NEVADA
CYBER CLUB

Cyber Clinic
Guidance

WHY IT MATTERS

Misuse of account credentials or personal information can cause significant personal, professional, and financial harm. Protecting your Identity involves managing multiple account credentials (IDs, usernames, e-mail addresses), using effective authentication codes (PINs, passwords, biometrics) and preventing the disclosure of credentials, authentication codes, and personal information.

Managing account credentials effectively and using stronger authentication will reduce the risk of accounts being "stolen" or compromised. The more important the account (banking accounts, e-mail accounts) the greater the need for stronger authentication techniques such as passphrases, two-factor authentication, and biometrics. Weak passwords and passphrases are one of the most common flaws in cybersecurity.

I

IDENTITY

WARNING: The incorrect use of authentication techniques can prevent account access. **Use with extreme caution.**

WHAT TO KNOW

Authentication is the process of determining whether someone or something is who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of login passwords or passphrases; knowledge of these are assumed to guarantee that the user is authentic. Thus, when you are asked to "authenticate" to a system, it usually means that you enter your username and/or password for that system. Additional forms of authentication, commonly referred to as two-factor or multifactor authentication, consist of combinations of authentication techniques (i.e. password plus fingerprint scan). An account using two-factor authentication is more difficult to compromise because both factors must be correct.

"What is authentication?" - Indiana University	https://kb.iu.edu/d/alqk
Wikipedia Article: Authentication	https://en.wikipedia.org/wiki/Authentication

WHAT TO DO

Use a Passphrase. While passwords and passphrases essentially serve the same purpose – providing access to secure services or sensitive information – passwords are generally short, hard to remember and easier to crack. Passphrases are easier to remember and type. They are considered more secure due to the overall length of the passphrase and the fact that it shouldn't need to be written down.

"What is the difference between a password and a passphrase?" – University of Iowa	https://its.uiowa.edu/support/article/2549
Diceware Passphrase Generator	https://www.rempe.us/diceware/#eff

Use a Password Manager. Password managers are applications that store information for you (conventionally passwords, but they will also work for passphrases, PINs, and security questions). They encrypt that information and use a single strong master password that you enter when you want to access your other passwords.

"Use a password manager" – Univ. of Illinois, Urbana-Champaign	https://security.illinois.edu/content/use-password-manager
"The Best Free Password Managers of 2016" – PC Magazine	http://www.pcmag.com/article2/0,2817,2475964,00.asp

HOW TO DO IT

Android – Two-factor Authentication	**iOS** – Two-factor Authentication
https://www.google.com/landing/2step/	https://support.apple.com/en-us/HT204915

WARNING: *Changes to device and application settings can have unintended consequences and may interfere with normal operation. Improper use of encryption and authentication can cause a loss of data and prevent access. Please do not attempt to apply any guidance that exceeds your level of knowledge and familiarity with your device or application. All guidance is provided "as-is" from referenced sources. User assumes responsibility for any changes made to their device and/or applications.*

Updated guidance at: nevadacyberclub.com/cyber-clinics/guidance