(U) VFC Highlight #20-37: Securing And Maintaining Online Accounts to Disrupt Scams

Date May 4, 2020; Tracked by: HSEC 1.8

(U) Key Points

- (U) Organizations utilize online accounts for day to day operations, such as email, calendars, accessing sensitive information, meetings, and training. Proper security of these accounts is essential.
- (U) Recently the Virginia Fusion Center (VFC) has received a notable increase in reports of scam and other exploitive emails. Intelligence indicates that limited awareness of online account integrity is a contributing factor.
- (U) Using secure applications and practices can help increase account confidentiality and integrity with little cost to availability.

(U) What Resources Are Available To Me?

- (U) There are many free tools which can be used to verify the integrity of online accounts. Tools like Firefox Monitor can identify if an account has been involved in a data breach.
- (U) Bitwarden, Firefox Lockwise, or KeePassXC are examples of tools that can be used to securely keep track of account information and generate secure passwords.
- (U) Two Factor Authentication (2FA) can be used through the Google or Microsoft Authenticator apps on Android and IOS. Using 2FA (if supported) increases the security of online accounts by requiring verification before allowing a user to log in.
- (U) The Cybersecurity and Infrastructure Security Agency (CISA) provides additional information regarding password creation, password management, social engineering, and other security best practices. This information can be found at https://www.us-cert.gov/ncas/tips/ST04-002 .

(U) Firefox Monitor

(U) Best Practices for Consideration

- (U) Use password managers to store and generate secure passwords to online accounts
- (U) Ensure passwords are at least 10 characters with upper and lowercase characters, as well as numbers and special characters (!#$@%^…).
- (U) Sign up to receive email alerts from free programs like Firefox Monitor to become alerted when an email is released in a data breach.
- (U) Enable 2FA at every opportunity to increase the integrity of your online accounts.
- (U) Avoid signing into online accounts from public computer kiosks or public wifi.
- (U) Using sentences or passphrases can increase security while maintaining availability.
- (U) Avoid using simple words as passwords, and do not reuse passwords.
- (U) Use only work issued devices to access work accounts
- (U) Change default passwords for internet connected devices.
- (U) Supplement characters with numbers. This is commonly referred to as “Leet speak”, or L33T SP34K.
- (U) Always verify the authenticity of the website you are entering your credentials. Be aware of websites which redirect to credential login sites. Malicious actors frequently take advantage of typos and custom portals designed to fool users into providing sensitive or valuable account information.

(U) Please report sensitive security concerns with online accounts to the VFC at VFC@vfc.vsp.virginia.gov.