Emojis in Domain Names: A Security Risk for Everyone

Emojis have taken over every form of digital conversation, but they create a serious security risk when used in domain names. The ambiguity and confusion they cause in domains can lead to a denial of service or misconnections, and expose users to phishing and other social engineering attacks.

Why Do Emojis in Domain Names Create a Security Risk?

IDNA 2008, the current standard for internationalized domain names, prohibits emojis in domain names (see RFC 5892). Therefore, applications that follow the standard strictly do not support emojis at all; others process them inconsistently.

As discussed by the Security and Stability Advisory Committee of ICANN (see SAC095) and approved by the ICANN Board, the use of emojis in domain names also creates a number of problems from an end user standpoint:

- **Emojis can be too visually similar to distinguish**
  Especially when displayed in smaller fonts or by different applications.

- **Emojis are not displayed uniformly across all platforms**
  Because there is currently no standard specifying how they should look.

- **Combining emojis is unreliable**
  Some emojis can be combined (or “glued”) using a joining character to display them as a single symbol, but:
  - Systems that do not support combining will render “glued together” emojis as a sequence of separate emojis.
  - To the user, a single unmodified emoji may appear to be “glued together” when it is not.

- **Emoji skin tone modifications are ambiguous**
  Some emojis allow users to apply one of five skin tone modifiers. These can make emojis difficult to distinguish and are subject to interpretation.

---

**SAC095**: [https://go.icann.org/2EG96iN](https://go.icann.org/2EG96iN)