging state-of-the-art AI-driven endpoint detection combined with meticulous human analysis and forensic investigation, the DARC team rapidly identifies, isolates, and mitigates threats. Their proactive measures include implementing comprehensive DNS and firewall-level domain and IP blocking, deep inspection for email traffic, scrutinizing email headers and logs for indicators of compromise, and conducting real-time threat correlation and containment. Additionally, they are managing credential resets, enforcing multifactor authentication, isolating compromised devices, re-imaging infected systems, and deploying advanced network monitoring tools to ensure persistent surveillance of suspicious activity. Beyond securing Geauga County's infrastructure, the team also proactively shares critical threat intelligence, actionable insights, and cybersecurity best practices with peer counties, substantially enhancing Ohio's overall cybersecurity posture and resilience.

Incident Timeline Overview

Narrative of Events: On May 20, 2025 – the day of the Land Records Modernization Conference – a Geauga County employee received an unusual email that appeared to come from a **Belmont County Health Department** account. The email, subject-lined as an invoice, contained a link and was later identified as the likely **initial phishing attempt** kicking off this campaign. It is believed that during the conference, attackers harvested one or more county officials' credentials (potentially a Belmont County attendee) by using a rogue Wi-Fi network or a malicious QR code at the venue (this attack vector is explained in a later section). Using those

stolen credentials, the adversary sent a phishing email from a trusted Belmont County email address to Geauga County on that same day (May 20). At the time, this email did not trigger alarms beyond user suspicion; however, it set the stage for the multi-county attack that unfolded in the ensuing days. We were incredibly fortunate and thankful that Geauga County had a vigilant stakeholder in the Geauga County Commissioners' Office who immediately identified and reported the original phishing attempt, enabling swift collaboration with our DARC team.

On **May 27, 2025**, Geauga County's Department of Advanced Research and Cybersecurity (DARC) received the first reported phishing email that was definitively linked to this campaign. A Geauga user reported a suspicious email appearing to come from the Belmont County Engineer's domain (`belmontcountyengineer[.]com`), also framed as an invoice and file shared request. Geauga's cybersecurity team quickly confirmed this email was malicious and **blocked the sender's domain**. This prompt containment likely prevented that phishing attempt from causing any internal damage.

As the investigation continued, Geauga DARC analysts uncovered signs that the **County Engineers Association of Ohio (CEAO)** communications had been exploited. By **June 5, 2025**, evidence confirmed that the attackers had **compromised the CEAO's email distribution list (ceao.org)** as well as multiple Belmont County email accounts/domains. This allowed the threat actors to send phishing emails widely to county contacts statewide under the guise of CEAO or Belmont officials. In response, Geauga immediately **blocked all email traffic from the CEAO domain and from all Belmont County government domains** until those entities could remediate the compromise. Geauga also identified any of its users who had received or interacted with the malicious emails; those users' devices were isolated and re-imaged as a precaution, as well as their account passwords were signed out of all sessions and passwords reset (details on remediation steps in a later section).

In the **early hours of June 6, 2025**, the threat expanded as another county was used to further the attack. **Coshocton County**'s domain (`coshoctoncounty[.]net`) was observed sending phishing emails in the same fashion. Geauga added Coshocton County's domains to the block list, cutting them off from Geauga's systems. Later that morning on June 6, **Wayne County Engineer's Office** fell victim – multiple Wayne County government domains began sending out phishing messages. Geauga similarly **blocked all Wayne County-related domains** to staunch the spread.

By mid-day **June 6, 2025**, two more counties were confirmed compromised: **Ashtabula County** and **Mercer County**. Phishing emails originating from those counties' addresses were detected, indicating that attackers had gained access to their systems as well. Geauga County moved decisively to **block every domain associated with Ashtabula County** (including court and clerk subdomains). For Mercer County, a blanket block on *all* Mercer County domains was instituted as a proactive safety measure. At this stage, Geauga's swift isolation of these domains ensured that even as the attack rapidly grew to *six* counties (Belmont, Coshocton, Wayne, Ashtabula, Mercer, plus the CEAO organization), **Geauga's systems remained safe** – no phishing email from those sources could reach county employees, and any previously affected devices/user accounts were already contained.

Throughout the timeline of May 27–June 6, Geauga County's DARC kept in close communication with peer counties and state cybersecurity resources. By June 6, Geauga's team had alerted many neighboring counties about the indicators of compromise (IOC) and steps for remediation. The **Timeline of Events** table below summarizes the key incidents and actions taken:

Timeline of Events (May 20 – June 13, 2025)

Date	Incident	Geauga County Action
May 20, 2025	Geauga receives phishing email from a Belmont County Health Dept. account (conference day). Likely initial credential compromise at conference leads to this phishing attempt.	User reported suspicious email; preliminary investigation started (email flagged but not yet linked to broader campaign). **Domain blocked.**
May 27, 2025	Phishing email received from **belmontcountyengineer.com** (Belmont County Engineer's domain) targeting Geauga user.	Geauga DARC confirms compromise; **domain blocked**. Affected user's device isolated and scanned.
June 5, 2025	Compromise of **CEAO (ceao.org)** confirmed; Belmont County's email systems found fully compromised (multiple Belmont domains abused). Attack spreading via CEAO's trusted contact list.	Geauga **blocks CEAO domain and all Belmont County domains**. All Geauga users who received Belmont/CEAO emails are contacted; their devices **re-imaged** and credentials reset as needed.

Date	Incident	Geauga County Action
June 6, 2025 (early AM)	**Coshocton County** added to threat vector – phishing emails emanating from coshoctoncounty.net and related domains.	**Blocked Coshocton County domains** (e.g. coshoctoncounty[.]net, coshcoauditor[.]org). Notified Coshocton County IT of compromise.
June 6, 2025 (morning)	**Wayne County Engineer's Office** compromised – multiple Wayne County domains start sending phishing emails.	**Blocked Wayne County domains** (e.g. waynecountyoh.gov, wayne-county-engineer.com). Geauga shares IOCs with Wayne County tech staff.
June 6, 2025 (midday)	**Ashtabula County** email systems confirmed compromised; phishing messages from Ashtabula domains observed.	**Blocked all Ashtabula County domains** (including courts and clerk sites). Reached out to Ashtabula County officials with incident details.
June 6, 2025 (afternoon)	**Mercer County** systems confirmed compromised. Mercer used to send phishing to others.	**Blocked all Mercer County domains** (full isolation of Mercer). Advised Mercer County to initiate incident response immediately.

Table: Key incidents in the phishing campaign and Geauga County's response actions.

Attack Vector: Wi-Fi, QR Code Exploitation, or Trusted Wi-Fi Hacking Attacks at the Conference

How the Attackers Breached Accounts: All signs indicate that the initial compromises stem from the **Land Records Modernization Conference** on May 20, 2025, where many county officials (engineers, auditors, recorders, etc.) gathered in one place. Cyber criminals likely took advantage of this setting by deploying a **rogue Wi-Fi network (Evil Twin)** or malicious **QR code** at the conference venue to steal login credentials from attendees. These are increasingly common tactics at public events:

- **Rogue "Evil Twin" Wi-Fi:** In an Evil Twin attack, an attacker sets up a fake Wi-Fi access point that mimics a legitimate network (for example, naming it similar to the

Quest Conference Center's Wi-Fi). Conference attendees may unwittingly connect to the stronger fake signal, thinking it's official. Once connected, all of the user's internet traffic passes through the attacker's device. The attacker can then intercept sensitive data and even present fake login pages. For instance, the attacker might redirect users to a counterfeit Microsoft 365 login portal via a captive portal trick – a **man-in-the-middle (MitM)** technique where the user is prompted to log in again to "Wi-Fi" or view conference materials. Any passwords entered (e.g. Office 365 or email credentials) are captured by the attacker. Evil Twin Wi-Fi attacks are dangerous because victims typically have no indication they're on a fake network; everything appears normal while their data (including login credentials) is being siphoned.

- **Malicious QR Codes:** The conference venue likely provided QR codes for convenience (e.g. to access digital agendas, Wi-Fi login pages, or contact info for vendors). Attackers can easily print and place their own **malicious QR code** stickers over legitimate ones or distribute them on fliers. Scanning a malicious QR code can lead a user's phone to a **phishing website** that impersonates a familiar service and asks for credentials. For example, an attendee might scan what looks like a conference survey or Wi-Fi access code, and be taken to a fake Office 365 login page where they enter their email and password – delivering those credentials straight to the attacker. Notably, security researchers have observed threat campaigns using **QR code "quishing" attacks** to harvest credentials; in one case, over 20 NGOs were targeted using QR codes that led to fake login pages, resulting in stolen cloud account passwords. Because QR codes hide the URL destination, users are less likely to spot a malicious link – making this an effective ploy in busy conference settings.
- **Hacking the Existing Conference Wi-Fi:**
  Another plausible scenario is that attackers directly compromised the legitimate Wi-Fi network at the conference venue through technical exploitation or unauthorized access to Wi-Fi infrastructure (routers or access points). By performing a Man-in-the-Middle (MitM) attack, they could intercept, monitor, and harvest sensitive credentials transmitted over the legitimate network. Victims would remain unaware because the network appeared authentic and trustworthy, yet attackers had full visibility and control over their internet communications.

Using one or any of these methods, the adversaries likely stole the email/network logins of several conference attendees on May 20. With those valid credentials in hand, they waited for an opportune moment (over the following days) to **log in to those users' email accounts** from outside and send phishing emails to other counties. The phishing messages were craftily tailored

– often referencing invoices or documents – and came from actual government email addresses, which gave them an air of legitimacy. This explains why Belmont County's domains (e.g., an account in the Health Department or Engineer's Office) were the first apparent source of phishing emails to Geauga. In effect, the attackers **turned their victims into unwitting senders** of further phishing, propagating the attack rapidly through inter-county trust channels.

For education and awareness, the key lesson is that **unsecured public Wi-Fi and unverified QR codes pose serious threats**. Connecting a work device to an unknown Wi-Fi network can open the door to credential theft, and scanning QR codes without caution can lead to compromise. These vectors allowed attackers to bypass traditional perimeter security – they didn't "hack in" through firewalls; instead, they *logged in with stolen passwords*. The next section details how Geauga County responded and contained the threat, but equally important is prevention: **avoid connecting county devices to public Wi-Fi and be wary of scanning QR codes** outside of controlled circumstances. (Policy changes addressing this are discussed later in this report.)

Geauga County's Defensive Posture and Response

Once Geauga County identified the phishing threat, the Department of Advanced Research and Cybersecurity (DARC) initiated a comprehensive incident response. Geauga's **defensive posture** prior to and during the incident has proved to be significantly more robust than that of many peer counties, which contributed to Geauga containing the attack with **zero internal damage to date**. Key elements of Geauga's defense and response included:

- **Endpoint Detection & Response (EDR):** Geauga has deployed **CrowdStrike Falcon** on county systems for continuous monitoring and threat response. This EDR immediately flagged unusual processes or malware attempts on any device that engaged with the phishing emails. Suspicious activity was either automatically blocked or rapidly investigated by the DARC team's analysts. This proactive endpoint vigilance ensured that even if a user clicked a phishing link, the payload (if any) could be contained.
- **Network and Domain Blocking:** Geauga's network security was leveraged to **filter and block malicious domains** as soon as they were identified. By adding compromised domains to blocklists at email gateways and DNS filters, Geauga **cut off inbound and outbound communication** with those domains. For example, as soon as belmontcountyengineer.com was confirmed malicious on May 27, it was blocked county-wide. Over the next week, domains from Belmont, CEAO, Coshocton, Wayne, Ashtabula, and Mercer were similarly **blacklisted** (see list of domains in the next

section). This prevented further phishing emails from reaching users and stopped any malware callbacks from infected attachments (had there been any). Multiple layers of filtering (email server rules, firewall, DNS filtering services) were used to ensure redundancy in blocking.

- **Threat Analysis and Monitoring:** DARC analysts undertook detailed **log reviews, email header analyses, and Indicator-of-Compromise (IOC) tracing** to understand the attack. They examined email metadata (e.g., sending IP addresses, email authentication protocols, timestamps) to confirm that the emails were sent via legitimate accounts (indicating account compromise). They also looked at whether any Geauga user clicked links and if so, whether any malware was dropped. Fortunately, no malware executions were detected internally – the attack's goal seemed to be credential harvesting and expanding access via email. Geauga's team also checked for any **lateral movement** inside the network and found none; the containment measures were effective.
- **User Remediation & Device Isolation:** Geauga County immediately isolated any user accounts or devices that showed signs of compromise. "Isolating" here meant **removing affected computers from the network, revoking account sessions, locking the user's account, and confiscating mobile devices** if they were potentially affected. At least one Geauga user had accessed a phishing email via their **mobile device**, highlighting the need to cover mobile threat vectors. Those devices were collected and **re-imaged (wiped and fully rebuilt)** to eliminate any hidden threats. The users were temporarily given loaner devices to continue work, and their passwords were reset. This aggressive remediation ensured that if any foothold had been gained on a Geauga machine, it was eradicated promptly.
- **Policy Updates in Real-Time:** During the incident, Geauga's IT leadership reinforced and updated certain security policies on the fly. For example, a memo was issued to all staff reminding them of the **dangers of using public Wi-Fi** and instructing them to immediately cease using any personal or conference Wi-Fi on county laptops. Plans were set in motion (later formalized; see Policy Changes section) to technically enforce this. DARC also mandated an immediate **user awareness refresher**: by early June, all county staff received a brief bulletin on how to spot similar phishing emails and were asked to report any suspicious message, even if from a known sender. These ad-hoc policy measures helped reduce the risk of any further user error during the active threat window.
- **Zero-Day Readiness:** Although this attack does appear to have involved malware, Geauga's team remained vigilant for any **follow-on payloads or unusual behavior**. Given the possibility that the phishing links could have dropped ransomware or other malware, they treated the situation as a potential zero-day event. System and application

logs were closely watched for anomalies, and extra backups were verified. This readiness paid off in peace of mind – no secondary malware was detected, but Geauga was prepared nonetheless.

Throughout the response, key DARC personnel (lead by Zach McLeod, Rob Bushman, Joe Birli, and Josh Holtz) worked in concert to monitor, contain, and communicate. They put in extended hours to ensure **total containment**, and as a result Geauga experienced **no spread of the phishing attack internally**. The contrast was stark: other counties without such dedicated cybersecurity resources were seeing their accounts abused and systems compromised, whereas Geauga remained a step ahead at each phase. This incident underscores that Geauga's investments in EDR, skilled staff, and strong policies have tangible benefits in defending against modern threats.

Impacted Entities and Blocked Domains

By the end of the incident, Geauga County had **blocked a number of external domains** to protect its network. These domains correspond to the counties and organizations that were identified as compromised during the phishing campaign. Table below lists all Counties and some other organizations that were temporarily *blocked from any email or network communication* with Geauga's systems, pending security remediation in those external entities (small businesses and organizations seen as potentially compromised are excluded from this list):

- **Belmont County**
- **County Engineers Association of Ohio (CEAO)**
- **Coshocton County**
- **Wayne County**
- **Ashtabula County Municipal Court**
- **Mercer County**
- **Seneca County**
- **Greater Columbus Convention Center**

Each of these entities was observed either sending phishing emails or otherwise exhibiting signs of compromise (e.g., being used in malicious login attempts). By blocking them, Geauga ensured no trust was given to emails or traffic coming from these sources until they could be verified as secure again. These blocks are **temporary emergency measures**. Geauga County's policy is to maintain the block until receiving **written assurance and independent confirmation** that the

affected county has cleaned the infection and secured their accounts. In essence, normal inter-county communications with these entities will remain suspended in Geauga's system until those counties confirm they have contained the threat on their side.

Geauga's action of blocking whole domains was understandably disruptive to routine business (since legitimate emails from those counties would also be blocked), but it was a necessary containment step given the circumstances. In an incident of this scope, **protecting our county's network takes priority over convenience**. Geauga has communicated these blocks to the affected counties and to state authorities, so that everyone understands the situation and can coordinate on restoring normal communications once it's safe.

Policy Changes and Enforcement Guidance

One immediate lesson from this incident is the urgent need to **tighten policies around the use of public networks and external devices**. Geauga County is implementing several policy changes to reduce the likelihood of a similar compromise in the future, with a strong focus on **eliminating unsafe Wi-Fi usage** by county personnel:

- **Ban on Unsecured Public Wi-Fi for County Devices:** Effective immediately, county employees **must not use public or unsecured Wi-Fi networks** on any county-issued device (laptops, tablets, smartphones). This includes networks at conferences, hotels, coffee shops, airports, or any network that is not explicitly trusted and secured by the County. The attack demonstrated that using open Wi-Fi can be extremely risky – attackers can eavesdrop, steal passwords, inject malware, or redirect users to fake sites. Going forward, all county mobile computers will be configured to **prevent connecting to open networks**. Technical enforcement will be achieved via device management settings: the IT department will push a configuration that disables auto-join for unknown SSIDs and prompts for administrator approval before any new Wi-Fi network can be added. Users attempting to circumvent this policy may be subject to disciplinary action, as this is a critical security mandate.
- **Use of Secure Alternatives (VPN/Hotspots):** In situations where internet access is needed on the go, employees are instructed to use **secure alternatives**. We recommend agencies provide **mobile hotspot devices** or reimburse cellular data so that staff can use either their phone's hotspot or a county-issued MiFi device instead of public Wi-Fi. Additionally, all county laptops have a **VPN (Virtual Private Network) client** installed. Policy now requires that if, in an exceptional case a public Wi-Fi must be used, the user

must immediately activate the County VPN before doing any work. The VPN ensures all traffic is encrypted and tunneled securely back through Geauga's network, mitigating the risk of local network eavesdropping. However, the preferred approach is to avoid third-party networks entirely and use trusted connectivity. This approach aligns with best practices: combining user training, VPN usage, and strong endpoint security to protect business data on the move.

- **No Scanning Unknown QR Codes:** As a related measure, a new advisory is in place about **QR code caution**. Employees should treat QR codes like unknown links – do not scan codes at events or public places unless you can verify the source. Our security training will include "**QR phishing (quishing)**" awareness. Where possible, IT will provide alternative ways to obtain resources (e.g., direct URLs) so that staff are not forced to rely on QR codes for official business. We will also investigate mobile security apps or settings that can **pre-scan URLs from QR codes** to warn users if they are known malicious sites.
- **Enhanced Device Security Policies:** We are reviewing mobile device management (MDM) policies to enforce stronger security on smartphones and tablets used for county email. This may include requiring mobile antivirus solutions, disallowing installation of unapproved apps, and ensuring device operating systems are kept up to date. Since one user's mobile phone was a point of exposure in this incident, we will improve protections on mobile endpoints. Another policy under consideration is enabling **multi-factor authentication (MFA)** for email access from mobile devices; this would make it much harder for a stolen password alone to be enough for an attacker to log in.
- **Incident Reporting and Training:** Policy is also being updated to reinforce that **unusual emails, even from trusted senders, must be reported immediately**. The quicker our team knows about a phishing attempt, the quicker we can respond (as was the case on May 27 when the user's prompt report allowed domain blocking within minutes). Regular phishing awareness training will be conducted, emphasizing that "internal" or inter-county emails can be spoofed or compromised, and showing examples of this attack (redacted) to drive the point home.

To enforce these policies, DARC will utilize a mix of **technology controls and administrative measures**. For example, network monitoring can flag if a county laptop is connected to an unauthorized Wi-Fi and automatically log or even terminate such connections. Periodic audits will be done, and compliance will be part of employee evaluations where applicable (especially for those who travel frequently or handle sensitive data). DARC has approved these policy changes and supports strict enforcement, recognizing that the small inconvenience to users is far

outweighed by the reduction in risk. Clear guidelines and help (such as providing hotspots and VPN instructions) will be given to employees to smooth the transition to these new rules.

Forward-Looking: Best Practices and Recommendations

Beyond the immediate policy changes, this incident highlights broader **best practices and areas for improvement** in cybersecurity that Geauga County and its peers should pursue. In this section, we outline several forward-looking recommendations in the areas of user awareness, mobile defense, and general cyber hygiene, to bolster our resilience against future attacks:

- **Continuous User Awareness & Training:** Humans remain the weakest link in cybersecurity, so ongoing education is critical. Geauga will implement a schedule for regular security awareness training – not just an annual video, but frequent reminders and simulated phishing exercises. Topics will include how to spot phishing emails (even those that appear to come from familiar contacts), the dangers of public Wi-Fi (reinforcing the new policy), and proper handling of unexpected attachments or links. By repeating this training and keeping it up-to-date with current threats (e.g., showing how QR code phishing works), we aim to keep cybersecurity "top of mind" for all staff. Users should feel empowered to pause and question suspicious scenarios and know exactly how to report incidents. We will also share success stories (for example, the employee who reported the Belmont Engineer phishing on May 27 potentially saved the county from a breach – this can be highlighted, anonymously if needed, to show the value of vigilance).
- **Strengthening Mobile Device Defense:** As work becomes more mobile, we need to treat mobile devices with the same level of security as desktops. This includes ensuring all county phones/tablets have device encryption, strong passwords or biometric locks, and are enrolled in our Mobile Device Management system for policy enforcement. We recommend deploying a **Mobile Threat Defense** app that can detect things like rogue Wi-Fi connections or malicious apps on the phone. Additionally, enabling phishing resistant **Multi-Factor Authentication (MFA)** for accessing county email or VPN from mobile devices is a crucial step – even if an attacker steals a password, MFA can prevent them from using it. We also advise employees to keep personal devices separate from

county work; but if they ever do access county email on personal phones, those should adhere to our security requirements too (or ideally, we discourage the practice entirely).

- **Adopt a VPN-First and Zero Trust Mindset:** With the new ban on open Wi-Fi, we want to encourage a culture of **"VPN-first"** whenever working remotely. This means users should connect through the county VPN by default, even on trusted home networks, to route traffic through a secure, monitored channel. Complementing this, Geauga will continue to advance a **Zero Trust security model** – assume no network (internal or external) is inherently safe, and continuously verify user identity and device posture. In practice, this could mean requiring authentication for sensitive systems, monitoring device health (ensuring OS and antivirus are updated) before granting access, and segmenting internal network access so that even if one account is compromised, an attacker cannot leapfrog freely to all resources.
- **Improved Incident Detection and Response Collaboration:** One takeaway is the importance of early detection. Geauga's tools and team detected the threat quickly; to further improve, we plan to evaluate additional **email security solutions** that use AI to detect account compromise or anomalous sending patterns (for example, if a user's account suddenly sends out a mass email at 2 AM, the system could quarantine those messages). On the response side, we will refine our playbooks for multi-county events – this incident was a learning experience in coordinating with external agencies. We will ensure contact lists for all county IT departments are up to date and that we have a streamlined process to notify others (possibly through the new intelligence-sharing group described next). Speed is paramount in such scenarios; the faster all parties are aware, the faster we can collectively shut down an attack.
- **Regular Security Audits and Drills:** To maintain readiness, Geauga will conduct periodic **penetration tests and phishing drills**. We will test whether our systems could detect and stop a similar attack if, say, an unknown rogue Wi-Fi appeared near our offices or if staff receive phishing from a compromised external partner. These exercises will reveal any gaps in technology or training so we can address them proactively. We will also encourage other counties to do the same, perhaps in a coordinated fashion via the new intel-sharing consortium.
- **Leverage Threat Intelligence and Sharing:** Staying ahead of attackers means knowing their tactics. Geauga will invest in threat intelligence services or subscriptions (for example, sources that alert us to government-targeted phishing campaigns, newly discovered malware, etc.). More importantly, we will contribute our own findings (IOCs, attack details) to state and federal cyber centers like the MS-ISAC (Multi-State Information Sharing & Analysis Center) so that broader communities benefit from our

experience. The forthcoming multi-county IT intel group will facilitate much of this exchange at the state level.

- **Phishing-Resistant Multi-Factor Authentication (MFA):** Implementing phishing-resistant multi-factor authentication is a vital step to protect county systems, especially in light of credential-stealing attacks. This form of MFA provides an extra verification step that attackers cannot easily trick or intercept, so even if an employee's password is stolen through phishing, the thief is still blocked from accessing the account. Unlike basic two-step methods such as email or text-message codes – which attackers can sometimes hijack or persuade victims into revealing – phishing-resistant MFA relies on more secure checks, like a trusted app prompt or physical security token that only works with the genuine system. These stronger authentication methods ensure that employees are confirming their login through a means that cannot be replayed by a fake website or imposter. By upgrading to phishing-resistant MFA, the county greatly limits the damage that a phishing scam can cause; a stolen password alone would not be enough to breach sensitive networks or data. This significantly strengthens account security and provides leadership with confidence that an additional barrier stands in the way of any attacker trying to misuse stolen credentials.
- **Cyber Hygiene and Training Away from Government Facilities:** Strong cybersecurity practices must be maintained consistently by staff, no matter where they are working. Being away from government facilities – whether at home, on the road, or at a conference – does not reduce the risk of cyber threats. In fact, remote and travel scenarios often introduce new vulnerabilities, such as using home or public internet connections that lack the county's network protections, or exposing devices to theft or unauthorized access. Therefore, employees are expected to follow the same security protocols off-site as they would in the office. This includes using only approved, secure devices for work, keeping those devices updated with the latest patches, and connecting through secure networks or VPNs when handling county information. Staff should remain just as vigilant with emails and attachments at home as they are at their desks, thinking twice before clicking on links or downloading files. When traveling or attending conferences, they must also guard their laptops and phones closely, avoid using untrusted USB drives or public charging stations, and be mindful not to discuss or display sensitive information in public areas. County policies should clearly state that cybersecurity rules apply universally, regardless of location, and it's important that regular training refreshers reinforce this mindset. By ingraining good cyber hygiene habits and awareness that extend beyond the office, the organization reduces the likelihood that an off-site moment of carelessness could lead to a security breach.

By implementing these best practices, Geauga County aims not only to shore up its own defenses but also to set a benchmark that other counties can follow. Cyber threats continue to evolve, and we must evolve with them, fostering a culture of security that extends from each individual user to the highest levels of county leadership.

Launch of Statewide IT Intelligence-Sharing Group

In the wake of this incident, Geauga County is taking a lead role in improving inter-county cybersecurity collaboration. We are announcing the formation of a new **high-level statewide IT intelligence-sharing group** focused on government cybersecurity. This initiative stems from the clear observation that **better information sharing could have slowed or even prevented the spread** of the phishing attack across counties. While Geauga's team was quick to identify and block malicious senders, not all counties had the same capability or awareness in real-time. By the time official alerts circulated through traditional channels, the attackers had already pivoted to new counties. We aim to change that going forward.

Group Purpose and Scope: This new group will serve as an **early warning and rapid communication network** for county IT departments and security officers in Ohio. When any member detects a cyber threat (phishing campaigns, malware outbreaks, suspicious network activity) that could potentially affect others, they will use the group to immediately share indicators of compromise, descriptions, and recommended actions. The goal is to **proactively notify** all members so they can check their own systems and if necessary, block or defend against the threat before it strikes them. In essence, if a similar multi-county attack happens in the future, a single email or message to this group from the first impacted county could alert everyone else within minutes, not days.

Leadership and Participants: Geauga County, given its robust response in this incident, will **lead the group initially**. The Department of Advanced Research and Cybersecurity (DARC) has been coordinating the group's activities and communications. We have invited several counties with strong IT capabilities to be the initial core participants. As of now, **Ashtabula, Stark, Franklin, and Mercer Counties** have agreed to join as founding members of this intelligence-sharing network. Each of these counties will designate a primary cybersecurity point-of-contact (and a backup). Stark and Franklin Counties (home to major urban centers) bring extensive experience and resources that will be valuable to the group, while Ashtabula and Mercer – both

directly impacted in this phishing incident – are eager to improve their defenses and share their lessons learned. Of course, the group will quickly expand to include **all interested Ohio counties**; our aim is inclusivity and statewide coverage. We anticipate involving state government IT security liaisons as well, to ensure alignment with state-level initiatives and support from agencies like the Ohio Cyber Reserve or Homeland Security.

Structure and Communication: Initially, the group will operate informally via a secured email listserv or messaging platform (e.g., an encrypted chat channel) restricted to verified members. Geauga's DARC will publish brief **threat intelligence reports** as needed, and any member can submit an alert to everyone. In the near future, we plan to hold **quarterly virtual meetups** to discuss trends and possibly in-person annual meetings coinciding with events like the CEAO conference (with a new emphasis on cybersecurity).

Benefits: The benefits of this collaboration are significant. As noted in Geauga's incident report findings, Geauga's capability to identify and contain threats was stronger than many peers – *"Geauga's cybersecurity posture is significantly stronger than many of its peers… We would be similarly situated as other counties without our security team,"* DARC noted. By leading this group, Geauga can help uplift other counties' security postures by sharing knowledge and tools. Conversely, Geauga will also benefit from others' perspectives and from early warnings if another county sees something unusual. Cyber threats do not respect jurisdictional boundaries, so our defense cannot remain siloed. This group effectively creates a **united front** across Ohio counties, turning what was previously a series of isolated IT departments into a more cohesive network akin to an immune system – when one part detects a virus, the whole system can respond.

Initial steps for the group include drafting a charter, setting confidentiality rules (since sensitive incident information will be shared), and establishing a secure communication method. These are underway and will be communicated to all county IT leaders in the coming weeks. Geauga County is committed to providing leadership and any needed resources to kick-start this effort. We are also reaching out to the **County Auditor's Association of Ohio**, **County Commissioners Association, and CEAO** to back this initiative, as their endorsement will encourage participation from all counties.

County Auditor's Association of Ohio Involvement: Auditor Charles Walder proactively engaged the County Auditor's Association of Ohio (CAAO) very early in the incident, promptly issuing a statewide notice bulletin. This timely communication enabled CAAO to rapidly inform

all Ohio auditors, significantly enhancing statewide awareness and cooperation during the response. The County Auditor's Association of Ohio (CAAO) must be formally included in all intelligence gathering efforts and security planning moving forward. Each Ohio County Auditor holds statutory authority over the county's financial systems and also plays a leading role in the county's Automatic Data Processing (ADP) Board, which oversees information technology and record-keeping infrastructure. This means Auditors have direct oversight and responsibility for critical data systems and fiscal operations at the county level. By involving CAAO in the incident response and future cybersecurity planning, counties ensure that any security improvements align with legal mandates and operational realities. Moreover, tight integration with CAAO leverages the collective expertise of all 88 county auditors, enabling more effective coordination and threat intelligence sharing across county lines – an essential factor when confronting a phishing campaign that targeted multiple jurisdictions simultaneously. In short, the Auditors' oversight of financial and IT systems makes their participation indispensable for implementing robust, compliant defenses and a unified response.

Ultimately, the creation of the statewide IT intelligence-sharing group is a proactive positive outcome from an otherwise damaging incident. It transforms our collective approach from reactive to proactive. By learning from each other and acting in unison where possible, Ohio's counties can significantly reduce the likelihood and impact of future cyber attacks. Geauga County is proud to lead this charge and looks forward to working closely with Ashtabula, Stark, Franklin, Mercer, and many other counties in safeguarding our digital infrastructure.

Conclusion

The **multi-county phishing attack** that unfolded starting in late May 2025 stands as one of the most extensive cybersecurity incidents to hit Ohio's local governments in recent memory. What began as a stealthy compromise of a few accounts at a conference quickly escalated into a statewide campaign, undermining the trust model of inter-governmental email communications. However, Geauga County's experience throughout this episode demonstrates that rapid detection, decisive action, and strong in-house expertise make all the difference between a contained event and a full-blown disaster. Thanks to early reporting by vigilant staff and the DARC team's aggressive containment strategy, Geauga **suffered no internal breach and minimal operational impact**. In contrast, counties that lacked such defenses found their domains being weaponized by attackers – a cautionary tale for investing in cybersecurity.

This incident has illuminated several critical points: **(1)** the importance of securing seemingly benign channels like conference Wi-Fi and cross-county communications, **(2)** the efficacy of a well-prepared defense (EDR, filtering, user training) in stopping an attack in its tracks, and **(3)** the need for collective resilience through information-sharing and uniform policies. Geauga County is taking these lessons to heart. By banning public Wi-Fi on county devices and tightening other policies, we are directly addressing the root vulnerability that led to this attack. By championing best practices and user education, we aim to make every employee an informed ally in cybersecurity. And by launching the new intelligence-sharing group, we acknowledge that we are stronger together – an attack on one can be a warning to all, if we communicate effectively.

Executive leadership should recognize that cybersecurity is not merely an IT issue, but a fundamental operational risk that demands attention at all levels. The response to this incident has required inter-department cooperation, support for urgent policy changes, and transparent communication with various stakeholders. Moving forward, continued support and resources will be needed to implement the recommendations in this report: from technology investments (VPNs, mobile defense tools) to training time and possibly staffing enhancements to maintain our security edge.

Geauga County's handling of the CEAO phishing campaign is ultimately a **success story in incident response thus far**. It showcases how a combination of the right tools, skilled people, and swift decision-making can neutralize a threat that was actively exploiting numerous governments. Our county has emerged as a leader in cybersecurity readiness, and we are committed to helping other counties improve their defenses as well. While we hope not to see another incident of this magnitude, we must stay **vigilant and prepared**. This report should serve as both a record of what transpired and a roadmap for future prevention. By learning and adapting, Geauga County and its peers will be far better positioned to face the next cyber threat, whatever form it may take.

Ongoing Vigilance:

It is critical to emphasize that we are treating this cyberattack as still active and ongoing. While Geauga County has effectively contained the initial impacts, we cannot yet conclude that the threat has fully subsided. Attackers retain access to extensive contacts, particularly through compromised accounts within the County Engineers Association of Ohio (CEAO), which could facilitate additional waves of phishing. We may be through only the initial wave, or potentially still in the midst of it, with subsequent waves possibly yet to come. Continued vigilance and heightened awareness remain absolutely essential. Staff and security teams must remain cautious and proactive, refusing to let down our guard until this incident is conclusively resolved.

Sincerely,

Frank Antenucci, Esq.

Chief Deputy Administrator
Geauga County ADP Department of Information Technology
12611 Ravenwood Dr., Ste. 327, Chardon, Ohio 44024
O: (440)279-1993 E: fantenucci@geauga.oh.gov
Help Desk (440) 286-4357 helpdesk@co.geauga.oh.us