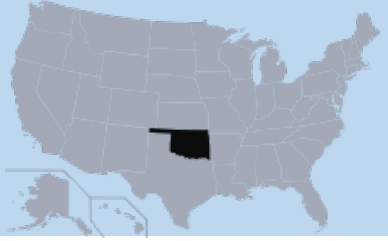
Cybersecurity Info Sheet



Best Practices

•Use strong passwords that are hard to guess and are at least ten characters and combines uppercase and lowercase letters, numbers, and special characters. Even better, use a long Phrase that would be easy for you to remember but uses mixed characters. And keep your password confidential.
•Do not use government email addresses to register for non-work related accounts/services.
•For different accounts, use different passwords. If you think the integrity of your account is lost, change password immediately.
•Use two-factor authentication where it is supported.
•Be alert and watch out for scams and phishing emails. Do not open email attachments or links/hyperlinks from unknown sources.
•Report all suspicious cyber-incidents to the security representative or the manager. If unsure, ask!

Helpful Links:

https://privacypros.io/cyber-security/
-Comprehensive article about being more secure online, why data security is important, staying safe on social media, protecting yourself and your company and more!

https://www.security.org/how-secure-is-my-password/
-A fun and interesting tool that will show the strength of your password and how many years it would take for a computer to crack it.

Interesting Facts

1. 95 percent of cybersecurity breaches are caused by human error. (World Economic Forum)
2. The worldwide information security market is forecast to reach $366.1 billion in 2028. (Fortune Business Insights)
3. The U.S. was the target of 46 percent of cyberattacks in 2020, more than double any other country. (Microsoft)
4. 68 percent of business leaders feel their cybersecurity risks are increasing. (Accenture)
5. On average, only five percent of companies' folders are properly protected. (Varonis)
6. 54 percent of companies say their IT departments are not sophisticated enough to handle advanced cyberattacks. (Sophos)
7. Cyber fatigue, or apathy to proactively defending against cyberattacks, affects as much as 42 percent of companies. (Cisco)
8. 43 percent of all breaches are insider threats, either intentional or unintentional. (Check Point)
9. Data breaches exposed 22 billion records in 2021. (RiskBased Security)
10. Approximately 70 percent of breaches in 2021 were financially motivated, while less than five percent were motivated by espionage. (Verizon)
11. In 2021, nearly 40 percent of breaches featured phishing, around 11 percent involved malware, and about 22 percent involved hacking. (Verizon)
12. There were 1,862 recorded data breaches in 2021, surpassing the 2017 record of 1,506 breaches. (CNET)
13. The top malicious email attachment types are .doc and .dot which make up 37 percent; the next highest is .exe at 19.5 percent. (Symantec)
14. An estimated 300 billion passwords are used by humans and machines worldwide. (Cybersecurity Media)
15. Around 40 percent of the world's population is offline, making them vulnerable targets for cyberattacks if and when they do connect. (Data Reportal)

Report any and all attempts of personnel attempting to gain information or access to you, yours or a coworker's information systems, or US Army/Government and US Industry systems!

U.S. Army Counterintelligence,
Oklahoma Resident Agency
2703 Pitman Street, Ft. Sill OK
Office: 580-442-8157
1-800-CALL-SPY
https://www.inscom.army.mil/isalute/