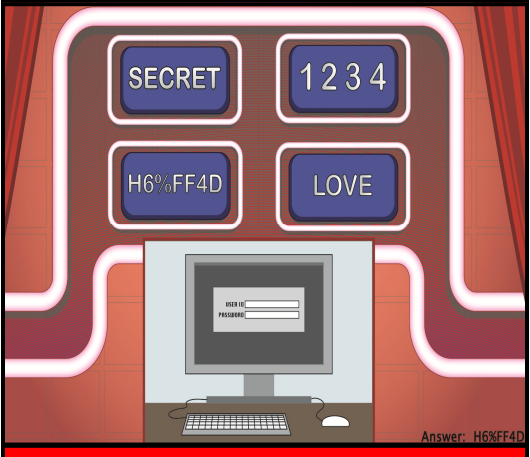
WHICH OF THESE IS A STRONG PASSWORD?



HELPFUL TIPS

- Longer is stronger. Each character that you add to your password increases the protection that it provides many times over. Passwords should be 8 or more characters in length; 14 characters or longer is ideal.

- Use a combination of upper and lowercase letters, numbers, and symbols. The greater variety of characters that you have in your password, the harder it is to guess.

- Use words and phrases that are easy for you to remember, but difficult for others to guess.

- Never share your password with anyone. As the owner of the account you are responsible for all activity (legitimate or illegitimate) associated with that account.

BEWARE OF PHISHING EMAILS

HELPFUL TIPS

- Never respond to requests for personal information via e-mail. legitimate businesses will never ask for passwords, credit card numbers, or other personal information in an e-mail.
- Do not enter personal information in a pop-up screen.
- Do not click on any links listed in an e-mail message. Copy and paste the URL into your browser.
- Use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly.
- Review credit card and bank account statements as soon as you receive them to check for unauthorized charges.

DISPOSE OF INFORMATION PROPERLY

HELPFUL TIPS

- Don't store confidential information longer than necessary.
- It is especially important to properly dispose of information that contains personal, private and sensitive information (PPSI).
- Read/writable media (including your hard drive) should be "wiped" using Department of Defense (DoD) compliant software. Software that meets DoD compliance standards can be downloaded from the Internet at no cost.
- CDs and DVDs should be physically destroyed. Shredding is a good option.
- Paper documents that contains PPSI should be shredded and destroyed when no longer required.
- At work, follow your organization's retention and disposal procedures.

PROTECT MOBILE DEVICES

HELPFUL TIPS

- Password-protect your portable device.
- Be sure all critical information is backed up.
- Disable Bluetooth when not required.
- Make sure your firewall and anti-virus are up-to-date.
- Store your portable devices securely.
- Record identifying information such as a serial number and label your equipment if possible.
- Report the loss or theft to the appropriate authorities as soon as possible.

CYBER SECURITY IS OUR SHARED RESPONSIBILITY

MULTI-STATE
Information Sharing & Analysis Center™

A DIVISION OF CENTER FOR INTERNET SECURITY

www.msisac.org