

Port of Vancouver USA

Cybersecurity Awareness for the Maritime Community

PNWA SUMMER CONFERENCE

JUNE 2022



CHRIS CARTER, INFORMATION SECURITY ANALYST

Things you need to be doing today

- Multifactor Authentication.
- Training.
- Offline backups.
- Update software / end-of-life systems.
- Restrict administrative rights.
- Third-party access.
- Segment.
- Logging and monitoring.
- Have a plan.



Time to think different

***The most dangerous phrase in the English language is:
"It's always been done that way"— Grace Hopper***

- IT and cybersecurity staffing.
- Too small to be attacked.
- Primary focus on nation state threat actors.
- Focus on the perimeter.



Information sharing



LOWER COLUMBIA RIVER
MARITIME INFORMATION EXCHANGE



MS-ISAC[®]
Multi-State Information
Sharing & Analysis Center[®]



Weekly cyber tips

- Tip of the week.
- Phishing emails seen.
- What to expect to see.
- News impacting you or your family.
- Maritime/Port specific cybersecurity.
- Upcoming training/ webinars.

Opt-in

chris.carter@portvanusa.com

Cybersecurity Tips for the Week – Aug 9th 2021

Tip of the Week

For this week, some travel tips from the FBI Portland office tech Tuesday blog.

- Leave any devices you don't truly need at home.
- For those devices you do take, make sure to update all anti-virus and malware options before departing and again after returning home.
- Also, before you travel, make sure to change your passwords and PINs to new, strong options that you do not use at home. When you get back after your trip, change them again to another new option.
- Make a backup of your device in case your phone or laptop gets hacked or targeted in a ransomware attack. Remember—back-ups should always be kept offline so the bad guy can't access those as well.
- Make sure your wireless and Bluetooth auto-connect and remote-connect settings are off while traveling. They are handy to use when at home, but on the road you could accidentally connect to a malicious network without even knowing it.
- Likewise, it's tempting to take advantage of free WiFi options when in airports, hotels, coffee shops, and elsewhere—but be careful. If you can get in, so can a hacker. If you must connect to a public network, make sure to only use "https" sites. Also remember—never do shopping, banking, or access sensitive data—such as your health care portal—while on a public network.
- Using your own data network connection or using a VPN are always better options.

<https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/oregon-fbi-tech-tuesday-building-a-digital-defense-against-travel-tech-fails>

Phishing Report (Subjects of phishing emails seen)

- **Fake fax/ Voicemail messages are being seen across the country in the Maritime community. This continues this week with a very high volume.**
- Executive spoofing emails (Continue)— Usually ask for a task with urgency.
- Display name spoofing imitating several companies and/ or associations.
- Domain names with one to two letters off. Seeing a lot of this targeting the energy sector.
- Fake Invoices for Norton/ McAfee Security 360 Plan.
- Spoofed display name emails from the "IT Department" or "Support Department".
- Fake Office 365 phishing emails with subjects as "Account expired", "Messages is quarantine" or "Verify Your Mail ("Your name") To Avoid Deactivation" or anything warning you something is about to "Expire".

Tide Table – (What I expect to see this week)

- **Known contacts continue to get compromised.**
- Fake Office 365 messages. Password Expiration Notices seem to be popular.
- Spam calls and text messages.

Disclaimer: The information contained in this document is provided for informational purposes only. No warranties of any kind regarding this information are provided and shall not be held liable for any damage that arose out of the results of, or dependence upon this information.



Thank You

Chris Carter
Information Security Analyst
Chris.Carter@portvanusa.com
360-693-3611

