When Systems Go Dark: Communicating through a Municipal Cyberattack

LOCAL

326

attacks impacted municipalities, law enforcement agencies, and other public safety organizations in 2024.

STATE

35

states said malicious code was a top 3 cause of cybersecurity incidents in the last 12 months.

FEDERAL

30,659

information security incidents were reported by federal agencies in FY 2022.

2. TEXAS SNAPSHOT

LOCAL INCIDENTS

93

local government entities in Texas experienced cybersecurity incidents requiring DIR assistance or guidance since September 2023.

PHISHING PRESSURE

+224%

more suspected phishing emails were analyzed by DIR than in the previous biennium.

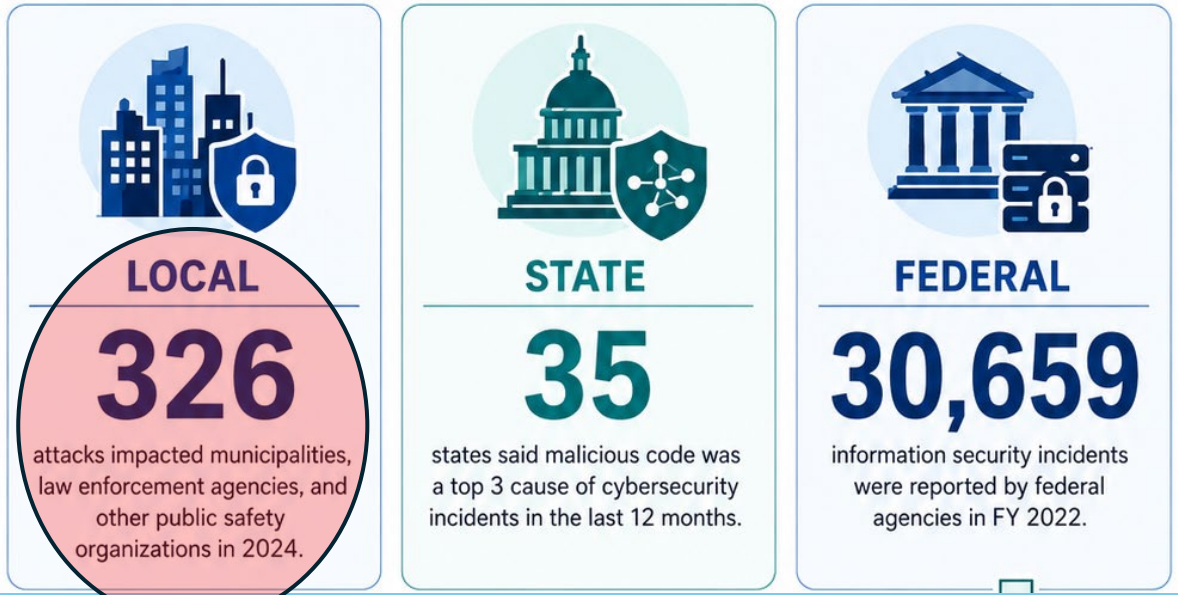
TOP LOCAL ATTACK TYPE

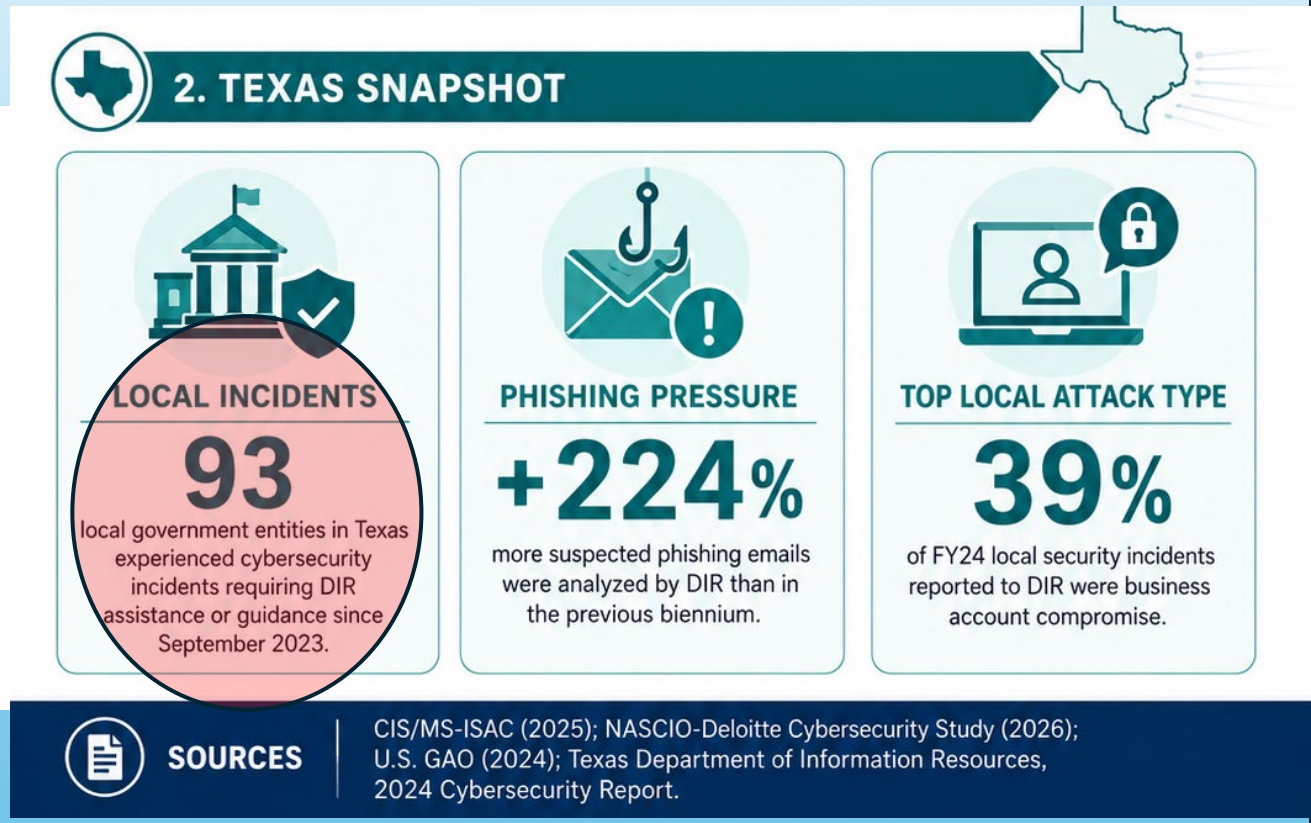
39%

of FY24 local security incidents reported to DIR were business account compromise.

SOURCES

CIS/MS-ISAC (2025); NASCIO-Deloitte Cybersecurity Study (2026); U.S. GAO (2024); Texas Department of Information Resources, 2024 Cybersecurity Report.


LOCAL
326
attacks impacted municipalities, law enforcement agencies, and other public safety organizations in 2024.
STATE
35
states said malicious code was a top 3 cause of cybersecurity incidents in the last 12 months.
FEDERAL
30,659
information security incidents were reported by federal agencies in FY 2022.


2. TEXAS SNAPSHOT
LOCAL INCIDENTS
93
local government entities in Texas experienced cybersecurity incidents requiring DIR assistance or guidance since September 2023.
PHISHING PRESSURE
+224%
more suspected phishing emails were analyzed by DIR than in the previous biennium.
TOP LOCAL ATTACK TYPE
39%
of FY24 local security incidents reported to DIR were business account compromise.
SOURCES
CIS/MS-ISAC (2025); NASCIO-Deloitte Cybersecurity Study (2026); U.S. GAO (2024); Texas Department of Information Resources, 2024 Cybersecurity Report.

“You just don’t understand how many things are tech-based in your world until this happens.”

“As a comparison, it’s like you’re being held hostage, and you can’t tell anyone.”

Mari Cockerell
Communications and Marketing Director at City of Abilene

Kelli Lewis
Marketing Director at City of Carrollton

Lacey Rose
Director of Communications & Public Engagement

What do you do?

10.10.19

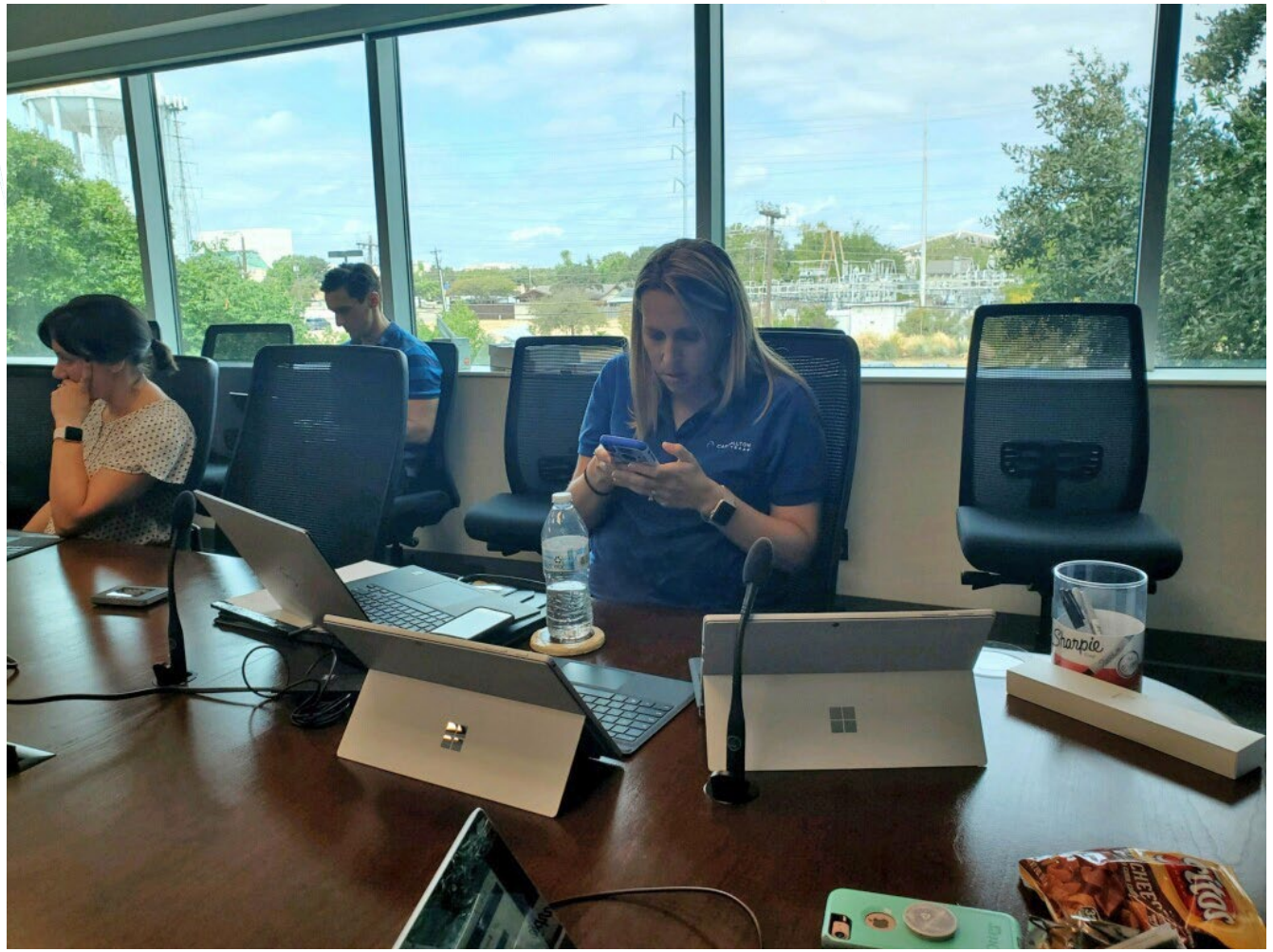
Where Connections Happen

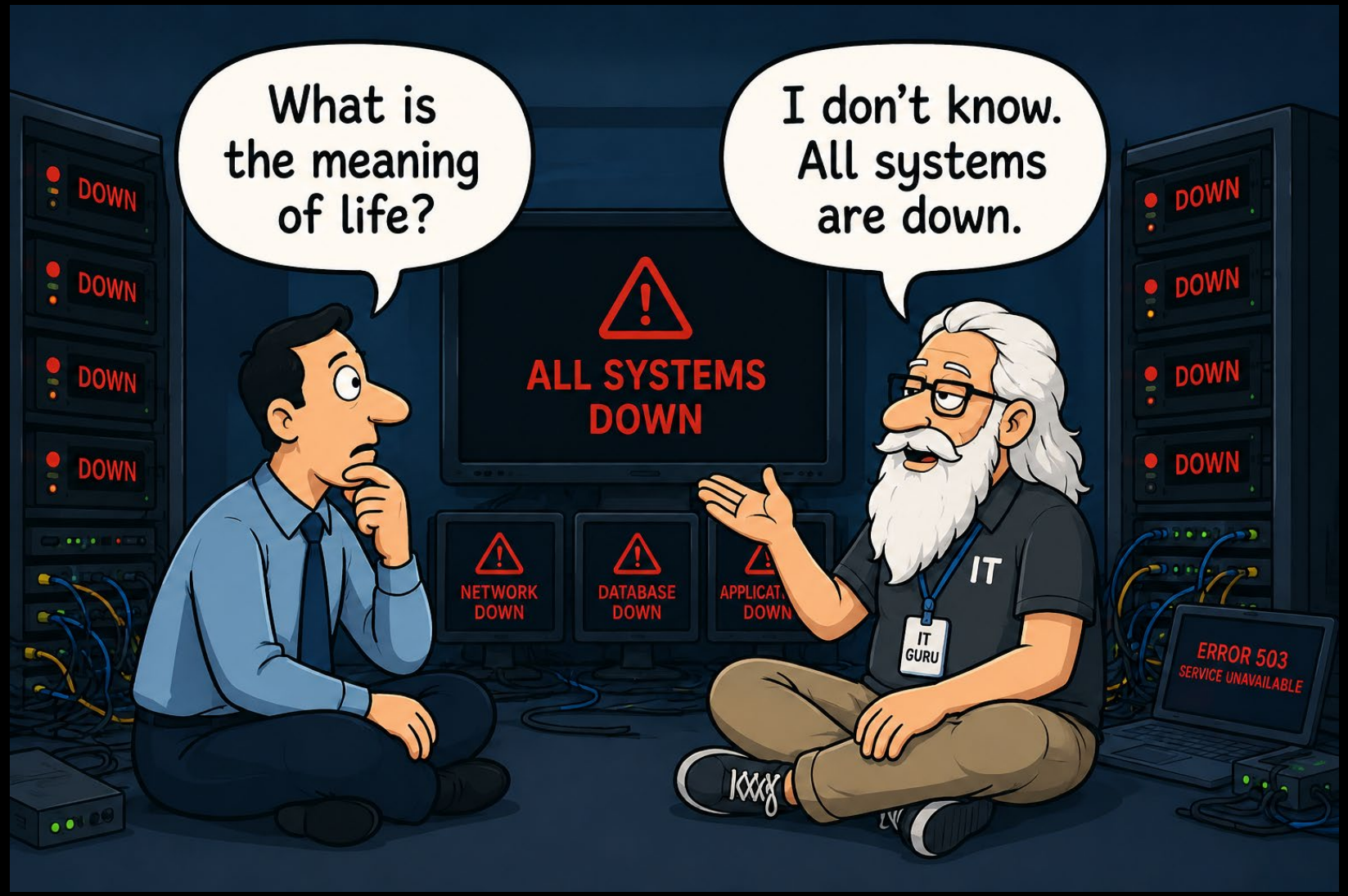
CARROLLTON
TEXAS

Impact

Full Network

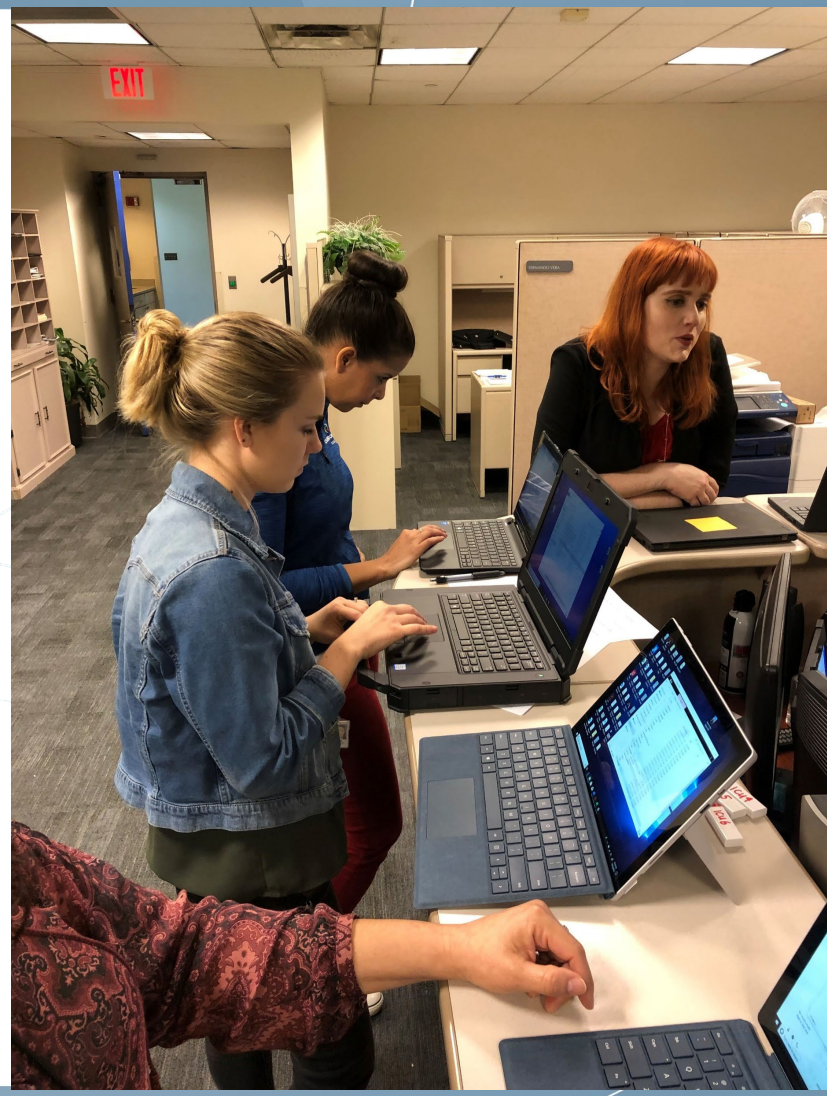
- Email
- Website
- Phones & Voicemail
- Account Access
- All Computers




What is the meaning of life?
I don't know. All systems are down.
ALL SYSTEMS DOWN
NETWORK DOWN
DATABASE DOWN
DOWN
DOWN
DOWN
DOWN
DOWN
DOWN
DOWN
DOWN
IT
IT GURU
ERROR 503
SERVICE UNAVAILABLE

Computer Assessment

- All computers considered infected until checked
  - Deployed new devices
  - Smiley sticker system



Kelli Lewis
To Susan Prosoco

Reply | Reply All | Forward

Tue 10/22/2019 10:11 AM

Yes. All devices must be stickered or they will take them away. If the surface doesn't have a blue sticker, take it to the help desk and they will give you one. We need EVERY device in our department stickered in some way.

Initial Messaging

Carrollton, TX - City Government
October 10, 2019 ·

At approximately 5 a.m. today, Thursday, Oct. 10, the City of Carrollton's network experienced a cyber attack. Public safety response and Carrollton's 911 emergency response are unaffected, however, some City services have been impacted. Currently, we have no reason to believe resident information has been accessed or will be affected. Water, sewer, and trash services are running on schedule and most residents shouldn't experience any interruptions. The City is working with state and federal officials on the investigation and will aggressively pursue prosecution of this criminal act to the fullest extent of the law.

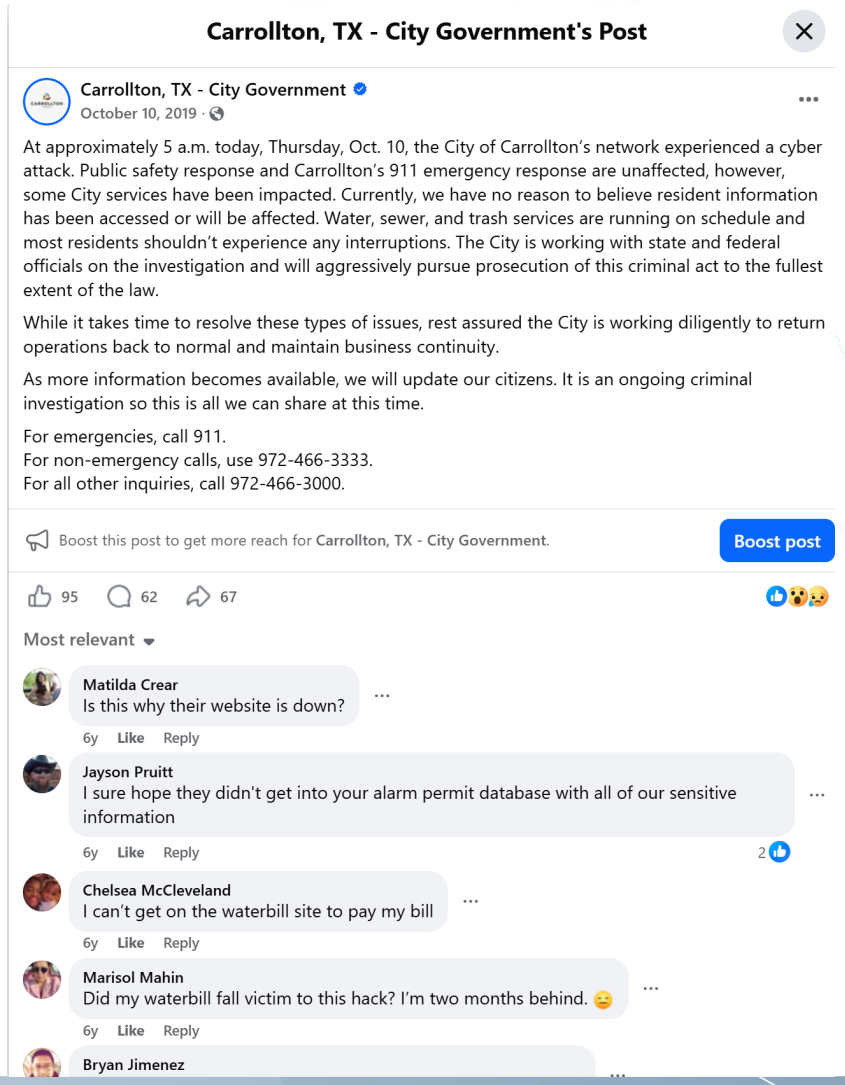
While it takes time to resolve these types of issues, rest assured the City is working diligently to return operations back to normal and maintain business continuity.

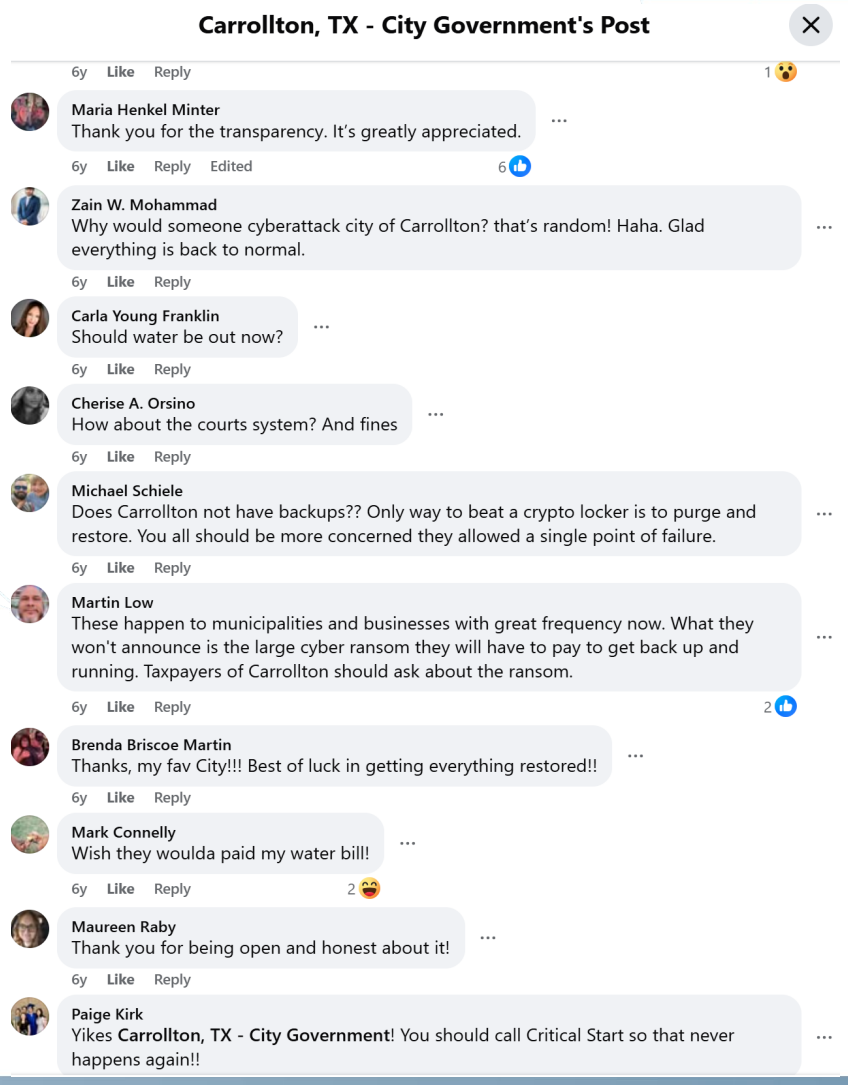
As more information becomes available, we will update our citizens. It is an ongoing criminal investigation so this is all we can share at this time.

For emergencies, call 911.
For non-emergency calls, use 972-466-3333.
For all other inquiries, call 972-466-3000.

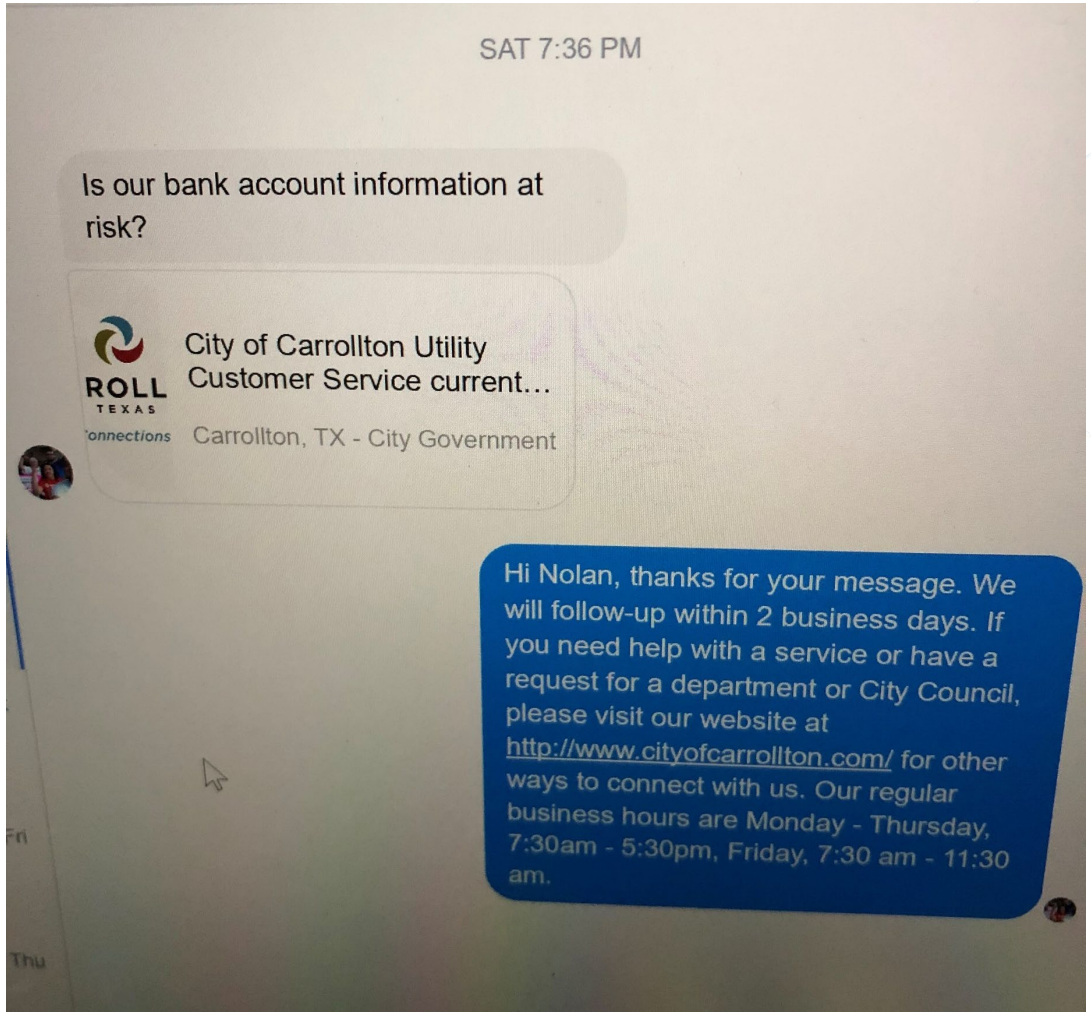
95 62 67

Citizen Response & Investigation





Citizen Response & Investigation



Rebuilding the Website

- On-prem vs Cloud
- Built Splash Page
- Rebuilt Pages
  - Wayback Machine
  - Staff in the EOC

Email

- All Email Lost
  - Yahoo & Gmail
  - Office 365 Licenses Deployed

Email

FW: O365 Users

Kelli Lewis
To Marketing Services

Reply | Reply All | Forward

Mon 10/21/2019 8:36 AM

Users.xlsx
31 KB

Marketing is on the list for having been set up this weekend. We should all be in the system now. See Andy's message below.

Subject: O365 Users

Good afternoon!

The following folks have been set up in 365. We still have a few more licenses to hand out, but we will need to buy a new chunk next week. I am now able to remotely add users to the system if any critical needs arise. Please pass this on to the necessary parties. Only about 80 users have actually gone in and signed in for the first time, so far. Users can actually set themselves up via web here, if they are so inclined: www.office.com .

Passwords are the password each user had prior to the incident last week.

Over the weekend, users who are actually working can call Dillon McVicar for setup. Next week, we should have the "Genius Bar" open again.

Dragging On

Jon,

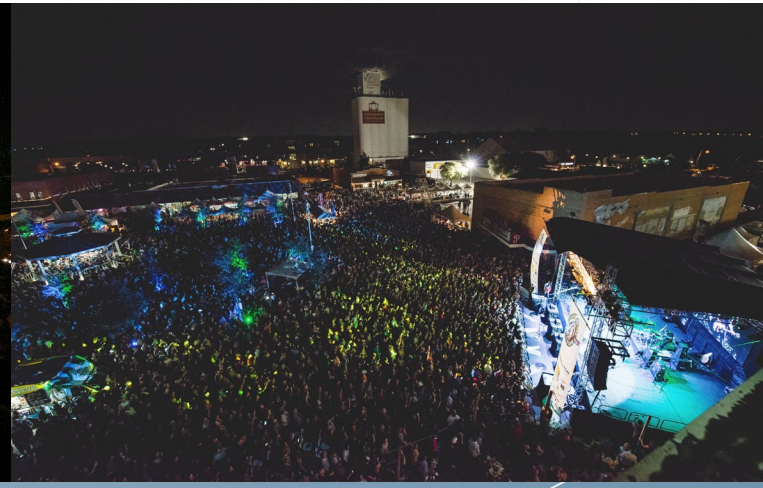
The City still doesn't have functioning email. Mine is turned on, but it's just a test right now and not fully functional (meaning I don't get all of them) so we can't count on it yet. Nobody else on my team has theirs turned on yet as the cyber team goes through scrubbing everything. I've included the carrolltonmarketing@yahoo.com email so that April can see this.

Thanks,
Kelli

Hi Scott,

The City experienced a cyber attack and we currently do not have functioning City email. I know you have several of us from the City of Carrollton on your list, but currently I'm the only one with email that is functioning appropriately and mine just came online yesterday and is still in test. We are in disaster recovery mode in Carrollton, so please don't remove us from your list but be aware the emails won't be back on just yet.

Thanks!
Kelli Lewis
City of Carrollton
Marketing Director

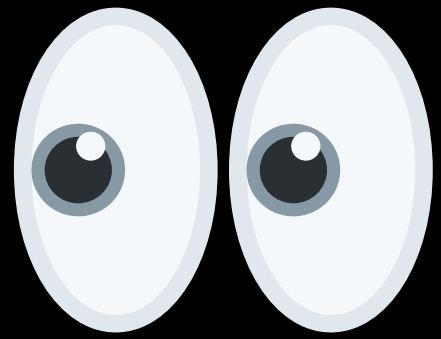


Lessons Learned

- Prioritize IT
- Cloud-Based with Redundancy & Resiliency
- Create City Business Continuity Plan, Policy, & Review Group
- Hard Copy Backups
- Pen & Paper Options
- Advance Discussion: Pay or Not


April 18, 2025
CITY HALL
555


BULLS
91



4/21/2026 All Employee Email:

Greetings, everyone!

Returning to work this morning, a lot of our team is becoming aware of a cyber event that occurred over the weekend, and the work being done to address it.

On April 18, 2025, City officials received reports of unresponsive servers within our internal network and immediately began executing our incident response plan and disconnecting affected and critical assets to secure our systems. We also launched an investigation and engaged industry-leading cybersecurity experts to determine the nature and scope of the incident and notified relevant authorities.

Our IT Department has worked around the clock to successfully restore our services to minimize downtime and the impact on our operations. Our investigation is ongoing, and we continue to closely monitor our systems for any unusual activity. Out of an abundance of caution, certain systems have been taken offline. However, emergency services are still up and running with the continued ability to timely assist, and no unidentified financial activity has been detected.

We are in the early stages of our investigation. Anyone who has experienced a cyber incident knows it is a time-intensive process. Every week, we will learn more about the scope of the incident and will communicate additional details as our investigation progresses. We take the security of our systems very seriously and appreciate your patience and understanding as we work diligently to restore our systems and resources.

We'd like to remind everyone that media or public inquiries in this situation, just like any other instance, should always be directed to mediarequest@abilenetx.gov. If you are contacted by news media or anyone outside of the City organization requesting information, please ask them to send their inquiry to mediarequest@abilenetx.gov. Feel free to utilize this response:

Thank you for your inquiry. I'm not the right person to speak with you about this matter, but if you could email your request to mediarequest@abilenetx.gov, our Communications Department will be happy to assist.

Thank you for your service and help as we move forward!

May 21-ish, 2026 Media Communication:

Media partners -

We can confirm the information included in the Comparitech article dated May 19, 2025 in regards to the cyber incident and demands made by the ransomware group, Qilin, is accurate. (Link to article)

The City of Abilene has been working with cyber security professionals since the incident began on April 18th and, given their expert direction along with adherence to the City's organizational values and standards, determined the payment of any kind of ransom to criminal or terrorist entities of this sort would not take place.

At this time the City is still limited in its ability to comment on the incident as the investigation continues and discovery efforts follow. We can, however, assure residents that City leadership is keeping close track of the cost of the incident and how those funds will be recovered. City leadership is also closely following any impact the cyber incident may have on personal information, and is prioritizing notification to individuals along with educational tools and resources.

The City of Abilene understands various aspects of functionality across several departments and services has been affected by the network outage that followed the cyber incident, and we sincerely apologize for the frustration and disruption this has caused. Our employees are working diligently to continue serving our community, and we greatly appreciate everyone's patience and understanding.

As stated previously, we look forward to sharing more information on the cyber incident as soon as the investigation concludes and we are able to do so.

6/2/25 All Employee Email:

Hello, City of Abilene team!

As many employees have likely noted from local news media reports, the past couple of weeks marked a milestone of sorts in our journey following the cyber attack and network shutdown of April 18. The hackers who infected our network with ransomware posted on the dark web that the City had a May 27 deadline to send payment in order to prevent the release of data stolen by the group. The City did not pay the hackers any money, and the deadline was allowed to pass.

Due to that situation and the investigation taking place prior to May 27, the City had been very limited in its ability to communicate details about the attack to the public and employees. With the deadline behind us, we are grateful to be able to share more information about the incident with the organization and the community.

This news release has now been posted on our website and social media channels, and explains the incident, its effect, and more about the data affected.

We are also able to provide this page on the Intranet that will give a weekly status of the City's network rebuilding efforts across the organization and its facilities. We look forward to updating it weekly over the coming months.

In both the news release and Intranet page you will see the City has worked with our cyber security insurance provider to provide all City employees a 12-month subscription to TransUnion credit monitoring services. Everyone should have received information about that via City email last Friday. We encourage everyone to take advantage of this service at no cost to you.

Thank you again to everyone for your efforts during this time and as we move forward. Your service is greatly appreciated!

Posted on: June 2, 2025

[ARCHIVED] Information on the City of Abilene Cyber Attack

The City of Abilene would like to thank residents for their patience and understanding over recent months as our organization began the work of identifying, circumventing, and recovering from a cyber attack on our network. While essential services continued through this time, we know the attack and its effects have caused frustration for the community. The City of Abilene is grateful for everyone's support as we move forward from this event, and are now able to share more information about it.

On the morning of April 18, 2025, City of Abilene officials detected that City servers were unresponsive. Around 4 a.m., the City's Information Technology department investigated the outage, and after determining a foreign actor had compromised the City's computer systems, the full network was shut down to prevent any further intrusion or data loss.

"The City suffered a ransomware attack," said Troy Swanson, Director of Information Technology for the City of Abilene. "They encrypted data and deleted data off our servers."

The City was given a deadline of May 27, 2025, to pay a ransom to restore the stolen data, estimated at 477 gigabytes.

Communication has occurred with the suspect hacking group claiming responsibility to ascertain the nature of the information taken. However, the City determined it will not aid or abet the perpetrators otherwise, and will not pay the ransom.

"I was involved in the acquisition of our cyber insurance because of my role in overseeing risk management," said Mike Perry, Director of the City's Office of Professional Standards. "Fortunately for us, we increased our insurance coverage last year."

Perry has used his background in law enforcement as a former Assistant Chief of Police to help direct investigation efforts related to the recent cyberattack.

Perry said his role as an administrator has in part been to work with the cybersecurity team hired by the city's insurance company to help mitigate damage and help with recovery efforts.

As of May 28, 2025, there is no indication the City's information has been misused by the threat actors, he said.

There also is no evidence that residents' information has been used or released by the hacking group, he said.

Perry said the investigation is ongoing, and the exact information taken by the hackers is unclear. However, the amount taken appears to be relatively small compared to the City's total storage capacity.

"We're currently in this pattern of waiting to see if and when they're going to publish the data," he said. "There's not a lot more dialog to be had because we've told them we're not going to pay the ransom."

The Hack and Its Aftermath

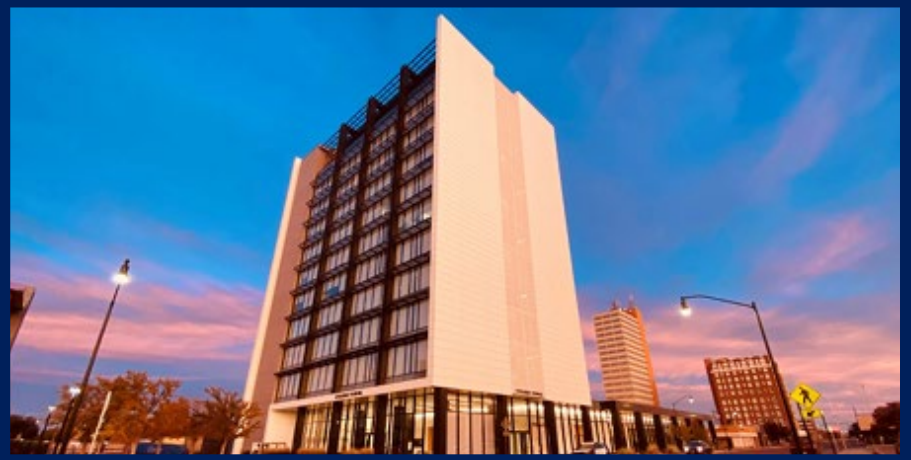
The hacking group was able to compromise the City's network and ultimately access administrative credentials, Swanson said. They also attempted to uninstall antivirus software and remove other protective measures.


Disney


*No humans are injured in this AI generated scenario
CITY HALL
555

How would you communicate with employees if you had no internet, computers, email, or phone access?


CAN I COME INSIDE?



Communicating During a Cyber Event

City of Lubbock

City of Lubbock TEXAS

Lacey Rose

Director of Communications & Public Engagement

City of Lubbock TEXAS

Timeline of Events

Tuesday, August 12, 2025

CONTEXT:

- **A regular City Council meeting was due to start with a live broadcast at 12:30 p.m. on Tuesday, August 12.**
- **This was a payroll week, so our accounting department was actively submitting electronic**

- **10:50 a.m.** – IT received an alert about malicious file attempt on a City PC.
- **11:15 a.m.** – federal and state agencies reached out to the City regarding the same computer
  - Suspected ransomware gang using possible imposter software download
- **12:00 p.m.** – Communications & Public Engagement Department made aware of the situation
- **12:20 p.m.** – all City networks were taken offline
- **5:00 p.m.** – IT meets with cyber insurance company and reviews

Timeline of Events

Wednesday, August 13, 2025

- **8:30 a.m. –** The City of Lubbock website is brought back online
- **9:00 a.m.** – Rocket.chat (moved to external domain connection)
  - IT began providing updates to all department heads

Timeline of Events

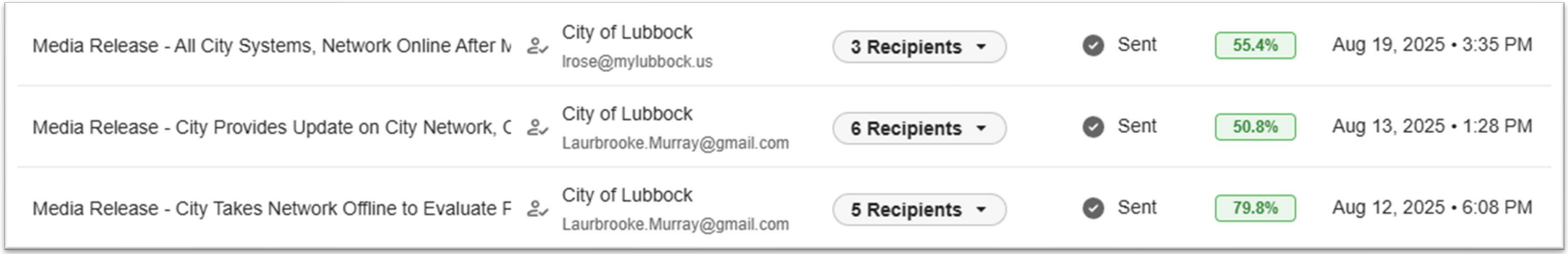
October – December 2025

- Each City department had an after-action review with IT and the Office of Emergency Management

Immediate Impacts

- Public safety
- Public broadcast of City Council Meeting
- Utility bill pay
- Ability to communicate internally
  - All communication between management > directors > staff was verbal/texted/or done via personal email accounts.

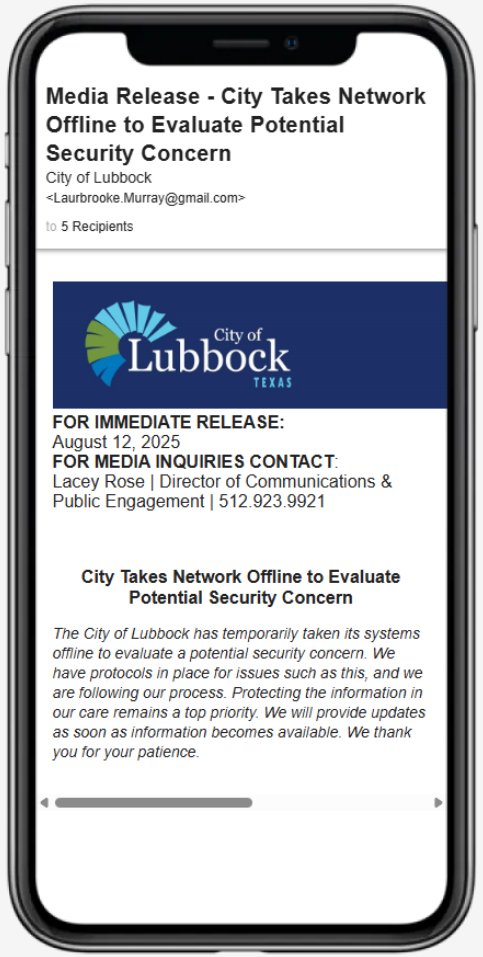
External Communication Timeline



Media Release - All City Systems, Network Online After M	City of Lubbock lrose@mylubbock.us	3 Recipients	Sent	55.4%	Aug 19, 2025 • 3:35 PM
Media Release - City Provides Update on City Network, C	City of Lubbock Laurbrooke.Murray@gmail.com	6 Recipients	Sent	50.8%	Aug 13, 2025 • 1:28 PM
Media Release - City Takes Network Offline to Evaluate F	City of Lubbock Laurbrooke.Murray@gmail.com	5 Recipients	Sent	79.8%	Aug 12, 2025 • 6:08 PM

External Communication Timeline

Day of incident (Tuesday, 08/12)



Media Release - City Takes Network Offline to Evaluate Potential Security Concern

City of Lubbock
<Laurbrooke.Murray@gmail.com>

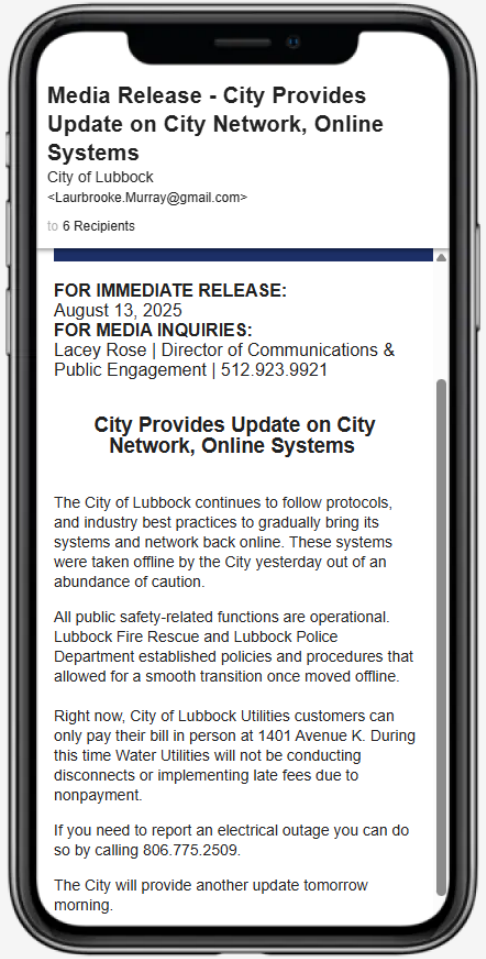
to 5 Recipients

FOR IMMEDIATE RELEASE:
August 12, 2025
FOR MEDIA INQUIRIES CONTACT:
Lacey Rose | Director of Communications & Public Engagement | 512.923.9921

City Takes Network Offline to Evaluate Potential Security Concern

The City of Lubbock has temporarily taken its systems offline to evaluate a potential security concern. We have protocols in place for issues such as this, and we are following our process. Protecting the information in our care remains a top priority. We will provide updates as soon as information becomes available. We thank you for your patience.

Day after incident (Wednesday, 08/13)



Media Release - City Provides Update on City Network, Online Systems

City of Lubbock
<Laurbrooke.Murray@gmail.com>

to 6 Recipients

FOR IMMEDIATE RELEASE:
August 13, 2025
FOR MEDIA INQUIRIES:
Lacey Rose | Director of Communications & Public Engagement | 512.923.9921

City Provides Update on City Network, Online Systems

The City of Lubbock continues to follow protocols, and industry best practices to gradually bring its systems and network back online. These systems were taken offline by the City yesterday out of an abundance of caution.

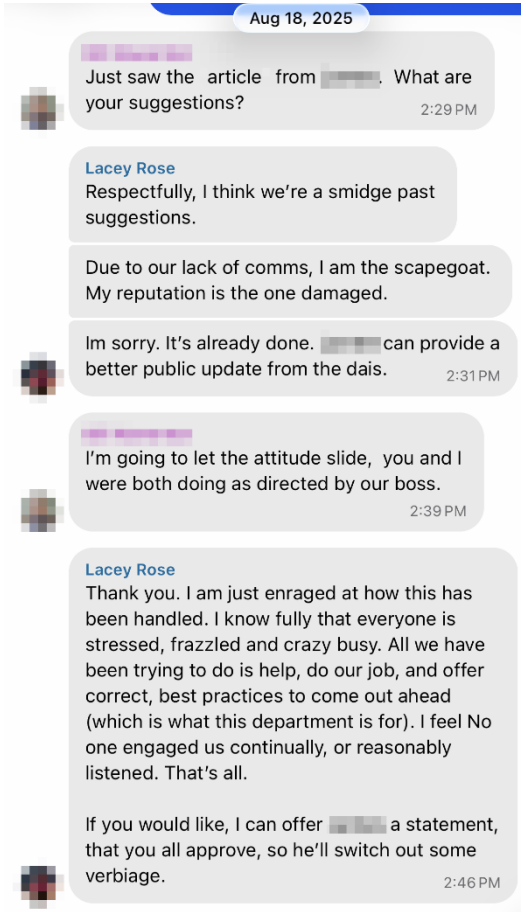
All public safety-related functions are operational. Lubbock Fire Rescue and Lubbock Police Department established policies and procedures that allowed for a smooth transition once moved offline.

Right now, City of Lubbock Utilities customers can only pay their bill in person at 1401 Avenue K. During this time Water Utilities will not be conducting disconnects or implementing late fees due to nonpayment.

If you need to report an electrical outage you can do so by calling 806.775.2509.

The City will provide another update tomorrow morning.

• • • *(not our decision)*



Aug 18, 2025

[redacted] Just saw the article from [redacted]. What are your suggestions? 2:29 PM

Lacey Rose
Respectfully, I think we're a smidge past suggestions.

Due to our lack of comms, I am the scapegoat. My reputation is the one damaged.

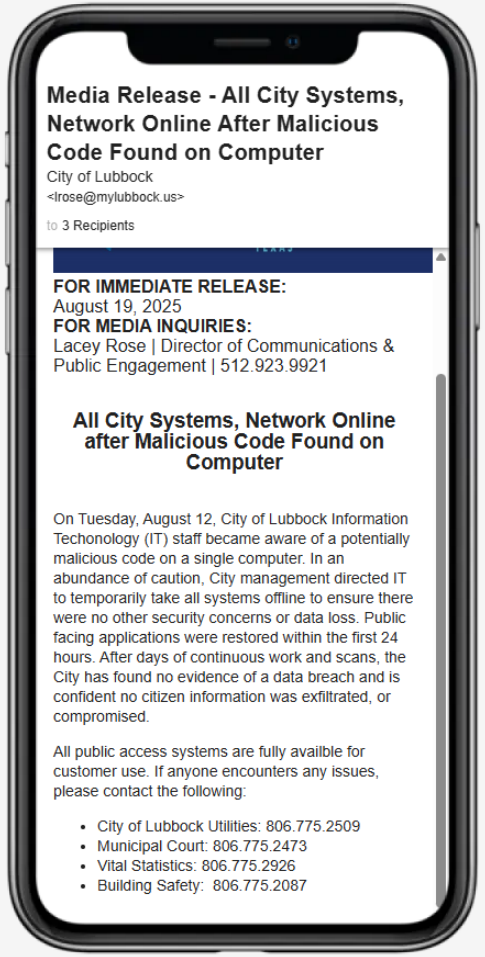
Im sorry. It's already done. [redacted] can provide a better public update from the dais. 2:31 PM

[redacted] I'm going to let the attitude slide, you and I were both doing as directed by our boss. 2:39 PM

Lacey Rose
Thank you. I am just enraged at how this has been handled. I know fully that everyone is stressed, frazzled and crazy busy. All we have been trying to do is help, do our job, and offer correct, best practices to come out ahead (which is what this department is for). I feel No one engaged us continually, or reasonably listened. That's all.

If you would like, I can offer [redacted] a statement, that you all approve, so he'll switch out some verbiage. 2:46 PM

The following week (Tuesday, 08/19)



Media Release - All City Systems, Network Online After Malicious Code Found on Computer

City of Lubbock
<lrose@mylubbock.us>

to 3 Recipients

FOR IMMEDIATE RELEASE:
August 19, 2025
FOR MEDIA INQUIRIES:
Lacey Rose | Director of Communications & Public Engagement | 512.923.9921

All City Systems, Network Online after Malicious Code Found on Computer

On Tuesday, August 12, City of Lubbock Information Techonology (IT) staff became aware of a potentially malicious code on a single computer. In an abundance of caution, City management directed IT to temporarily take all systems offline to ensure there were no other security concerns or data loss. Public facing applications were restored within the first 24 hours. After days of continuous work and scans, the City has found no evidence of a data breach and is confident no citizen information was exfiltrated, or compromised.

All public access systems are fully availble for customer use. If anyone encounters any issues, please contact the following:

- City of Lubbock Utilities: 806.775.2509
- Municipal Court: 806.775.2473
- Vital Statistics: 806.775.2926
- Building Safety: 806.775.2087

Issues Identified by Our Department

- **Internal communications**
  - Directors were not given adequate information to funnel down to the rest of the City staff.
  - This led to rumors and frustration.
  - Staff sitting at their desk unable to login to computer to work.
- **Not bringing our department in early**
  - Communications & Public Engagement was only brought in when it became apparent that it would impact the live broadcast of the City Council Meeting.
  - Our department was only brought into discussions at the end of the day on Tuesday.
- **Not including all pertinent staff on Rocket.Chat group**
  - When a broader attempt to communicate internally was finally made, it didn't include all departments and management staff.
- **Not communicating publicly**
  - Our department advised leadership that it was important to be as transparent as possible. Due to the nature of the situation, there was a lot of reluctance to share anything at all.
  - The cyber insurance team also agreed with us, and gave the green-light for us to handle all public communications.
- **Not meeting public promises/expectations**
  - In the first release that was approved to be sent, there was promise made to provide an update the following morning. Leadership would not allow us to do so. A new update was not proved until the following Tuesday (1 week after the incident occurred).
- **Not replying to internal requests from PIO for updates**
  - Because of the uncertainty about these types of incidents and a fear of further targeted attacks, our leadership was mostly unresponsive to our department's requests for information during this time.

Recommendations/Key Takeaways
(from our department's POV)

If this happened again tomorrow, these are things that we think would have improved our City's response:

- **Add ongoing floor-by-floor updates in Rocket.Chat as departments are cleared to get back online.**
  - Even once many departments had been cleared to return to normal operations, the staff in those departments were not made aware for hours in some cases.
- **Provide more clear and consistent updates to department heads about what their staff can expect as soon as information is available.**
  - Morale was severely impacted by a lack of communication with our own staff, leading to employees feeling forgotten or devalued.
- **Have designated communication liaison between IT and PIOs**
  - It was discovered post-mortem that there was not a member of the IT team who felt that it was within their power to share sensitive information with our team. The director of IT acknowledged that it would have been beneficial to have a designated person to communicate regularly as the situation evolved.
- **Doing a better job of managing and meeting internal and external expectations**
- **Utilize C&PE to produce graphics that matched the recognizable format of our usual official (trusted) internal emails to disseminate information to departments through their respective department heads.**
  - This provides a more structured update to aid in rumor control. Lack of info was the main identified cause of misinformation during this incident. Staff rumors get shared with their families, friends, and other community members. This information makes its way onto social media and ultimately leads to public misinformation. With a staff in the thousands, our internal communication is nearly as important as external communication. Each member of the City's staff is like an ambassador of information.

Things that worked well
(from our department's POV)

- Getting Rocket.Chat involved in the internal communications
- Using departmental phone-tree style communication

Questions?


Greetings from
TAMIO
Worth Writing Home About
AUSTIN ★ JUNE 3-5, 2026

Feedback...

CITY OF ABILENE

City of Lubbock TEXAS

CARROLLTON TEXAS

AUSTIN ★ JUNE 3-5, 2026