Lincoln Archives, Inc.

SAFE. SECURE. SOLUTIONS.™

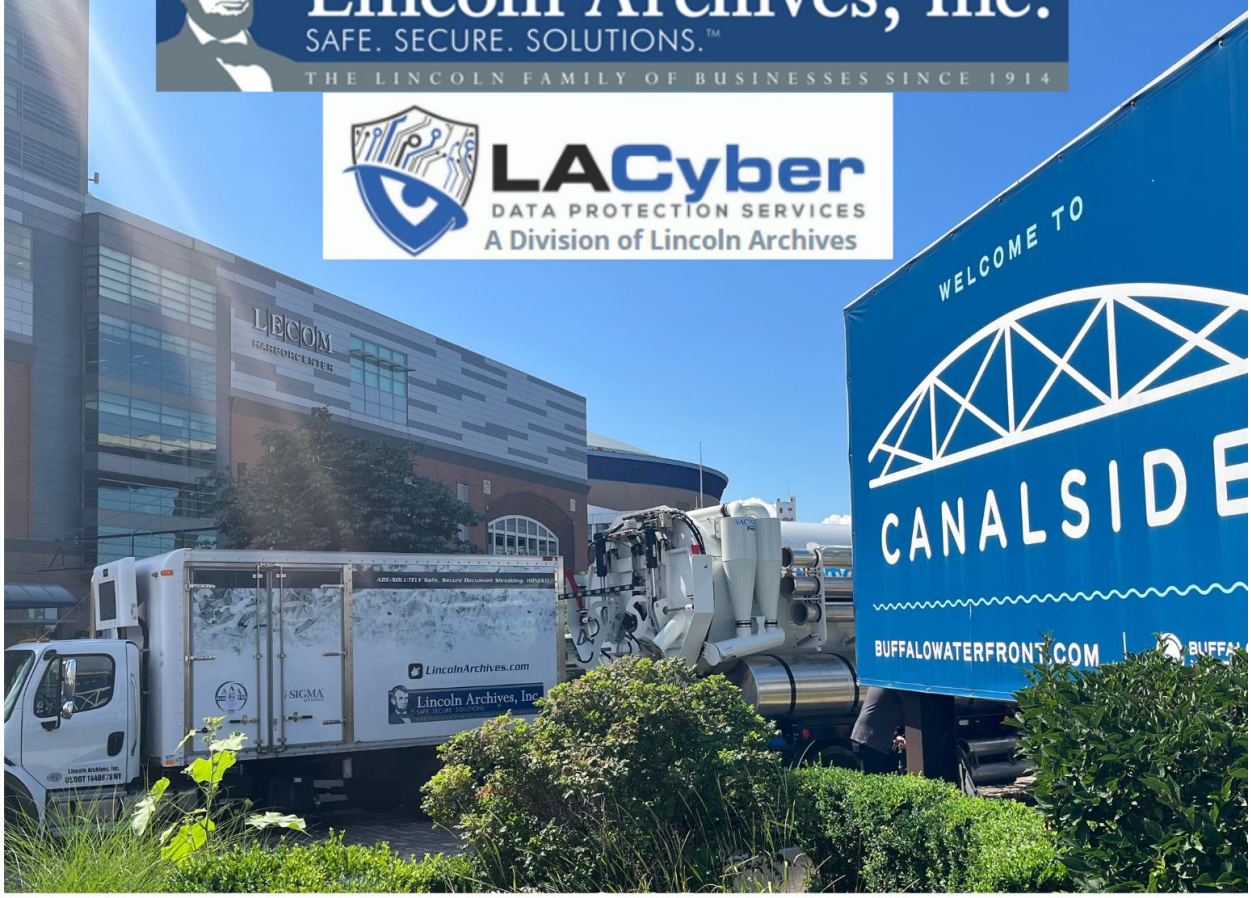
THE LINCOLN FAMILY OF BUSINESSES SINCE 1914

August 2023

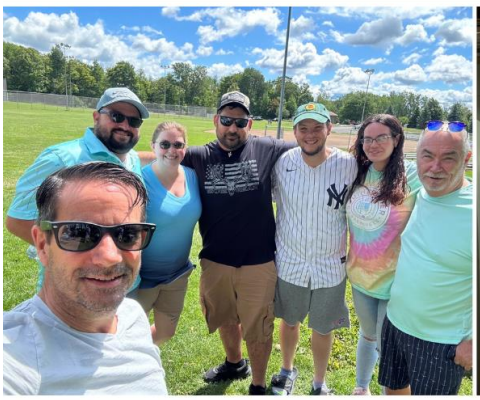
LACyber

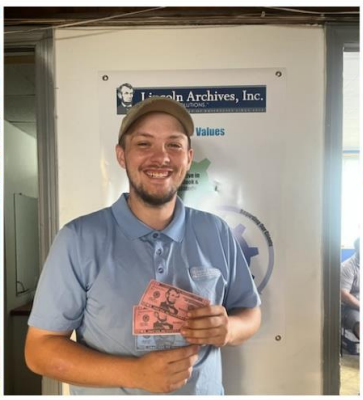
DATA PROTECTION SERVICES

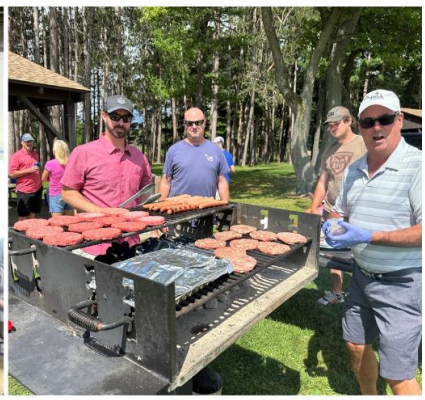
A Division of Lincoln Archives



Wrapping up our summer in style!







BILL'S PICKS

LACyber's exclusive online page for all things cybersecurity

THE HIDDEN BENEFITS OF NEGOTIATING WITH RANSOMWARE ATTACKERS

MORE THAN HALF OF BROWSER EXTENSIONS POSE SECURITY RISKS

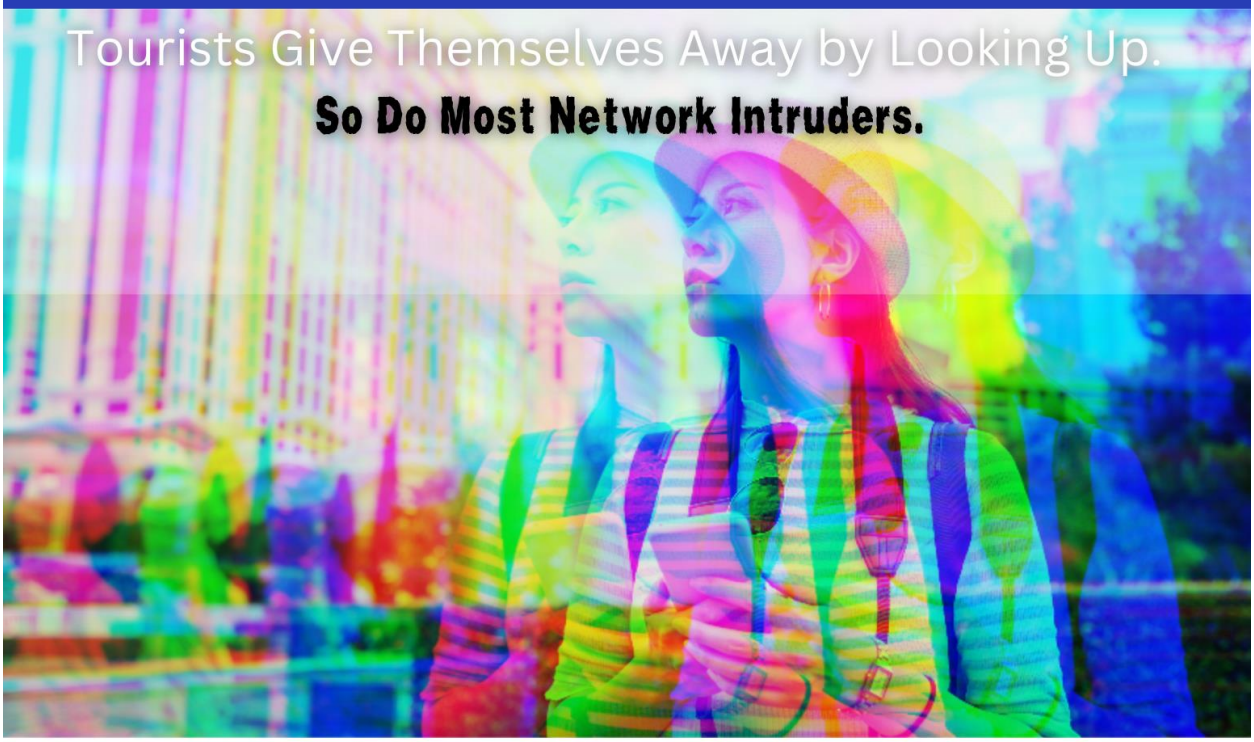
RANSOMWARE PROTECTION FOR STATE, LOCAL GOVERNMENTS (AND HOW TO PAY FOR IT)

BARRACUDA XDR INSIGHTS: HOW AI LEARNS YOUR PATTERNS TO PROTECT YOU

Latest ActiveCyber Threats

Watch for the latest in cybersecurity threats sent right to your inbox every week!

08.22.2023	Sneaky Amazon Google ad leads to Microsoft support scam
08.23.2023	Scraped data of 2.6 million Duolingo users released on hacking forum



In large metropolitan areas, tourists are often easy to spot because they're far more inclined than locals to gaze upward at the surrounding skyscrapers. Security experts say this same tourist dynamic is a dead giveaway in virtually all computer intrusions that lead to devastating attacks like data theft and ransomware, and that more organizations should set simple virtual tripwires that sound the alarm when authorized users and devices are spotted exhibiting this behavior.

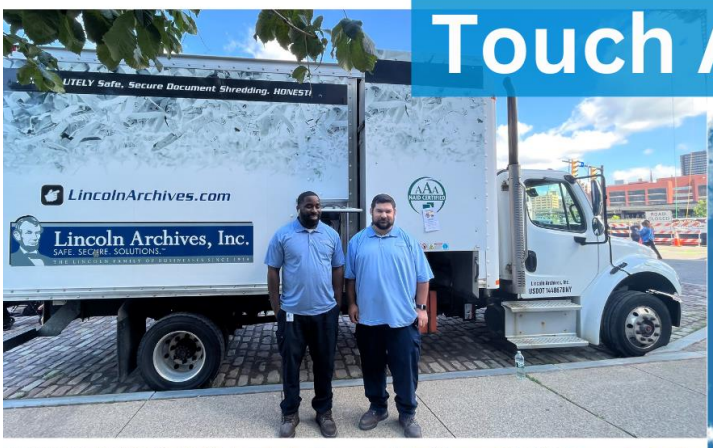
The same tourist behavior that attackers exhibit vis-a-vis older routers is also incredibly common early on in ransomware and data ransom attacks -which often unfurl in secret over days or weeks as attackers methodically identify and compromise a victim's key network assets.

These virtual hostage situations usually begin with the intruders purchasing access to the target's network from dark web brokers who resell access to stolen credentials and compromised computers. As a result, when those stolen resources first get used by would-be data thieves, almost invariably the attackers will run a series of basic commands asking the local system to confirm exactly who and where they are on the victim's network.

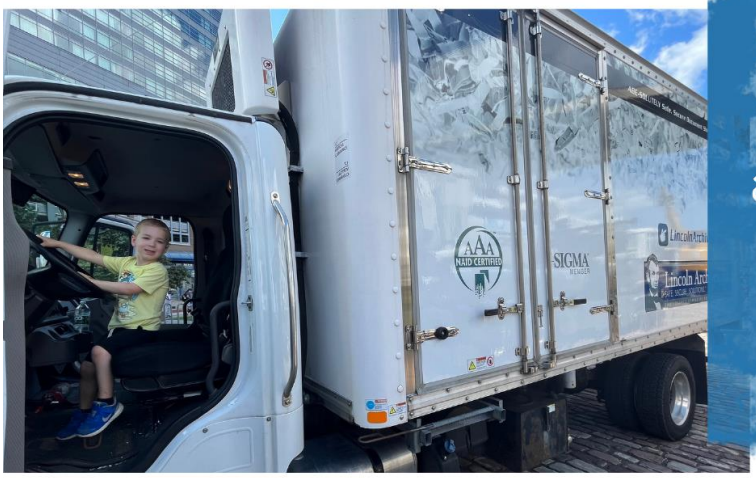
This fundamental reality about modern cyberattacks — that cybercriminals almost always orient themselves by "looking up" who and where they are upon entering a foreign network for the first time — forms the business model of an innovative security company called Thinkst, which gives away easy-to-use tripwires or "canaries" that can fire off an alert whenever all sorts of suspicious activity is witnessed.

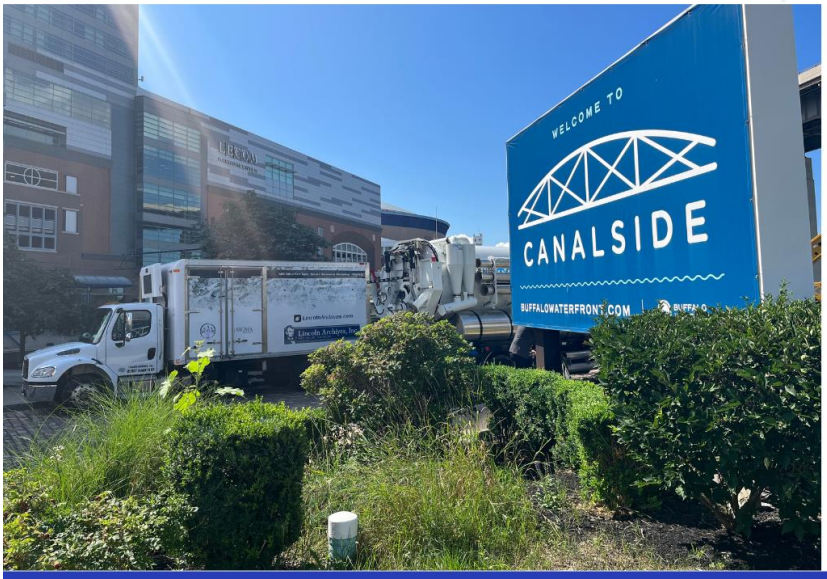
Click here to continue reading this article

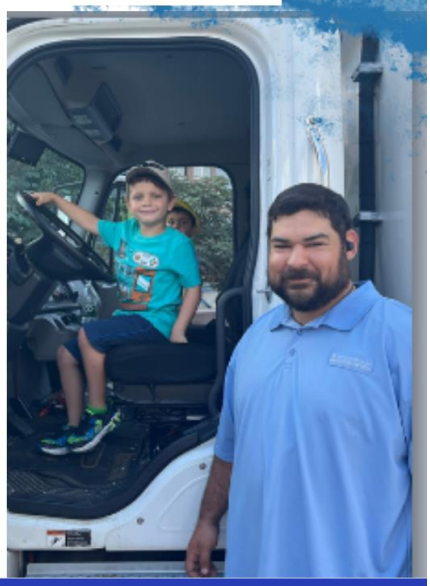
Touch A Truck 2023



Lincoln Archives participated in the annual event held down at Canalside that allows kids of all ages to climb aboard our truck and see what we do!







uRISQ℠
cyber privacy suite

Comprehensive Data Security Services

Be Compliant.
Reduce Risk.
Protect Your Business

Click Here to learn more

Data Breach Support

Do you know what to do if you have a data breach? Most businesses don't. uRISQ's Data Breach Support gives you the peace of mind that a Certified Privacy Expert (CIPP) is at the tips of your fingers.

Privacy Policy Assessment

Managing risk is an important aspect of all successful businesses. Developing and maintaining a security and privacy program is key to managing your organization's risk of data loss. Privacy Assessment helps you with your annual assessments, and policy and plan templates for your organization.

Threat Scanning

uRISQ's Threat Scanning performs a recurring vulnerability scan on your website and firewall, making you aware of your open vulnerabilities.

Data Subject Access Request Process

Data Subject Access Request is a request initiated by the individual or a legal representative requesting the specific information you as a company collect, store, and transmit on an individual. uRISQ's DSAR module is a workflow management tool that helps organizations manage their requests from beginning to end and make sure they adhere to the legal time requirements.

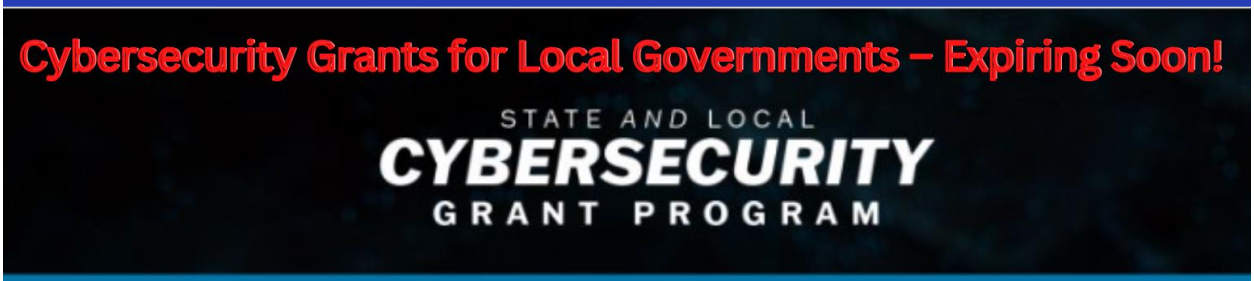
Vendor Management

Every business relies on third-party vendors to perform some aspect of its operations. It is a requirement that you ensure those vendors are handling the information you have entrusted to them to the same privacy and security standards you are publishing in your privacy policy.

Contact us today!

JamieJ@LA-Cyber.com

Cybersecurity Grants for Local Governments – Expiring Soon!



NOTICE OF FUNDING OPPORTUNITY (NOFO)

Are you aware of the $374.9 million in grand funding for the 2023 State and Local Cybersecurity Grant Program (SCLGP)?

Why is this important:

- SLCGP is a first-of-its kind cybersecurity grant program specifically for state, local and territorial governments across the country to help them strengthen their cyber resilience.
- State and local governments have until **October 6th** to apply for the fiscal year 2023 grant opportunity.
- If you need assistance with utilizing funds from this program, LACyber's experts can help you with cybersecurity plans and services.

If you aren't aware of this program, click below and we'll send you the program fact sheet right away.

Join us for a webinar next month presented by Barracuda:

How Hybrid Workforces Open Doors for Hackers

(And What You Can Do About It)

Register Now!

September 21st 2pm- 3pm ET