Health Information Compliance Alert

Pocket This TTPs' Breakdown

The feds often put cyber criminals' differentiated actions under the umbrella of tactics, techniques, and procedures, or TTPs for short. However, you may not realize that the **National Institute of Standard and Technology** (NIST) actually categorizes and defines each separate part of TTPs. Here's a quick outline of the different parts, according to NIST:

- **Tactics:** This is a high-level description of a cyber actor's behavior. An example might be the initial access a hacker gains to your network after usurping your organization's private data.
- **Techniques:** This is a detailed description of the infiltrator's behavior in the context of a tactic. Email phishing is an example of the technique or tool that a hacker uses to break into your system.
- **Procedures:** These low-level details are a subcategory under techniques and are generally the order of operations that threat actors follow. For example, a ransomware attacker might have a checklist with certain steps to tick off to reach their goal of encrypting your data.