



## CHAIRMAN'S NOTE

Dear Friends,

Supporting our Customers' Missions as our own is at the heart of our Mission. In this edition of ActionNews, we share how to avoid and defend against common scams. These include constant phishing attempts in e-mails, text messages and malicious websites with fake shopping and social media scams. Beware before you click.

ActionNet has leveraged our Integrated Team Service Delivery Excellence Model with our Service Desk, Software Engineering, & ServiceNow Development teams. The in-person collaboration with our customers in their Operations Center was extremely valuable to get first-hand experience in how they analyze hurricane patterns which have National and Global Impact.

We also share a trip down memory lane with our Team Videos since 2013 that include our ActionNeters across the country and around the world. Together we continue to make a difference.

Best wishes for the Summer Season!

Ashley W. Chen  
Founder & CEO

## IN THIS ISSUE

|  |   |
|--|---|
| Watch Out: 5 Common Computer Scams You Should Know ..... | 1 |
| ActionNet Videos, A Trip Down Memory Lane Speed.....     | 3 |
| Integrated Team Service Delivery Excellence .....        | 4 |

## Turning VISION into ACTION®

### Watch Out: 5 Common Computer Scams You Should Know About!

By Aaron Grafton, IT Ops Manager

**T**he Internet is a fantastic tool, but it is also full of sneaky scams designed to trick you out of your money or personal information. While scams can come in all shapes and sizes, some are more common (and more convincing) than others.

Our duty within is to keep our customers safe, but attackers do not stop after the workday ends. It is important to always remain vigilant not only in the office, but also at home or while using personal devices too. Here is a quick breakdown of the usual suspects so you can stay a step ahead.

#### 1. The "Tech Support" Trap

You are browsing the web when suddenly, a terrifying pop-up tells you your computer is infected. Or worse, someone calls pretending to be from Microsoft or Apple, offering to "help" or to "Run a free virus scan".

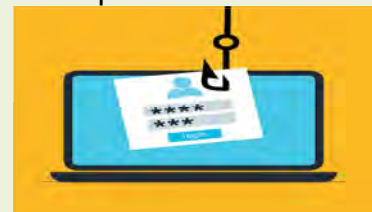


**Spoiler Alert:** They are scammers! They will ask for remote access to your computer or try to charge you for bogus repairs.

**Pro Tip:** Legitimate tech companies never cold-call or throw scary warnings on your screen. Most times, these pop-ups are limited to your web browser only. Close the tab and report to your IT Department.

#### 2. Phishing Emails

These emails look legitimate. They mimic your bank, Amazon, Netflix, sometimes even your coworkers and senior management. They will usually copy signatures, company logos and use email display names in order to try to look real and hope you let your guard down. Often they ask you to click a link to verify your account, fix a problem, or process a payment, but those links lead to fake websites that will steal your information and your money!



**Watch out for:** Odd sender addresses, typos, and a sense of urgency.  
**Always verify your senders before clicking on any links or taking any actions.**

continued on page 2



ActionNews®, the newsletter of ActionNet, Inc. is published to provide examples and applications of cutting edge IT topics and practices.

ActionNews® is published quarterly (March, June, September and December) as a service to its staff, customers, and potential customers.

### ActionNews Staff

Lead Designer

Karen Tepera

Contributing Authors

Timothy Gray

Aaron Grafton

ActionNet grants permission to educators and academic libraries to use ActionNews® for classroom purposes. There is no charge to these institutions provided they give credit to the author, ActionNews®, and ActionNet. All others must request permission at [actionnews@actionnet.com](mailto:actionnews@actionnet.com).

ActionNet, Inc.  
2600 Park Tower Drive  
Suite 1000  
Vienna, VA 22180  
[www.actionnet.com](http://www.actionnet.com)  
[info@actionnet.com](mailto:info@actionnet.com)

Copyright © 2025 by ActionNet, Inc.

**“Scammers are getting smarter, but so can you!”**

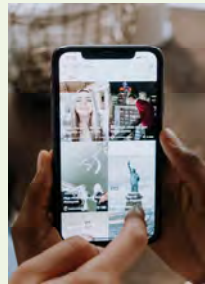
## Watch Out continued from page 1

### 3. Smishing & Vishing

Phishing is not just for email anymore. Now it is hitting your phone too:

- Smishing = scam texts - “Your package is delayed!”
- Vishing = scam calls - “You owe the IRS money!”

Best move: Do not reply, do not click, and do not call back. Block and delete.



### 4. Fake Shopping Sites

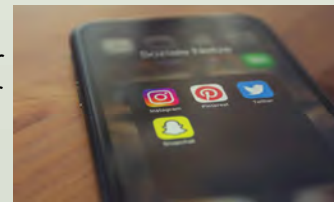
That amazing deal on designer shoes or the 50% discount on an iPhone. If it seems too good to be true, it probably is. Scammers set up convincing shopping sites to take your money and then vanish.



**Red flags:** No contact info, weird payment methods, or no customer reviews. Look out for fake Websites/URLs too. Just like phishing, attackers can make their site look like a legitimate online store.

### 5. Social Media Impersonators

Scammers pretend to be your friend, coworker, or relative online. Once they gain your trust, they could ask for money or gift cards, but all they need to access your personal info is for you to click “Accept” or “Add Friend”.



**Heads up:** If something feels “off”, it probably is. An online profile claiming to be your friend/relative that has no mutual friends on social media is likely a scammer. Reach out through another channel to confirm their identity before accepting any friend requests.

### Bottom Line

Scammers are getting smarter, but so can you! Be skeptical, slow down, and double-check before clicking anything or giving out information. A little caution goes a long way!

Our ActionNet IT Team is a constant advocate with awareness training to help our employees and customers recognize these threats, take the proper actions and report suspected scammer activity. A compromise at home could easily become a compromise in the office. Stay vigilant and stay safe!



We honor to the brave men and to the women who served in our nation. Their courage and sacrifice are the reason we enjoy the freedoms we have today—and we are forever grateful.

As a company that proudly supports federal agencies and national defense missions, we are especially grateful for those who have served and continue to serve. We also extend our heartfelt appreciation to the families of the fallen—your loved ones will never be forgotten.

To all who serve, have served, and those we’ve lost: Thank you for your service!!!



# ActionNet Videos, A Trip Down Memory Lane 2013 – 2025

By Ashley W. Chen, Founder & CEO

In December 2013, I was asked by our ActionNet Ohana to play the Ukelele and join the ActionNet Winter Pau Hana in Oahu, Hawaii. I replied, “Sure, I will play & sing if you find me a tambourine!” It was recorded and this started our ActionNet Video tradition. It makes me laugh when I look back at the videos.

**2013 - Aloha**



**2014 - Shake It Off**



**2015 - Lights, Canera, ActionNet**



**2016 - ActionNaeNae**



**2017 - Can't Stop The Feeling**



**2018 - Never Give Up**



**2019 - This Is Us**



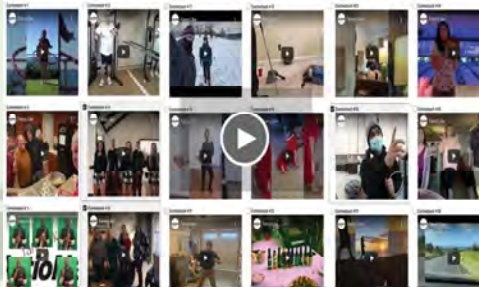
**2020 - Hall Of Fame**



**2021 - Turning Vision Into Action**



**2022 - Be Your Very Best**



**2023 - Be Kind**



**2024 - Shaka Shaka**



Since 2013, this has become part of our ActionNet Culture with many special shared moments in our history. A lot of people asked me, “Ashley, what are you most proud of?” My answer has been always “ActionNet Corporate Culture”. A Contract vehicle, \$100K; A Company, \$100M; A Corporate Culture, Priceless!

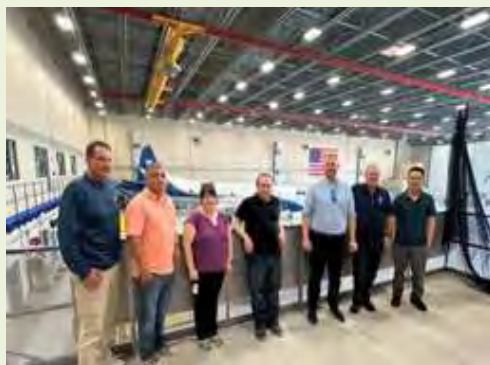
See the link here and enjoy! <https://www.actionnet.com/reflection-on-mothers-day/>

I hope you feel the Love, Joy & Energy after watching our ActionNet Videos. In 2025, we celebrate ActionNet Anywhere, Cheehooooo! Please enjoy our trip down memory lane.



# Integrated Team Service Delivery Excellence

By Timothy Gray, Program Manager



Recently, members of the ActioNet Service Desk and ServiceNow Development teams, who provide support to our DOC Customer, had the unique opportunity to visit their Operations Center.

This site visit served as more than just a tour; it was a vital step in deepening our understanding of the customer's frontline mission operations and strengthening our alignment with their technology needs. During the visit, the team toured the full facility, where they engaged directly with

onsite customer personnel and collaborated closely with ActioNet's onsite Software Engineering Group. These interactions offered valuable insight into the day-to-day challenges and innovations driving Mission success.

A highlight of the trip was an exclusive, hands-on tour of a hurricane reconnaissance aircraft. This highly specialized aircraft is an essential asset during hurricane season, as it is flown directly into severe storms to deploy scientific probes that collect critical atmospheric and storm data. Seeing this aircraft and its technology up close gave our team a new appreciation for the life-saving work that our customer conducts and the indispensable role that IT infrastructure plays in supporting these efforts.

Most significantly, this trip marked the first in-person collaboration between the Service Desk, Software Engineering, & ServiceNow Development teams. This face-to-face interaction fostered a more cohesive working relationship and enabled focused discussions on improving service delivery, user support, and IT responsiveness. These collaborative sessions laid the groundwork for more streamlined, agile solutions that will enhance operational continuity and resilience, both key to the broader mission to monitor and protect the environment.

## Partnership for Mission Success

The insights gained from this visit are not only critical to supporting the customer's Mission but also reflect ActioNet's broader commitment to excellence in government IT services. The tools, practices, and lessons emerging from this partnership have direct applicability across other federal agencies with similar operational demands, such as emergency response, environmental monitoring, and aviation logistics. By enhancing IT support in such dynamic environments, we contribute to the success of missions that have National and Global Impact.



- SBA Certified WOSB under NAICS 517111, 517121
- GWAC and IDIQ Contract Vehicles
  - GSA Alliant 2
  - GSA MAS
  - GSA OASIS Pool 1
  - CIO-SP3 SB/WOSB OTSB
  - DHA MHS GSP
  - DISA Encore III
  - ARMY ITES-3S
  - NAVY Seaport-NxG
  - FAA eFast
  - HHS SPARC
  - NRC GLINDA
  - SEC OneIT
- Past Performance on Large Contracts
  - DOE ITSS, \$1.2B
  - DOT COE, \$350M+
  - FAA ATO, \$300M+
  - CMS CIOIM, \$200M+
  - DOS CA DEDM, \$150M+
  - DISA CORENet, \$78M
- CMMI®-DEV V2.0 ML 4 with SAM
- CMMI®-SVC V2.0 ML 4 with SAM
- HDI Certified Support Center
- ISO 20000/27001/9001
- Approved Accounting System
- Approved EVM System
- Approved Purchasing System
- Approved Cost Estimating System



**“Face-to-face interaction fosters cohesive working relationships and enabled focused discussions on improving service delivery.”**