Cyber Security

- **Threat level – on the increase**

- **For municipalities – targeted attacks**
  - o "Spear phishing"

- **Defense at the perimeter**
  - o Firewall – intrusion prevention
    - ▪ Updated every 2 hours
  - o Web filter -- by category
  - o Spam filter – scan contents, sources
  - o Proactive threat protection – analyze packets

- **Defense on the desktop**
  - o Desktop antivirus – stop known malware, suspicious activity

- **Defense at the fingertips**
  - o Alert and informed users
  - o Awareness training
  - o Penetration testing

- **The pound of cure**
  - o Backup – on site
  - o Backup – off site

- Ransomware attacks are costly for state and local government entities. From 2017-2020, the estimated reported ransom paid per event in municipalities was $125,697.

- Ransomware attacks can cause significant downtime and denial of critical community services, such as healthcare and law enforcement. One analysis pegged the average downtime from a ransomware attack at 9.6 days.

- Attacks on local government have risen significantly. Between 2018 and 2019 known attacks on local governments rose 58.5%.

Municipalities Remain Ripe Targets for Cyber Attacks: Research - MSSP Alert

Even our trusted
commercial
partners . . .

eso

Dear John,

We recently discovered bad actors have purchased the domain
"esosolutions.org" and are sending emails from this domain in an
attempt to spoof our customers. Unfortunately, the emails appear to
use the name of a current ESO employee and our current signature
format. The only giveaway is the "@esosolutions.org" in the email
address. Specifically, these bad actors are communicating that ESO's
"receiving payments method has changed" and offering to send a copy
of updated banking instructions.

To verify the email address of the sender, see the sample screenshot
below. Note the ".org" in the email address that confirms it is fraudulent.
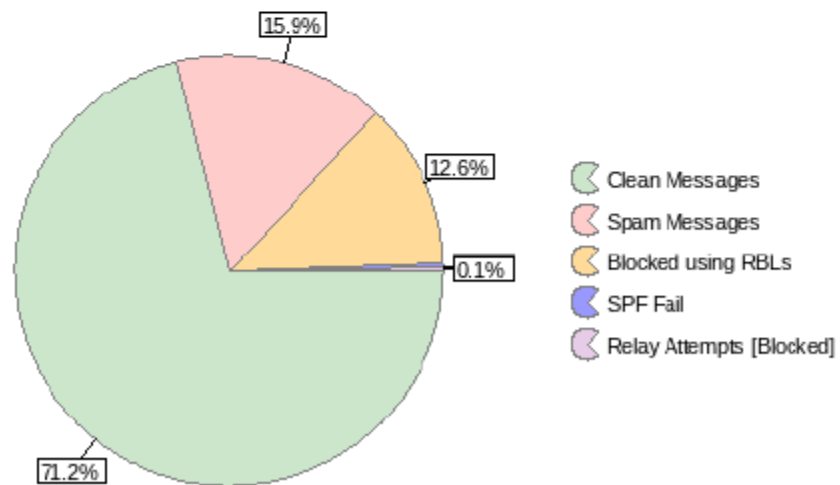
Defend the Periphery

TitanHQ
SpamTitan

SpamTitan Mail Firewall Report

Report Type:	Summary Report
Hostname	spamtitan.wiltonct.org
Report Period:	26-Feb-2021 00:00 -
	26-Feb-2021 23:59
Report Generated:	27-Feb-2021 04:31

	Mail Type	Count
1.	Clean Messages	2824
2.	Spam Messages	630
3.	Blocked using RBLs	501
4.	SPF Fail	12
5.	Relay Attempts	2

Pie chart percentages: 15.9%, 12.6%, 0.1%, 71.2%

Legend:
- Clean Messages
- Spam Messages
- Blocked using RBLs
- SPF Fail
- Relay Attempts [Blocked]

Prevention + Cure

All-In-One BCDR For Managed Services

Built for MSPs to ensure their client's business is always on and resilient to disasters, SIRIS is a complete solution—local and cloud BCDR backed by 24x7x365 single-vendor support. Deliver BCDR services without the need to cobble together individual technologies.

Ransomware Recovery

All backups are scanned for ransomware and mounted to ensure they are ready to restore. Simply 'turn back the clock' to a snapshot before the attack happened.

A Job for the Whole Organization

Why Do Chief Security Officers Leave Jobs So Often?

In both public and private organizations, chief information security officers have shorter tenures than CIOs. Why do cybersecurity heads so quickly leave jobs — or get forced out?

BY DAN LOHRMANN / FEBRUARY 28, 2021

Is it time to look elsewhere?

Everyone knows that cybersecurity is a red-hot career field, and chief security officers (or chief information security officers in many organizations) are the ones leading the online security defense. So how can we explain the current situation where about 24 percent of Fortune 500 CISOs last just one year, according to Cybercrime Magazine?

Digging deeper, the average tenure of a CISO is just 26 months, according to ZDNet.