MS-ISAC

MS-ISAC Security Primer

Securing Personal Social Media Accounts

March 2017, SP2017-1423

Social media websites serve as platforms for global interaction and the sharing of ideas, but are simultaneously a platform frequently leveraged by cyber threat actors. Cyber threat actors target social media accounts in takeover attempts, with the goal of posting fictitious or embarrassing information. Cyber threat actors may also use personally identifiable information (PII) posted by you or friends to build a profile about you, including your identity, location, relationships, and affiliations. This information makes you more susceptible to doxing, identity theft, spear phishing emails, virtual blackmail, or potential physical threats. In addition, there are several scams which target the friends, family, and co-workers of a compromised account, and may result in financial loss or account compromise for additional victims. Appropriate usage of social media accounts and implementing proper security procedures is the best way to protect against these threats.

RECOMMENDATIONS:

- Do not post any PII such as your date of birth, telephone number, home address, or images that identify your job, hobbies, family, and friends. This information may often reveal the answers to security questions used to reset passwords, making you an easy target to victimize by giving malicious actors easy access to your accounts and secured information.
- Do not post anything you would be embarrassed to see on the evening news. Everything posted online becomes a permanent part of the Internet; assume it may become public.
- Do not accept friend/follower requests from anyone you do not know.
- Be cautious when accessing online accounts from public Wi-Fi connections. It is possible for malicious actors to capture login credentials and other sensitive information.
- Passwords should have at least 10 characters and include uppercase and lowercase letters, numerals, and symbols. Do not use the save password, “remember me,” or keep me logged in options. Do not share your password with anyone or write it down. Do not use the same password for all of your accounts. Make sure the passwords for your financial sites are not permutations of your other passwords. Change passwords every 60 days. More information regarding securing passwords is available on the MS-ISAC website.
- Use multi-factor authentication if available.
- Do not use your social networking website to login to other sites. If that website becomes compromised, then all accounts associated with that website are vulnerable. Create a different user account on the new website instead.

SETTINGS AND TECHNICAL RECOMMENDATIONS

- Configure social networking accounts to ensure only trusted contacts can see your information.
- Do not use automatic “check-in” features that disclose your geographic location.
- Avoid using third-party applications; if needed, do not allow them to access your social networking accounts, friends list, or address books.
- Do not allow others to tag you in images they post. Doing so makes it easier for malicious actors to collect information on your network of friends, relatives, and associates.
- Keep all operating systems, applications, antivirus solutions, and essential software up-to-date to mitigate potential exploitation by malicious actors.

The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation’s state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance for SLTT governments, is available at 866-787-4722, SOC@cisecurity.org, or https://msisac.cisecurity.org/. The MS-ISAC is interested in your comments - an anonymous feedback survey is available at: https://www.surveymonkey.com/r/MSISACProductEvaluation.