Computer Know How Series

Presented by Adam Lacey (*Applications Etc*) 916-813-7819

Password Security and Management – Thursday February 14th 2019 @ 2pm

http://www.aehost.net/morpd or http://www.morpd.com

Password Security is the most important part of computing and privacy today. This important issue is the center point of most hacking and access to your resources. Managing your online presence can be a full-time job but it is ultimately for your privacy and protection. This is due to the average user having approximately 150 or more online accounts.

1) Password Security
    a. Criteria to construct a strong and complex password.
        i. A length of 8 characters minimum and some services have 32 character maximum.
        ii. Use complexity in your passwords by combining a minimum 3 out of 4 types of the following characters; Upper Case letters (ABC), Lower Case letters (abc), Numbers (123) and Symbols (!@#$).
    b. Enable Enhanced Security.
        i. Use Two Factor Authentication (2FA) via email or text message to your mobile device.
        ii. Use Authentication Apps as a security key or approval method.
    c. Recommendations
        i. Create **strong** and complex (ex: c0mp/3x) passwords or passphrases.
        ii. Consider using passphrases instead of passwords (Ex: kidsjump2high + complexity = k1d$juMp2H1gh).
        iii. Avoid using the same password for multiple accounts.
        iv. Change your passwords frequently (some recommend every 3-6 months).
        v. Change your passwords immediately if an account is compromised (all accounts with same password).
        vi. Do NOT write down or store passwords in an insecure manner.
        vii. Do NOT share your passwords.
        viii. Do NOT use auto login/saved passwords.
        ix. Do NOT use dictionary words.
        x. Do NOT use numbers at the beginning or end only.
        xi. Do NOT use any part of your username.
        xii. Do NOT use personally identifying information.
        xiii. Do NOT use publicly available information (Facebook, etc.).
        xiv. Lie when setting up Security Question answers (Some personal info can be found on your Social Media).
        xv. Use Enhanced Security when possible but especially on important accounts (financial and email).
2) Password Management (Rein in the madness.)
    a. Operating System Credential Managers
        i. Windows Credential Manager (MS Edge and other MS Apps) or Apple Keychain and iCloud Keychain.
    b. Password Managers (3rd party) and Lists
        i. We don't prefer them, but they can be useful to help store and protect your passwords. (see links)
        ii. Spreadsheet or document lists are not recommended but can be a necessary evil. If lists are used, encryption and password protection of the document are recommended. (MS office offers both)
        iii. Use Authentication Apps when possible. Microsoft Authenticator, Google Authenticator, LastPass, etc.

3) Resources/Links
    a. Guidelines for Password Management - https://www.cmu.edu/iso/governance/guidelines/password-management.html
    b. Password management - https://en.wikipedia.org/wiki/Password_management
    c. The Best Password Managers for 2019 - https://www.pcmag.com/article2/0,2817,2407168,00.asp
    d. Uncovering Password Habits - https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic
    e. Your Password Has Expired and Must Be Changed - http://www.infotoday.com/it/apr16/Kennedy--Your-Password-Has-Expired-and-Must-Be-Changed.shtml
    f. Check if your information has been compromised - https://sec.hpi.uni-potsdam.de/leak-checker/search?lang=en