

# Cybersecurity Services from CivicPlus®

Your Ally in the Fight Against Cybercrime

With the growing importance of online access for municipal services, local government websites are increasingly becoming the targets of cyberattacks. Since the beginning of the COVID-19 crisis, cyber-extortionists recognizing the vulnerability of municipal websites are looking to capitalize on exposed weaknesses and hold civic data and digital properties hostage for personal gain. The best way to protect your website and the integrity of your digital presence is through a partnership with the trusted local government website security experts at CivicPlus.

# A Rapid Escalation in Cybercrime due to COVID-19

Cybercrime has increased by [600% since](#) the start of the COVID-19 crisis. These threats appear in the forms of sophisticated email schemes from malicious actors posing as representatives from the U.S. Centers for Disease Control and Prevention (CDC) and the World Health Organization (WHO).

Not only can cyber-attacks cripple systems and degrade data integrity, but they can also be financially devastating to attacked entities. Seven out of every ten malware payloads are ransomware—a software program that effectively holds a website hostage with the controlling cyber-extortionist refusing to relinquish control of the website unless a monetary ransom is paid. The consequences of not remitting payment is a threat of data loss or extortion.

Over 18 million websites are infected with malware at a given time each week, and over 34 percent of businesses hit with malware took a week or more to regain access to their data. Such a loss of time and information access is not sustainable for local governments attempting to maintain business continuity while serving socially distanced citizens. Ransomware attacks are estimated to cost \$6 trillion annually by 2021.



## What is Phishing?

An email designed to deceive and trick recipients into taking an action—clicking a malicious link or opening an attachment with a virus.

## What is Network Security Vulnerability?

A weakness that can be exploited by a malicious actor to perform unauthorized actions within a computer system.

## What is Malware?

Any software intending to harm data, devices or to people. It includes computer viruses, trojans, spyware, ransomware, adware, worms, file-less malware, or hybrid attacks. Malware attacks are becoming more sophisticated due to machine learning and targeted spear phishing emails.

# Internal Threats and Vulnerabilities

Ninety-eight percent of cyber-attacks rely on social engineering, the psychological manipulation of people into performing actions or divulging confidential information.

Sixty-three percent of successful attacks come from internal sources, which means every administrative staff member in your administration must understand the threat of cyberattacks and avoid making systems and data vulnerable to attack.

## In addition:

21%

of all files are not adequately protected

41%

of companies have over 1,000 sensitive files, including credit card numbers and unprotected health records

69%

of organizations don't believe their anti-virus software can block modern threats

50%

of organizational security risk comes from stitching together multiple security vendors and products



Atlanta, Georgia spent over \$5 million rebuilding its computer network, after being hit by the SamSam ransomware attack in March 2018.

In 2019 hackers breached the Maryland Department of Labor and illegally accessed names and social security numbers for 78,000 individuals.

# The Benefits of External Security Hosting

Smart municipalities that choose to outsource their cybersecurity and hosting benefit from less strain on existing staff, a reduced vector footprint, less exposure to other vital infrastructure and systems, and they can refocus their hiring strategy so as not to require dedicated funding to a single cybersecurity internal resource.

## Local governments that outsource their hosting to a trusted partner also benefit from:

The convenience of trusting that a critical data management component is being serviced and monitored by experts.

The ability to focus more time and attention on IT matters that require the attention and strategy of directors and other key personnel, such as leading digital transformation initiatives.

Integrated service offerings such as website design and development and a single source for support.

Local government CIOs that outsource their hosting also benefit from having time to focus on impactful strategic initiatives.

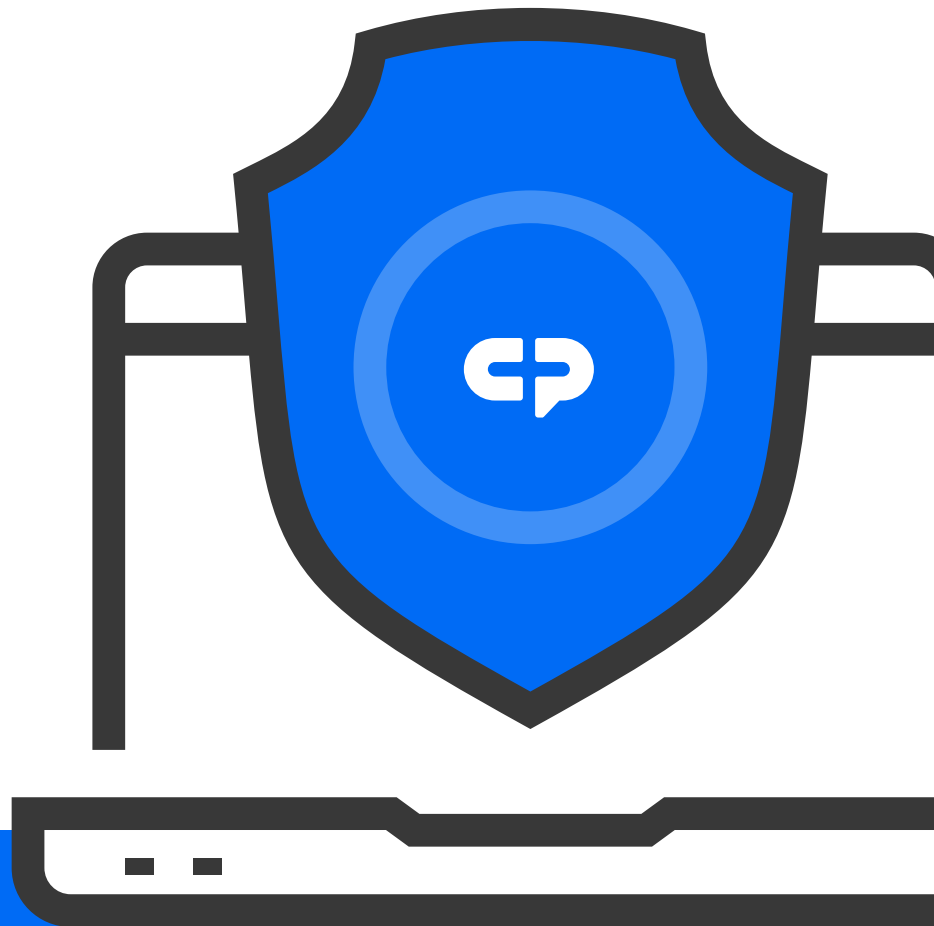
# Partner with the Pressure-

## Tested Security Experts at CivicPlus



CivicPlus is the trusted leader in cybersecurity for local government, successfully having mitigated many threats. We let our clients focus on what they do best: serving the needs of their communities. We invest nearly \$4 million annually on cybersecurity to monitor and reduce the risks that local governments face and have teamed up with local and federal enforcement agencies to share information.



The benefits of our investment include the ability to offer 99.9% up-time in a Tier II fully redundant data center. With multiple network providers, burst bandwidth, and live 24/7/365 emergency support, we're working hard to stay ahead of the ever-changing security landscape.



We offer disaster recovery via geographically diverse data centers and defined RTO and RPO to provide you options in determining the security posture you want to implement for your community. Visit our website for more information regarding our security service.







# Coverage and Security Benefits of DDoS Advanced Security Protection

 Included  DDoS Advanced Security Protection Upgrade

Hosting & Security		
Web Application Firewall		✓
OWASP ModSecurity Core Rule Set		✓
Reverse Proxy Server		✓
SSL (TLS) Certificates	Available for Purchase	✓
Server Management	✓	✓
Software Updates and Security Patches	✓	✓
Antivirus Management and Updates	✓	✓
System Monitoring	24/7/365	24/7/365

Performance and Bandwidth		
Server-Side Caching		✓
Regional Content Deliver Network		✓
Bandwidth Usage	Unlimited (does not apply in the event of a cyber attack)	Unlimited
Burst Bandwidth	22 Gb/s	45 Gb/s

Insights		
CivicEngage Security Analytics Module		✓

DDoS Mitigation		
Defined DDoS Attack Process	✓	✓
Identify Attack Source	✓	✓
Identify Type of Attack	✓	✓
Monitor Attack for Threshold** Engagement	✓	NA
If Threshold Engagement Occurs, Offer Options*	✓	NA
DDoS Attack Mitigation	See Options*	✓

Client Cost		
Cost		\$2,625*** one-time set-up, \$250*** per month quarterly contract

### \*DDoS Attack Options

#### Option #1: Site Off-line

- Status Check traffic at eight-hour intervals during business hours
- Traffic below thresholds = site taken back online
- Traffic above thresholds = site stays down and monitoring continues until traffic falls below thresholds

\*\*\*Per Domain, Per Site

#### Option #2: DDoS Advanced Security Protection Upgrade

- Site can come back online after setup is completed, additional charges may apply

#### \*\*Thresholds

- Traffic exceeding 25 Mb/s sustained for 2+ hours
- Traffic over 1 Gb/s at any point during attack

# DDoS Advanced Security Protection

Includes the Following Benefits:

**Our DDoS Advance Security Protection comes with enterprise-level Cloudflare software, which includes the following:**

The Open Web Application Security Project (OWASP) ModSecurity Core Rule Set protects you against the Top 10 vulnerabilities identified by OWASP, such as SQL Injection (SQLi) and cross-site scripting (XSS) attacks

Fully customized Web Application Firewall (WAF), customized for our application

User agent blocking

Block or challenge visitors by IP address, autonomous system number (ASN) or country code

Reputation-based threat protection and collective intelligence (CI) to identify new threats

# DDoS Advanced Security Protection

Continued:

## DDoS Mitigation

Our Hosting and Security staff work around-the-clock to mitigate DDoS attacks against your website so that you can focus on the other local priorities and initiatives.

## Performance

With the use of Cloudflare's Content Delivery Network (CDN), we bring cached content nearer to your end-users. Additionally, we have optimized Cloudflare's caching capabilities for our application, allowing us to safely cache static content so that you benefit from faster page load times for your citizens and site administrators.

## Insights

The Security Analytics module displays comprehensive insights into attacks against your website in real-time.



## Value

Our all-inclusive package comes with not only enterprise-level Cloudflare software but also the staffing to mitigate threats for you and all at a much lower price point. Ask us for a quote today.