NORTH Dakota | Joint Information Center
Be Legendary.™ INFORMATION TECHNOLOGY

March 20, 2020

State officials provide COVID-19-related cybersecurity threat information

BISMARCK, N.D. – Chief Information Security Officer Kevin Ford, along with North Dakota's Joint Information Center leadership team, today provided information regarding widespread phishing and social engineering attacks malicious actors are using to exploit the coronavirus pandemic.

"The global spread and widespread news coverage of COVID-19 has created an opportunity for criminals to take advantage of people, making cyber hygiene equally as important as physical health and safety precautions." said Ford. "In the same way that we want all citizens to follow recommended guidelines to help prevent the spread of coronavirus, we want to encourage all North Dakotans to exercise extreme care when surfing the web or sharing information online."

Current cyber threats include social engineering activities like phishing emails that try to manipulate end users into clicking on links or attachments that are infected with malware or ransomware. These messages appear to come from a legitimate source, like the Centers for Disease Control or World Health Organization websites. They may also request personal information or ask users to provide financial information under the guise of donating to charities.

Malicious actors are also making fake maps with interactive dashboards. These maps use global data and look nearly identical to maps hosted by legitimate sources. However, the fake maps deploy malware that infects the user's computer. This can result in information-stealing, including stealing accounts and personal information, as well as creating secret accounts to control computers. There is also evidence that malicious maps are showing up in online advertisements and Google searches.

Users should only use coronavirus dashboards and websites from trusted and reputable sources like well-known news organizations, healthcare providers or universities. As long as this global health threat remains in the news and top-of-mind, hackers will try to exploit it for illicit gain. Top tips include:

- Be cautious and pay attention to links/attachments in unsolicited emails. If you aren't expecting the email or don't recognize the sender - don't open it.
- Use trusted websites like the CDC.gov. Bookmark trusted sites and avoid web surfing and clicking on random website links.
- Don't reveal personal information or financial info if asked over email.

Attorney General Wayne Stenehjem also issued a press release earlier this week advising North Dakotans to be cautious about coronavirus-related scams, including helpful tips.

NDIT is also playing an active role supporting the transition of most state government team members to work remotely following an executive order issued by Gov. Burgum yesterday. Although access to the Capitol and other state facilities will be restricted, state services will continue to be available in alternative ways, such as online. Burgum reinforced that state government remains open and functioning, but rather is modifying the way agency business is conducted during this unique and unprecedented time.

For the most updated and timely information related to COVID-19, visit the NDDoH website at www.health.nd.gov/coronavirus, follow them on Facebook, Twitter and Instagram, and visit the CDC website at www.cdc.gov/coronavirus.