Security Objective Mapping  
CYB 200 Cybersecurity Foundations

Sergio Mateos

Southern New Hampshire University

|  |  |  |  |
| --- | --- | --- | --- |
| TOPIC | CATEGORY | JUSTIFICATION | SOURCE |
| Ensure all computers you use, or control have an up to date, supported antivirus software installed. | Availability | The information should always have the latest update to properly take care of any bug | Hoffman, C. (2020, August 25). *Why you should update all your software*. How. https://www.howtogeek.com/686687/why-you-should-update-all-your-software/ |
| Turn on your operating system's firewall. | Confidentiality | If the computer is connected to a network without firewalls, malicious user could leak data | Rusen, C. (2019, May 1). *Windows firewall: Your system’s best defense*. How. https://www.howtogeek.com/school/windows-network-security/lesson4/ |
| Install and use a reputable anti-spyware program. | Confidentiality | Anti-spyware prevents leaking of confidential information | Kaspersky. (2023, April 19). *How anti-spyware provides the best defense for your computer*. usa.kaspersky.com. https://usa.kaspersky.com/resource-center/preemptive-safety/antispyware-provides-best-computer-defense |
| Ensure that the anti-virus software is running at all times. | Availability | It’s important to always run antivirus programs to protect PC from threats on an ongoing basis | *Microsoft*. Microsoft Support. (n.d.). https://support.microsoft.com/en-us/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963 |
| Change your password every 120 days. | Confidentiality | The change of password during certain period will prevent access from malicious users | Writer, S. K. (n.d.). *Password changes to be required every 120 days*. The Simpsonian. <https://thesimpsonian.com/13442/uncategorized/> password-changes-to-be-required-every-120-days/ |
| Open email attachments only if you are expecting them from people you know. | Integrity | If the information is not provided from and expected person, the information will be invalid. | *Using caution with email attachments: CISA*. Cybersecurity and Infrastructure Security Agency CISA. (2023, June 22). https://www.cisa.gov/news-events/news/using-caution-email-attachments |
| Always use strong passwords and keep them secret. | Confidentiality | The use of strong password makes the illicit access to your account harder for malicious users | LaSalle, C. (2022, October 13). *Cybersecurity Awareness Month 2022: Using strong passwords and a password manager*. NIST. https://www.nist.gov/blogs/cybersecurity-insights/cybersecurity-awareness-month-2022-using-strong-passwords-and-password |
| Lock your keyboard when you step away from your computer for even a moment. | Confidentiality | Locking the keyboard will prevent to access to malicious user to your station | Mihaila, R. (2021, July 6). *How to lock your keyboard and mouse: 3 ways to keep your PC safe*. MUO. https://www.makeuseof.com/tag/3-ways-lock-keyboard-mouse-computer-safe-unwanted-guests-windows/ |
| Never check your Purdue email account on a "free" or "public" Internet kiosk or Internet Café.. | Availability | Public spaces are perfect target for malicious user to access toy your account via malicious hot spots | Johansson, A. (2018, February 4). *Is your email account secure on public WIFI?*. HuffPost. https://www.huffpost.com/entry/is-your-email-account-sec\_b\_14595516 |
| Do not set your computer to automatically log in. | Confidentiality | The automatically access to your account provide all the information necessary for a malicious user to access to your personal information | Hoffman, C. (2015, July 1). *Why you shouldn’t automatically log into your windows PC*. How. https://www.howtogeek.com/220660/why-you-shouldn%E2%80%99t-automatically-log-into-your-windows-pc/ |