PREPARE FOR THE FUTURE OF VEHICLE CYBERSECURITY

ATA FLEET CYWATCH

Cybersecurity Program for Fleets

More Info &
ATA Fleet Cywatch Video:
• fleetcywatch.trucking.org

- Facilitates Information Sharing of:
  - Emerging Cyber-threats
  - Proper Countermeasures/Best Practices
- Provides Awareness, Prevention, & Mitigation of Threats
- Improves U.S. Road Transport Safety by Connecting Industry, Federal Enforcement & Trade Groups
- Provides Cybersecurity Training & Education
- Communicates Applicable & Emerging Standards

Cybersecurity
Protecting internet-connected systems from the stealing of information, money and the growing ability to disrupt, destroy, or threaten the delivery of essential information.

Access Points
Points of access where a hacker may gain entry to a vehicle network, commonly through Bluetooth, Wi-Fi, hotspots, In-Vehicle Infotainment (IVI), or Dedicated Short Range Communications (DSRC).

Malware/ Spyware
Software intended to infiltrate, damage or disable computers and pass information about a computer user's activities to an external party.

Virus
Code that can copy itself, typically having a detrimental effect, such as system or data destruction.

Helpful References

TMC CONNECT
tmcconnect.trucking.org

dhs.gov/topic/cybersecurity

NMFTA National Motor Freight Traffic Association, Inc.
nmfta.org/pages/HVCS

DG TECHNOLOGIES Vehicle Network Solutions
dgtech.com/cyber-tech

SAE INTERNATIONAL
saemobilus.sae.org/knowledgehubs/cybersecurity

CDSE
cdse.edu

CYBER TECH
#CYBERTECH
#VEHICLECYBER
dgtech.com/cyber-tech

SECURE YOUR VEHICLE AGAINST NETWORK THREATS

NETWORK THREATS

- Gaining access to company or vehicle data via wired or wireless network connections.
    - Wireless network connections include Wi-Fi, Bluetooth and cellular.
    - Wired network connections use cables to connect devices (USB, Ethernet, vehicle networks including CAN, etc.)
- Disrupting vehicle operations by infiltrating the system.
    - Computers with malicious diagnostic software.
    - Data monitoring and remote control of diagnostic sessions.
    - Piggybacked network access/data acquisition.
        - Unapproved users obtain access to data.
        - Typically occurs when a computer session is not closed.
        - Prevented by auto-initiated screensaver requiring re-login.
- Unauthorized access to the company's network.
    - Gaining access to the company networks and data.
    - Reducing network throughput by purposely saturating the network with large amounts of data.

SECURE YOUR NETWORK

- Make your wireless networks more secure:
    - Set up routers so that administrative wireless networks do not broadcast their presence.
    - Use obscure router names to help hide your networks identity.
    - Use the most secure wireless network encryption that your hardware supports.
    - Set up Guest Wi-Fi networks that do not access company-critical assets.
    - Use complex passwords that are not easily guessed.
- Use firewalls to help block untrusted network traffic.
- Open file sharing only as needed, and never share the computer's entire hard drive.
- Set up groups to limit access to job-related data on network drives.