Security Awareness / Trends

April '18

2018 INFORMATION SECURITY POLICY

Security is Everyone's Responsibility

Account and Password Policy

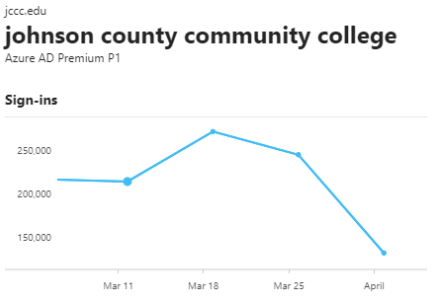
The focus of this newsletter is on the policies that directly apply to JCCC user accounts and passwords. The password policy states, "Computer accounts and passwords to JCCC Technology and Communication Systems may not be shared." Do not allow family members, co-workers or others access to your password. A natural extension of this policy should also include the re-use of this password on other personal accounts. **When you register for other services online choose unique passwords.** Be thorough in reading the Terms of Service and understand how these entities treat your personal credentials and information. **In order to comply with this policy staff need to protect and keep private their JCCC password.**

The policy also addresses the use of cloud, social media and mobile applications, "Users should be aware that some Technology and Communication Systems are controlled by third parties." In today's cloud and mobile environments it is very common for these applications to allow you to sign-in with an existing account. **Do not use your JCCC email address or credentials to affiliate with these services unless it is for official College business and even then should be done with care.** Utilize personal accounts when signing up for services like Amazon, Netflix and banking.

Homeland Security
Science and Technology

Attacks on Accounts and Passwords

Recently the Department of Homeland Security released an alert. According to information derived from FBI investigations, malicious cyber actors are increasingly using a style of brute force attack known as password spraying against organizations in the United States and abroad. JCCC was targeted in a "Password Spraying" attack, which is an attack against multiple accounts using a known password database. The attacker leverages compromised password such as those disclosed in breaches against LinkedIn, Adobe and others. These passwords are then "sprayed" across all accounts on another login portal, such as JCCCC's login portal, in attempt to gain access. This is the risk of password re-use, using the same password across multiple accounts.



This graph shows the active attack pattern that we experienced. The attempted logins to our environment spiked to almost 300,000 during its peak. As we protect our infrastructure we will include plans to implement Multifactor Authentication (MFA). This protection is essential with our use of single sign-on (SSO) and federated authentication.

Brute Force Attacks Conducted by CyberActors in 2018, https://www.us-cert.gov/ncas/alerts/TA18-086A (accessed Mar. 2018)
Use of Technology and Communication Systems, http://www.jccc.edu/about/leadership-governance/policies/information-services/college-technology-communication-systems/ (accessed Apr 2018)
Technology Security Tips: Passwords, http://www.jccc.edu/about/leadership-governance/information-security/passwords.html (accessed Apr. 2018)