CYBERSECURITY ADVISORY

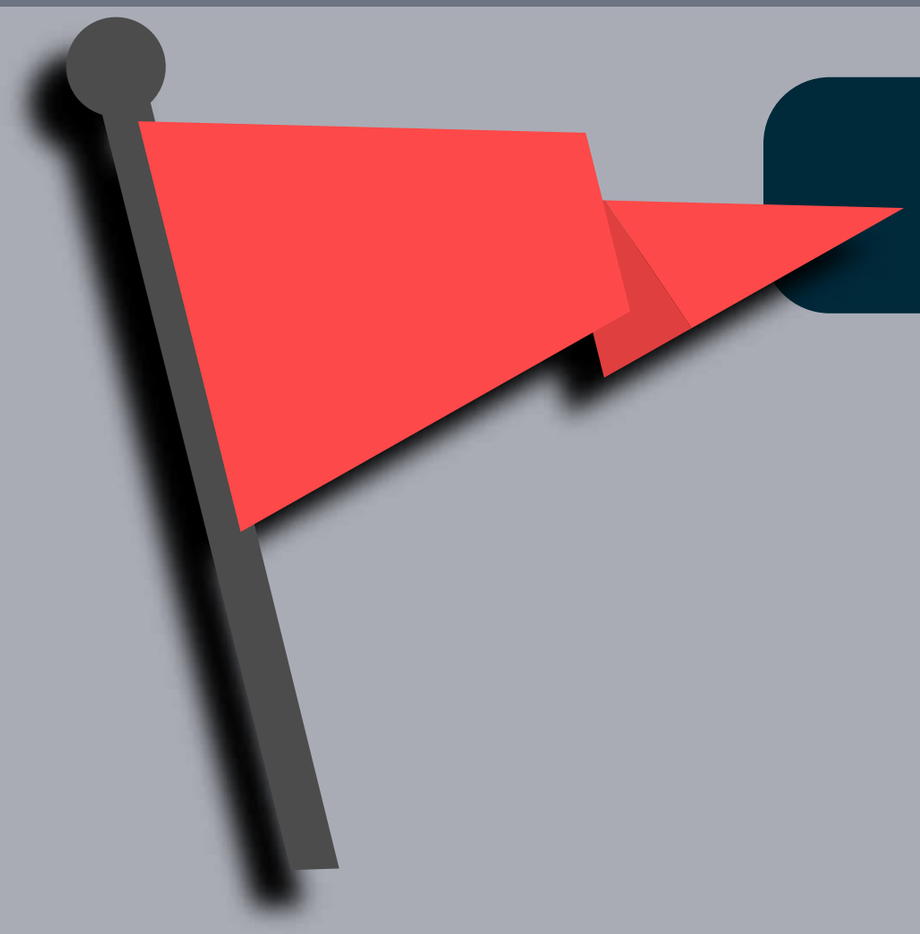
North Korea Using Social Engineering to Enable Hacking of Think Tanks, Academia, and Media

DPRK cyber actors are impersonating and targeting journalists, academic scholars, or think tank researchers in order to:

- Solicit responses to foreign policy-related inquiries
- Conduct a survey
- Request a resume
- Offer payment for authoring a research paper
- Request an interview
- Review a document

Victims

- People with both direct and indirect knowledge of policy information
- U.S. and ROK government employees with high level clearances
- Members of the military



Red Flag Indicators

- Requests to click “Enable Macros” to view documents
- Official emails received from unofficial email addresses (Google, Yahoo, Outlook, etc.)
- News media site emails not matching company’s official domain.

Mitigation

When in doubt, verify identity of the sender:

- Get contact info from organization’s official website
- Email to known good address

If you cannot verify the source:

- Do not enable macros on documents received
- Do not click on URLs provided
- Consider the risks before responding

Ministry of Foreign Affairs

Visit NSA.gov/cybersecurity-guidance to read the Cybersecurity Advisory.