DigiKnow

CYBER SECURITY DEPENDS ON YOU

MDM - Just Another Acronym?

May 2022 | Issue 2022:5

SHIELDS UP
GUIDANCE FOR CYBER RESILIENCE

Every organization – large and small – must be prepared to respond to a disruptive cyber activity. In this month's column I am sharing suggestions for building cyber resilience at the state government level and at home.

STATE ORGANIZATIONS
Now is the time to review your COOP plans and ensure your processes are sound before you or one of your partners experience a disruption. Things to review in your COOP plan include:

• When was the plan last reviewed? Does it need to be updated?

• Discuss your COOP plan with your designated COOP Coordinator/Plan Builder.

• Does your COOP plan address cyber incidents or third party/vendor interruptions?

• Does your plan include contact information for all your vendors/customer partners?

• Have you exercised your Crisis Communication plan?

HOME PREPAREDNESS

A major cyber outage will affect everyday life, from gas pumps to banks to drugstores. Here are some prep steps all of us should take, courtesy of the Duke Clinical Research Institute.

• Have enough cash for 2-3 weeks of incidentals

MIS DIS and MAL Information

The United States' Cybersecurity and Infrastructure Security Agency's (CISA) Mis-, Dis-, and Malinformation (MDM) team is charged with building national resilience to MDM and foreign influence activities. Through these efforts, CISA helps the American people understand the scope and scale of MDM activities targeting elections and critical infrastructure and enables them to take actions to mitigate associated risks.

CISA DEFINITIONS

• **Misinformation** is false, but not created or shared with the intention of causing harm.

• **Disinformation** is deliberately created to mislead, harm, or manipulate a person, social group, organization, or country.

• **Malinformation** is based on fact, but used out of context to mislead, harm, or manipulate.

The Ukraine-Soviet conflict is a hotbed of Misinformation and Malinformation in all forms, print, broadcast, digital and social media. Many social media companies have been taking steps to limit misinformation on their platform; however, the volume and diversity of Ukraine-related posts challenges these systems. Here are a few examples Norton Labs' researchers found of Ukraine-related MDM:

A recent video was captioned to suggest Russian military jets flying in formation over Kiev in 2022. The footage was recorded in 2020 and shows the jets flying over Russia.

This tweet includes a video claiming to show the Ghost of Kyiv, a potentially mythic Ukrainian pilot rumored to have shot down five Russian jets. The video has since been debunked in multiple news outlets.

A deepfake video posted to YouTube and Facebook appeared to show Ukrainian President Volodymyr Zelensky surrendering to Russian forces and instructing Ukrainian soldiers to lay down their arms and surrender. The use of a deepfake video presented a new front in cyberwarfare.

Closer to home there's a conspiracy theory circulating online that claims 5G cellular networks cause cancer despite there being no scientific evidence to support this. The idea behind the false claim is that 5G radio waves are harmful to the brain. However, experts have debunked this, explaining that 5G radio waves cannot damage the DNA in our cells, nor can they penetrate past the skin, which acts as a protective barrier. This theory is an example of misinformation because it presents incorrect and out-of-context information as fact. The misinformation about high-frequency waves was first distributed by the state-run television network Russian Today, according to a 2019 New York Times report.

• Write down all important phone numbers on paper and have available

• Purchase and activate a cheap, non-smartphone (sometimes called a "burner") phone for emergencies

• Print out your most recent banking, credit card, and utility statements so that you have copies of all important account numbers and addresses

• Print out copies of all recurrent prescription medications

• If you use electronic locks on your home, be sure to know the physical code and/or be sure that each family member has physical keys

• Completely power down all computers, smartphones, tablets, etc. when not in use

And finally, to sleep tight:
• Log out of everything before bed; clear your cache and update your antivirus and VPN software.

Solomon Adote
Chief Security Officer

TIPS TO ASSESS DISINFORMATION AND MALINFORMATION

When you come across information with the following characteristics, consider it suspicious if:

• If it seems too good to be true
• If it plays to your own implicit biases
• If it elicits either extreme positive or negative emotions
• If it's not properly sourced, or the stats appear out of date

The best, baseline way to interrogate a source of information is to check:

• The author
• The organization
• The date it was published
• The evidence
• What other sources say

SOURCE - Brian Southwell, Director
RTI International

READ MORE CYBERSECURITY NEWS at DIGIKNOW!

Delaware Department of Information & Technology publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links or want to print a PDF copy, go to:https://digiknow.dti.delaware.gov/news/index.shtml?dc=newsletters