VT's 2-Factor Authentication (2FA) - What You Need To Know

- What is 2FA?
  - Something you know (username & password).
  - Something you have (landline, cell phone, USB/hardware token, pre-generated passcode).
- Why do we need 2FA?
  - Users credentials continue to be acquired through various techniques (phishing, brute force password attempts, and malware like key loggers).
  - If the bad people get your credentials they still can't access your resources since they won't have your 2nd factor.
  - Compromised email accounts have been the primary reason why the @vt.edu email domain continually gets blacklisted and you can't communicate with your colleagues outside of VT. 2FA will help prevent this!
- All VT services (Banner, HokieMart, Canvas, WebOutlook, …) that require authentication will eventually have 2FA implemented. A lot of them already do.
- As of July 4th 2016 there will no longer be a "Not Now" option so we will all have to use the new system. I've been using it for months now and it's amazing how fast you get used to it.
- Each service type should have a "Remember me for 7 days" option. If selected, you will only have to 2FA into that particular service type every 7 days using that browser on that computer. If you change computers or switch browsers you'll have to 2FA again for that session but you will have the remember me option for that combination as well.
- The three main methods of implementing your 2nd factor and the devices that support them are:
  - Phone Call
    - Landline.
    - Cell phone regardless of type/age assuming you have cellular service.
  - Application Push
    - Smartphone / Tablet with the DUO app installed, requires network service.
  - One Time Passcode (OTP)
    - Any cell phone that can receive SMS text messages.
    - Smartphone / Tablet with the DUO app installed, does not require network service.
    - YubiKey token which is a USB based dongle that generates a OTP when needed.
    - Duo D-100 hardware token generates a OTP, convenient but can become out-of-sync.
    - Pre-generated OTPs via a SMS text message. You get 10 at a time and they never expire. Each one can only be used once but you can request another 10 at any time. However, as soon as you do any of the previous 10 that were not used are automatically deactivated so you can't bank more than 10 at any time. I'm going to recommend that everyone who can should do this option and keep them written down in your wallet, purse, or whatever you are used to keeping with you and secure. That way you should always have an emergency 2nd factor if all your other 2nd factors are not an option for whatever reason.
    - Web interface, not available yet so no details on how this will work.
    - Call 4Help and once you prove you are who you say you are they can issue a OTP for you.
- There is no limit to the number of devices you can have enrolled in your 2FA profile and its recommended that you do enroll multiple devices so you have options. I have my smartphone, my office landline, my home landline, a YubiKey token, and a Duo D-100 token all associated with my 2FA profile along with my 10 pre-generated OTPs in my wallet. I have my office landline set as my default but I can select any of my other devices from a pull down list based on my situation at the time.
- For more information please visit: http://www.it.vt.edu/2factor/