Strong User Authorization

Your Password Shouldn't Be "password"

CyberSecure Fleming Group Project Winter 2023
Prof Mamdouh Mina, Computer Security & Investigation

Some Definitions

USER AUTHENTICATION – This phrase refers to how and by what process a person gains permission to access certain systems and information from a computer system. This is typically managed by an IT section or department.

USER AUTHORIZATION – This is how permissions are divvied up to the users. It is used to limit access to a system or information based on the needs of the organization. While IT also manages this as well, it is in concert with the supervisors assessment of employee needs.

PASSWORD MANAGER – A software application for the creation, recall, and storage of employees passwords. It is not strictly needed for CyberSecure certification, but is a fairly popular way for users to manage many usernames and passwords, and can help make things easier. Access to a password manager account should be limited to the employee and the IT lead.

TWO-FACTOR AUTHENTICATION – A type of authentication that is used to confirm or deny the identity of a user. It is done by the use of two different devices or pieces of software. It is strongly recommended to use this, however, company policy should dictate usage and what constitutes a valid second device.

Scope Statement Examples

TWO-FACTOR AUTHENTICATION:

All employees of Fuzzy Bunny LTD will make consistent use of two-factor authentication. This policy will apply to all staff and non-staff members of the organization and all applicable systems. The focus will be on the following:

- Cloud Admins
- All Remote Access
- Financials
- System Admins

PASSWORD CREATION:

All passwords must be a minimum of 16 characters long. The default passwords on new accounts/devices are to be changed immediately upon assignment to an employee. They will contain, at minimum:

- One upper-case letter
- One lower-case letter
- One number
- One special character (ex: !@#$%^&*())
- No spaces

PASSWORD MANAGEMENT:

**NOTE - A decision must be made at the company level about whether to use a password manager. If yes, policy must be created and written governing its use).*

Passwords at Fuzzy Bunny LTD will not be shared with anyone. "PasswordsRUs" is the only password manager permitted on company property. Passwords and other login information is not to be written down or left out on work surfaces. Auto-login features are to be disabled for security purposes.

PASSWORD UPDATES:

NOTE – CyberSecure does **NOT require a company to have a policy of timed (every 6 months, every quarter, etc.) password changes. If a company wishes to have this, it will not reflect either negatively or positively on certification. There must be a policy of password changes in the event of a suspicion or confirmation of a breech/compromise of the system. This breech could be an individual password or an entire section of passwords.*

ENFORCEMENT:

It is the purview of the IT section at Fuzzy Bunny LTD to implement password policies, in conjunction with the needs of the employees and the company goals.

Other Certification Requirements

An overview of the usage of two-factor authentication needs to be provided to all users. It would probably be best to make this as easy to understand as possible, to avoid confusion. Also, if there are any devices that will not require two-factor authentication, there must be a provided explanation as to why it will not be needed.