Information Technology Division's Daily Communication
Remote Working Preparation Information
March, 23, 2020

Information for Agency Management

Remote Access options

- We continue to make progress on getting remote Access request for VPN/Citrix/RSA Tokens processed; incorrect information or not following process has slowed down our ability to get these processed and over to WaTech
- We are currently updating the latest spreadsheet information on how many request are completed so that we can send you an update
- WaTech is working as quickly as they can, but please remember we are one of many Agencies asking for the same service

TO ALL DNR EMPLOYEES

Remote Access options

HOW TO USE SKYPE DEMO

- ITD will be hosting another how to use SKYPE Demo on March 24, @ 1:00 PM AND 3:00 PM! To join the training, please use the following links:

- Join Skype Meeting
- Trouble Joining? Try Skype Web App
- Join by phone

- 1 (360) 407-3864 (DNR Information Technology Division) English (United States)
- Find a local number

- Conference ID: 1250039
- Forgot your dial-in PIN? | Help

VPN Difficulties on Friday, March 20:

Employees may have experienced issues trying to log in using the Virtual Private Network (VPN) last Friday, the 20th. If so, ITD has worked with WaTech, and those issues are now resolved. If you're still having difficulties, please log a ticket with our Service Portal and we'll help you get connected. https://help/

Cyber Security/Safety Updates and Reminders

In this time of change and uncertainty caused by COVID-19, we want to remind you to continue to practice good cyber-safety. News reports indicate threat actors are taking advantage of the coronavirus outbreak in new phishing email campaigns.

Threat actors are using public fear to increase the likelihood that users will click on a link or open an attachment.

In one campaign, the phishing email reportedly impersonates the U.S. Centers for Disease Control and Prevention, warning of new infections and promising to provide a list of active infections in the surrounding area if users click on a link.

Other phishing emails ask recipients to open an attachment to view safety measures regarding the spread of the virus.

As this latest attack method demonstrates, phishing campaigns are continuously evolving. It is becoming increasingly difficult to identify malicious emails. This incident provides a good opportunity for reminding staff to:

- Be suspicious of any emails that urge you to take action and try to create a sense of urgency.
- Never click on links or open attachments without first making sure the request is authentic.
- Call the sender by looking up their phone number independently.
- Never call a phone number included in a suspicious email or reply to the sender.

If you are a state employee and receive a suspicious email at work, please contact your information technology (IT) security staff immediately.