Dear Colleagues,

This message is to notify you of changes coming to the network firewall configurations beginning the week of March 25, 2019. After considerable dialogue with faculty leaders across the District, we have reached consensus to remove the website filters for certain sites categorized as high risk for malware and viruses; sites containing adult content and those that are gambling related. Beginning next week, the following message will be displayed when an individual elects to reach a url that has the aforementioned categorizations, with the ability to continue to the site:

"*The website you are attempting to access has been categorized as highly prone to malware and viruses by the District's internet security blocking system. Among such websites are many containing adult content or related to gambling. Additionally, the District's Acceptable Technology Use Procedure stipulates that the technology systems are only intended for instructional and work related purposes and that surfing inappropriate websites such as those that are sexually explicit, gambling related, or that subscribe to hate propaganda, are prohibited. Finally knowingly or carelessly introducing any invasive or destructive programs (i.e. viruses, worms, Trojan Horses) into District computers or networks is prohibited.*

If you would like to continue to the site click on "continue" otherwise close your web browser. Should you continue, the access will be logged.

Please be aware that the following sites will retain their blocked status:

- Command and control – sites that infected computers attempt to communicate with in order to send data they capture then "listen" to future instructions on what to do next.
- Hacking – known sites that hack or advance hacking.
- Malware – sites that spread malware and/or viruses.
- Peer-to-peer – sites that allow the illegal sharing of music/videos/movies - most of which are copyrighted. This block has been in place for the past eight years.
- Proxy avoidance – sites that are used to "hide" where one visits and is also used by malware/viruses and ransomware to hide their tracks once computers are infected.

The Chancellor and I would like to thank the Academic Senate Presidents and faculty members across the District who participated in the dialogue. Our collective goal is to support academic freedom and educational equity while balancing the need for security and safety of our network infrastructure. We will monitor this process and re-evaluate as a team in the coming months.

Thank you,
Mojdeh

Mojdeh Mehdizadeh
Executive Vice Chancellor, Education and Technology
Contra Costa Community College District
500 Court Street | Martinez | CA | 94553