Monthly InfoSec Newsletter

March 2021

Ransomware as a service or RAAS is a growing trend in cybersecurity, as it is becoming easier for attackers to pay a company to utilize these services. To give the readers some more information we have provided a video link about RAAS, by an expert on the subject.

https://www.youtube.com/watch?v=Kgx_teNOo-U

Hopefully, this will give you a good explanation on how the services work.

Top 4 Cybersecurity tips

This month we wanted to highlight 5 personal security tips to keeping yourself protected from cyber-attacks.

1. Keep your software updated

   The **second Tuesday** of each month is the one most commonly referred to as Patch Tuesday. That's when **Microsoft releases security-related updates** for Windows (desktop and server editions), Office, and related products. Turning on automatic updating can help keep you up to date and safe. If you're using a work computer at home, you'll need to bring it to campus once a month to update your Security Patches.

2. Anti-virus and firewall

   Make sure your firewall is turned on and that your anti-virus software is set to automatically update and run a full scan nightly (at least weekly).

3. Strong passwords

   Ensure that you create complex passwords and change them every 60 to 90 days. NEVER reuse your passwords for other websites. ALWASY use complex passwords. A good rule of thumb is to use something simple to remember, a minimum of 16 characters that include numbers, special characters and a combination of upper and lower case letters. An example: *IL0v3CSUPu3bl02021!

4. Two-Factor Authentication

   Most websites today add another layer of security by allowing you to use your phone or email as a verification method to protect against unwanted password changes. An internet search on "setting up two-factor authentication" for the import online services you use can get you started.

CSU Pueblo Disaster Recovery Tabletop Exercise

On March 10th, the IT department of CSU Pueblo will be conducting a virtual tabletop exercise (VTTX) to test our IT Disaster Recovery Plan (DRP). The VTTX will replicate the conditions of an IT disaster on our campus. By performing these tests, the IT team will be tested in their ability to mitigate this disaster and get the system(s) back online. The DRP VTTX is an annual tests to ensure that our IT team can respond to a natural, manmade, or hardware incident in a timely and efficient manner.

Campus InfoSec Stats Last 30 Days