MDS Alert

Reader Question: Make Documentation Easier With This Update

Question: How often should we change our passwords for our computers? Right now our information technology consultant set things up so that our passwords expire every 30 days, but my staff is a bit overwhelmed with the need to constantly remember new passwords, and I think the efforts are distracting them from their jobs. I'm always trying to remove obstacles to documentation, and this feels like a big one.

Utah Subscriber

Answer: Though frequent password changes have been the norm for years, the National Institute of Standards and Technology (NIST) updated their guidelines and recommendations concerning identity security. If your team members and staff are already struggling with the demands of providing excellent care, removing the mental barrier of frequent password changes could help facilitate more and better documentation.

"Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets. Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator," NIST says (all emphasis original).

With this advice, encourage your IT manager and all your staff who use computers to choose a strong password (or "secret," in NIST parlance) for each function requiring a password, and don't require any changes unless you must.

Additionally, NIST does not recommend requiring that passwords have multiple composition rules, like mixed-case letters, numerals, or special characters.

"These rules provide less benefit than might be expected because users tend to use predictable methods for satisfying these requirements when imposed (e.g., appending a ! to a memorized secret when required to use a special character). The frustration they often face may also cause them to focus on minimally satisfying the requirements rather than devising a memorable but complex secret," NIST says.

When updating your password rules and regulations, NIST recommends creating a "blacklist" of passwords that are common enough to be vulnerable to attack.

To read the rest of the NIST updates, go here: https://pages.nist.gov/800-63-3/.