Safe and Secure

CHARLOTTE COUNTY SHERIFF'S OFFICE

TAMMY WILKIE, COMMUNITY AFFAIRS SPECIALIST

Identity Theft What to do

What to Know

- Read your credit reports. You have a right to a free credit report every 12 months from each of the three nationwide credit reporting companies. Order all three reports at once, or order one report every four months. To order, go to annual credit report.com or call 1-877-322-8338
- Shred all documents that show personal, financial, and medical information before you throw them away.
- Create passwords that mix letters, numbers, and special characters. Don't use the same password for more than one account.
- If you shop or bank online, use websites that protect your financial information with encryption. An encrypted site has "https" at the beginning of the web address; "s" is for secure.
- Do not share your social security number, give only the last four if you must.

ATM Safety

Safeguarding Your Bank Identity

Have one credit card that you keep for purchases, gas pumps with a low credit line.

Protect your personal identification number (PIN)

Money should be put away as soon as you withdraw it from the ATM.

Use a well-lighted ATM or night deposit – be observant. Get your extra cash from stores.

Keep an eye on your cards!

Credit card skimming is one of the most dangerous forms of credit card fraud.

If You're A Victim

1. File a report with your local law enforcement agency in the community where the identity theft took place. Get a copy of the report in case the bank, credit card company or others request a copy.

2.Contact the fraud department of the three major credit bureaus. Request that a "fraud alert" is place in your file, as well as a statement asking creditors to call before opening any new accounts. Also, order copies of your credit reports. Credit bureau must give you a free copy of your report, if the report is inaccurate or you have been denied credit. Review your reports carefully, Look for inquiries from companies opening fraudulent accounts – make sure no new fraudulent activity has occurred

3. Contact your creditors about tampered with or fraudulently opened accounts. Speak with someone in the fraud department of each creditor and follow up with a letter. Immediately close any tampered with account and open a new one with a new PIN and password.

Trends we are seeing:

Exploitation: Romance Scheme;

Grandson in jail scheme.

Imposter Scams:

Jury Duty and or Sheriff's Office Deputy Calling

IRS scheme to threaten warrant.

Sweepstakes/Lottery Scams: Jamaican/Canadian Lottery.

Resurgence of check forgery/uttering (Fraudulent checks)

Solar Power for Homeowners

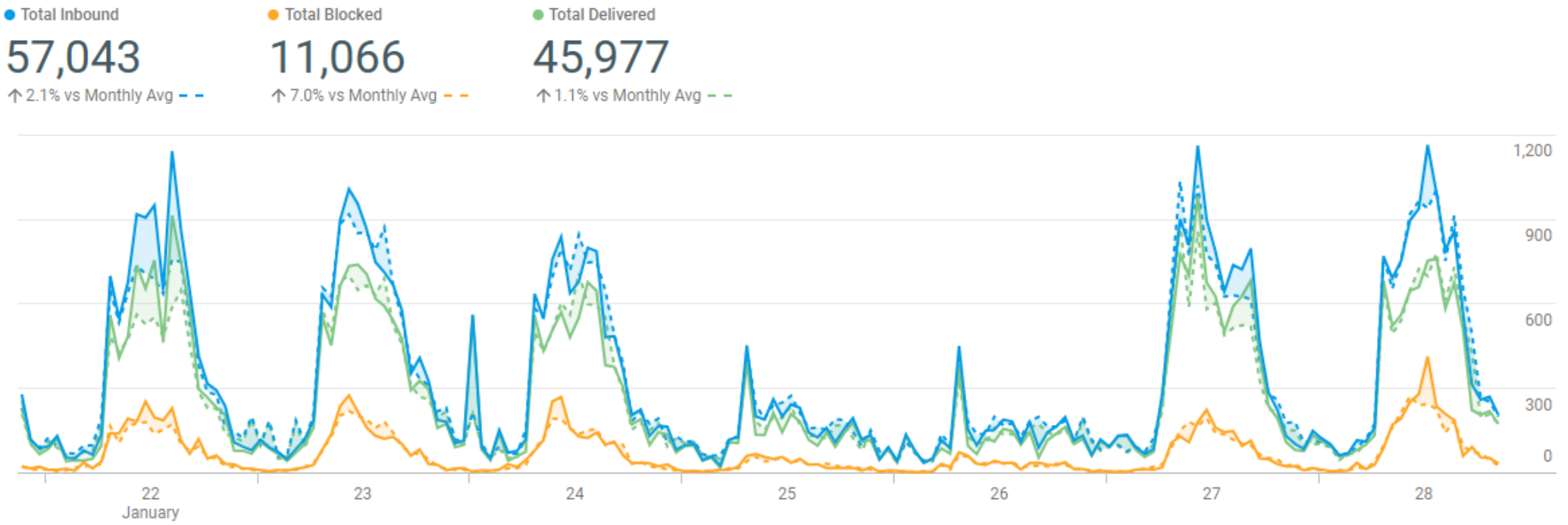
Craigslist / Let It Go / Facebook Marketplace.

Cybersecurity incidents continue to rise and with the advancement of AI bad actors can widen their attacks quicker. We are not immune from these attacks. We continue to see attempts against our users through phishing emails including from compromised emails and websites of vendors, community partners, and other government organizations. With these types of attacks time is critical in protecting our network.

With that said, if you become aware of any of our vendors, community partners, or other government organizations are potentially dealing with a cyber incident, please let IT know as soon as possible. When we are made aware of these incidents, we can bolster our IT security posture. The security of our network and resources is the responsibility of all of us not just IT. Your cooperation and assistance in successfully achieving that mission is vital.

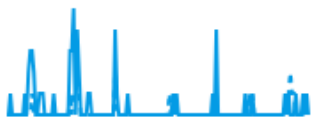
To illustrate what we are seeing, the graph below shows email traffic to our agency over a 7-day period. Within that 7-day time frame the agency received over 57k emails of which 11,066 of those emails were blocked for threats. These threats include attempts to deploy Malware which is used to deploy Ransomware, Phishing for user's credentials, and emails sent to other CCSO employees and/or departments by bad actors posing as CCSO employees asking for assistance with actions to include payroll redirection.

Inbound Email Overview

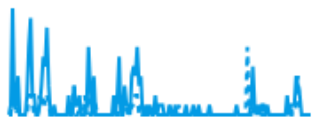


Connections Blocked
16,408
7.9% of total connections

Total Malware
55
↑ 223.5% vs Monthly Avg



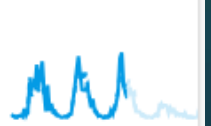
Total Phish
174
↑ 205.3% vs Monthly Avg



Total Spam
2,986
↑ 8.0% vs Monthly Avg

Total Impostor
24
↑ 100.0% vs Monthly Avg

Total Bulk
7,715
↑ 6.3% vs M




Dr. Phil
Dr. Phil
Dr. Phil

District Offices

District 1 Office Englewood
11051 Willmington Blvd.
Englewood, FL 34224
(941) 475-9005

District 2 Office Port Charlotte
992 Tamiami Trail
Port Charlotte, FL 33948
(941) 613-3245

District 3 Office Port Charlotte
3110 Loveland Blvd.
Port Charlotte, FL 33980
(941) 258-3900

District 4 Office Punta Gorda HQ
7474 Utilities Rd
Punta Gorda FL 33982
(941) 639-2101

Charlotte County Jail
26601 Airport Rd.
Punta Gorda, FL 33982
(941) 833-6300

Major Terry Branscome Training
25500 Airport Rd.
Punta Gorda, FL 33950
(941) 833-6281

District 5 Office Babcock Ranch
17000 Telegraph Street
Punta Gorda, FL 33982

CCSO
Integrity, Professionalism, Trust

Emergency
911
(Accepts Text)

Non-Emergency
Charlotte County
(941) 639-2101