Name and Affiliation
NARALO

Proposed Session Title
Capacity Building Session: DNS and Domain Abuse in the Digital Economy

Brief Description
The DNS remains the backbone of the Internet. It is a tried and tested system that is globally distributed and extremely scalable. People are continuing to explore new and creative uses for the DNS. DNS is facilitating the growth of the broader digital economy, digital transformation, and cybersecurity. This session will discuss these issues anchoring digital asset information in domain name and the latest technological developments as it relates to domain abuse, resulting from new domains that are designed to fool people into thinking they are files generated by their systems or files they have requested such as as .zip, .mov, .image, .photo. The problem lies in its association with a commonly used file format. .zip is universally recognized as a compressed file format, .MOV is also a commonly used file format to represent a movie and its usage as a TLD could lead to confusion and potential misuse. TLDs are the letters that come after the dot at the end of the domain name in an Internet address, like example.com, example.org, and example.zip. File extensions are the three letters that came after the dot at the end of a file name, like example.docx, example.ppt, and example.zip, example.mov, example.gif. The key to it all is misdirection. The attack chain is there to confuse and mislead users and security software. Criminals make extensive use of open redirects for example—web pages that will redirect you anywhere you want to go—to make it look as if their malicious URLs are actually links to Google, Twitter or other respectable sites. Here are some of the potential cybersecurity issues associated with the .zip TLD: Phishing attacks: The .zip or .mov TLD could be used to trick users into believing they're downloading a legitimate .zip file or movie when, in fact, they're being redirected to a malicious site. This tactic could significantly increase the success rate of phishing attacks. Malware distribution: Attackers could potentially use the .zip or .mov TLD to host and distribute malware. Given the association of .zip and .mov with downloadable files, users might be more inclined to download files from these domains, inadvertently infecting their systems. Confusion and misdirection: The .zip and .mov TLD could be used to create confusion, making it easier for cybercriminals to misdirect users and mask their activities. Target Groups: Cross-Community Session This Capacity building session will explore these issues related and seek to educate the users on how to avoid these pitfalls and succumb to hackers who are seeking to take advantage of people. Duration: 90 minutes

Rationale/Desired Outcomes
(nothing listed)

Which, if any, other community groups do you plan to involve in your session? Please explain your plans for working cooperatively with the group(s), including your contacts, skill sets sought, etc.
All of at large and GNSO

Session Leaders/Facilitators and Panelists/Presenters
(nothing listed)

Under which At-Large FY25 Strategic Priority Activities work track area does this topic fall?

tracks: https://community.icann.org/display/atlarge/At-Large+FY25+Strategic+Priority+Activities

(nothing listed)

Additional information or comments:

none