CYBERSECURITY AND CRITICAL INFRASTRUCTURE

When infrastructure is under attack, everything is at risk

THIS MONTH'S TOPICS:

Our modern way of life depends on systems we rarely stop to consider: power grids, transportation networks, healthcare facilities, and more. These pieces of critical infrastructure are so seamlessly integrated into our daily routines that we often don't notice them until something goes wrong.

Cybercriminals and nation-state attackers realize just how vital these systems are. That's why they often target weak links, where one compromised account can open the door to larger disruptions. In this issue, we'll explore the hidden connections between cybersecurity and critical infrastructure, and how you play a vital role in protecting the systems we all rely on.

THE WEAKEST LINK PROBLEM

5 WAYS NON-CRITICAL COMPANIES BECOME ATTACK GATEWAYS

Critical infrastructure doesn't just depend on power plants or hospitals. It relies on everyday businesses and people like you. Hackers often target smaller, less secure organizations to gain access to much bigger systems. Here's how it happens—and how to stop it.

Third-Party Vendor Access

Smaller companies often provide services—like HVAC, IT, or billing—to critical infrastructure organizations. A hacker only needs one weak credential or unmonitored remote login to slip through the cracks.

Overlooked Software Updates

Unpatched software can create backdoors. If your device or software connects to partners in healthcare, energy, or public services, an unpatched vulnerability becomes a shared threat.

Credential Reuse

If you reuse passwords across accounts, a breach at your company can expose credentials that work elsewhere—including portals tied to infrastructure support services.

Social Engineering & Phishing

Cybercriminals often gather information from non-critical businesses to craft more convincing phishing attacks on critical targets.

Lack of Security Awareness Culture

When security is seen as "just IT's job," risky behaviors slip through. Every careless click, ignored warning, or missed scam report opens the door to a larger breach.

Every employee is part of the cybersecurity supply chain. Even if your company doesn't build infrastructure, you're still connected to it. Be the strongest link: update often, question everything, and report quickly.

HIDDEN INFRASTRCTURES YOU DEPEND ON

GPS Satellites

What They Do: Sync banking transactions, guide airplanes, support farming equipment, power rideshares and deliveries.

Why It Matters: Without GPS, everything from emergency services to ATMs could grind to a halt.

Cloud Platforms

What They Do: Store data and run applications for hospitals, schools, city governments, and businesses.

Why It Matters: A single outage or attack on a cloud provider could delay surgeries, shut down classrooms, or block vital public services.

Payment Processing Networks

What They Do: Process debit/credit card purchases, mobile wallets, and online payments.

Why It Matters: If attackers disable these systems, grocery stores, gas stations, and pharmacies could stop accepting digital payments, disrupting daily life.

Internet Exchange Points (IXPs)

What They Do: Act as “meeting hubs” where different internet networks connect to keep global data flowing.

Why It Matters: If IXPs are disrupted, websites, apps, and even communications across whole regions could slow or fail.

Water Treatment Systems

What They Do: Monitor and manage clean drinking water and wastewater systems.

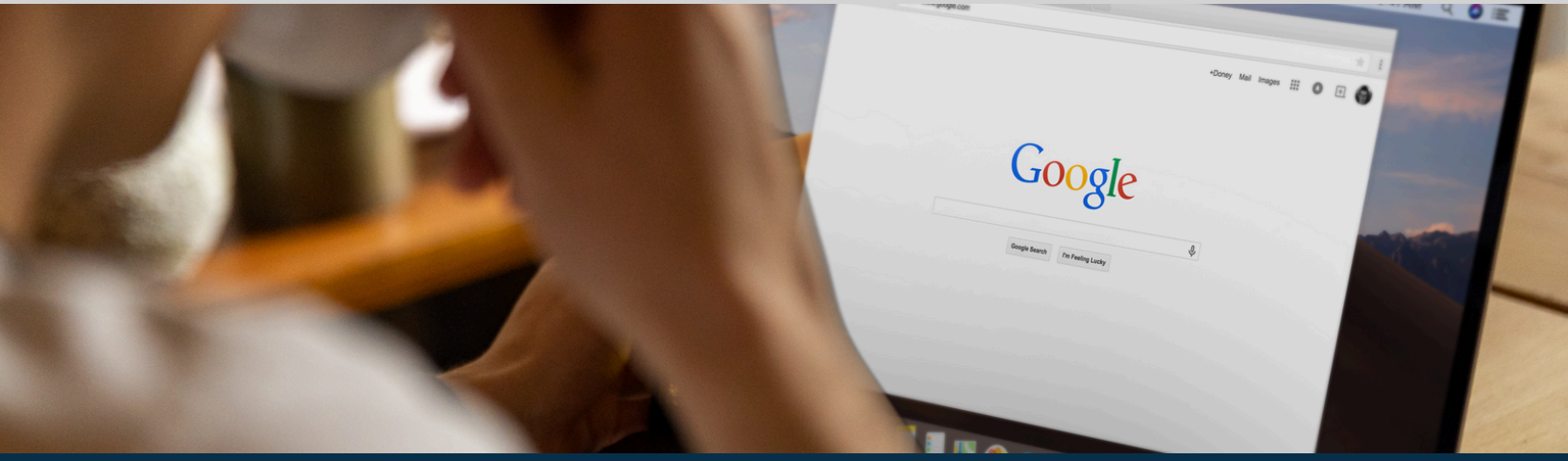
Why It Matters: A cyberattack on these systems could contaminate water supplies or cut access entirely, impacting millions overnight.

SCAM OF THE MONTH: DISTRIBUTED DENIAL OF SERVICE SCAMS (DDOS)

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

Last spring, a regional hospital suddenly found its online patient portal unreachable. Families trying to check lab results or message doctors were met with error screens, while staff struggled to access scheduling tools. Behind the scenes, the hospital's servers were flooded with millions of junk requests per second—a classic Distributed Denial of Service (DDoS) attack. Soon after, a threatening email arrived: "Pay 10 Bitcoin within 24 hours, or your systems stay down."

The hospital refused to pay, but the disruption lasted long enough to delay critical patient communications and force staff into paper-based backups. While no sensitive data was stolen, the attack highlighted how cybercriminals use DDoS not to breach systems, but to overwhelm them—and then extort victims for money. It was a stark reminder that even organizations focused on saving lives can be held hostage by digital traffic jams.



DID YOU SPOT THE RED FLAGS?

- When a hospital's patient portal and internal tools suddenly went offline, the sheer volume of junk traffic was the giveaway.
- The threatening email demanding Bitcoin payment in exchange for restored service is another classic red flag.

STAY SAFE

HOW TO PROTECT YOURSELF

- If you receive a ransom note after a service disruption, never pay. Paying only encourages attackers and doesn't guarantee they'll stop.
- Organizations can prepare by using DDoS protection services, firewalls, and traffic monitoring tools to filter out malicious requests.

CYBERSECURITY IS THE NEW PUBLIC SAFETY

Just like fire drills and seatbelts, cybersecurity is a habit that protects everyone.

Think of Everyday Safety Habits

- Fire drills prepare us for emergencies.
- Seatbelts protect us before accidents happen.
- Handwashing prevents the spread of illness.

Cybersecurity works the same way. It's an IT concern, but it's also a public safety measure that depends on everyone's participation.

Simple Actions, Big Impact

- **Updating Devices Regularly** → Prevents attackers from exploiting old software.
- **Avoiding Phishing Scams** → Stops ransomware before it spreads to hospitals, utilities, and schools.
- **Reporting Suspicious Activity** → Early reporting can halt a larger attack in progress.

Your Role in the Chain

Every small action, like clicking carefully, patching on time, and reporting quickly, helps protect more than just your own inbox. It helps secure the systems that deliver clean water, keep the power running, and support emergency services.

Public safety isn't just about locks and alarms anymore. It's about cybersecurity, and it starts with you.