Maryland
DEPARTMENT OF INFORMATION TECHNOLOGY

The Weekly Cybersecurity Bulletin

Newsletter by Chazz Kibler

Hello Maryland,

Happy National Cybersecurity Awareness Month. We hope you are staying cyber-safe. For the last full week of the campaign, we will focus on recognizing and reporting phishing, and, as a bonus—because we love you so much, we're going to throw in some messaging about physical security absolutely free!

Physical Security PSA

Any organization with controlled access points should have some protocols to ensure their sensitive data remains protected.

Check out this PSA that shares some dos and don'ts regarding physical security.

Cybersecurity Tips of the Week

If you receive a suspicious email that appears to be from someone you know, reach out to that person directly on a separate secure platform. If the email comes from an organization but still looks 'phishy,' reach out to them via customer service to verify the communication.

When in doubt, reach out. Some of you have demonstrated the behavior mentioned in the tip regarding the initial newsletter, which is excellent! The initial newsletter contained external links, and some State employees reached out to DoIT for reassurance of the legitimacy of the links. Those cautious instincts should be used whenever you see a red flag in an email. If you're still unsure of what to look for, here are some tips to spot a phish:

1. They create a sense of urgency or claim to need help.
2. They ask for your personal info.
3. They want you to download a file or click on a link.

Speaking of links, click the button below to learn more.

More Phishing Tips

Keep Your Maryland Devices Secure

If you work remotely and connect your Maryland devices to your home network, it is essential that you take some basic steps to make your

home network more secure. Weak cybersecurity practices at home expose Maryland systems and information to risk. Check out the graphic to learn more.

PRECAUTIONS TO TAKE TO SECURE YOUR MARYLAND DEVICES AT HOME

ADMIN USE

Do not use administrator accounts for daily use.

WHAT'S NEW?

UPDATE

Update your systems, computers, phones, and any device connected to wifi.

KEEP HACKERS GUESSING

Change default passwords.

PROTECT YOURSELF AND OTHERS

Password protect your WIFI, including for guests.

POST WITH CAUTION

Be careful what you post online.

BACKUP DATA

Back up your personal systems to an external drive or cloud.

LOCK IT UP!

Lock your Maryland laptop screen when not in use.

SHARE YOUR KNOWLEDGE

Teach your family about phishing and social media security.

www.doit.maryland.gov

Reading Recommendations

Don't Take the Bait

No need to fear your inbox. Fortunately, it's easy to avoid a scam email, but only once you know what to look for. With some knowledge, you can outsmart the phishers every day. Check out the article below to learn more.

Read more

Can You Find the Security Violations?

Your mission, should you choose to accept it, is to launch this virtual simulation, identify as many security violations as possible, and click on each one to eliminate them before time runs out. Hot Spot is a simple yet quick, fun game highlighting some good cyber safety tips. It could be a good intro game at the start of a training session to gauge where people are at in terms of their cyber know-how.

Eliminate the Threats Here

Upcoming Events

Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY

Lunch & Learn

VIRTUAL EVENT
OCTOBER 25, 2023
12 - 12:45 P.M.

FOR MORE INFO
CYBER.TRAINING@MARYLAND.GOV
410-697-9396

Pack a lunch and come learn with the Maryland Department of Information Technology's Office of Security Management for a Virtual Lunch and Learn on **Oct. 25, 2023, from noon to 12:45 p.m.**

During the event, the OSM will reinforce key messages from the Cybersecurity Awareness Month campaign, such as enabling multi-factor authentication, using strong passwords, and more.

There will also be a security trivia game and a Q&A session to ask whatever cybersecurity-related questions you may have. If you have any questions, please email cyber.training@maryland.gov or call (410) 697-9396 for more information.

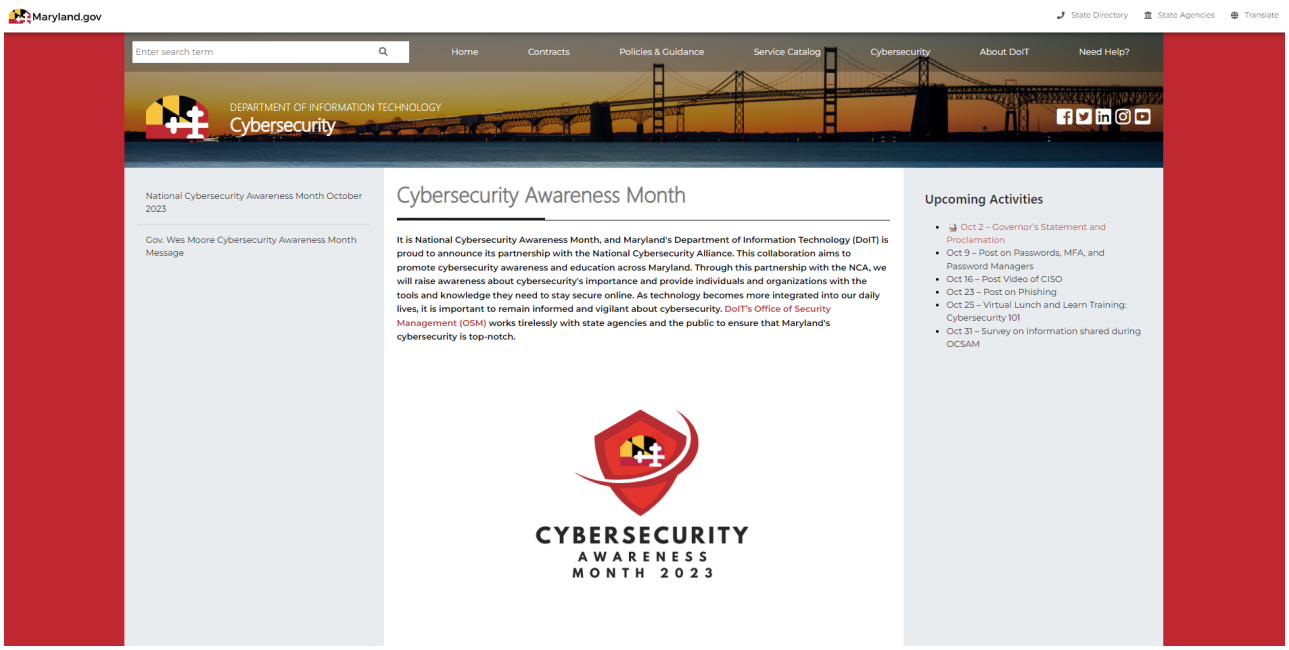
Note: The event will be recorded for those who can't attend.

Dial: (US) +1 470-327-0667 PIN: 944 643 294#

Time Zone: America/New_York

Video Call Link

Maryland State Security Awareness Portal



Stay in the Cyber-Loop All Month Long

If you haven't done so already, stop by our Maryland State Security Awareness Portal to stay up-to-date on the latest happenings regarding National Cybersecurity Awareness Month.

Stop on By

Your Input Matters

Comments for Chazz

Do you have some questions, suggestions, or content for the newsletter? If you do, I would love to hear from you. Feel free to email me at chazz.kibler@maryland.gov

Connect with me on LinkedIn

Maryland Department of Information Technology
100 Community Place, Crownsville
United States of America