Boost Your Security with **Multi-Factor Authentication**

Multi-Factor Authentication (MFA) adds a second layer of security to help prevent anyone other than an authorized individual from gaining access to a secure system.

Access requires the following different types of authentication:

Something you know:
i.e., your username and password

Something you have:
i.e., a USB hardware token, or mobile device, phone, etc., that allows you to confirm your identity

Something you are:
i.e., biometrics like a fingerprint, retinal scan, or facial recognition

The most common and convenient forms of MFA include a mobile phone with an MFA application installed, a text message that is generated with a series of passcodes after the initial password is provided, or a phone call that allows you to authenticate that it is you who is attempting to connect.

Even when hackers successfully phish a user's login ID and password or obtain passwords through installed malware, their access to a system protected by MFA remains unsuccessful without the second factor.

REDLENS INFOSEC™