

SECURITY EDUCATION NEWSLETTER

OPM Breach: Blackmail

Remember the US government already knows everything in your SF-86 and has already deemed you trustworthy. Due to the recent OPM breach, individuals affected must be cognizant of the potential for blackmail.

In the unlikely event individuals are blackmailed based on the contents of the SF-86, embarrassing or uncomfortable discussions with loved ones may have to happen and individuals need to accept that possibility. Each person must determine how damaging his or her stolen information could be to his or her life.

Make sure you report ANY blackmail attempts to your local Security office.

Things to remember that will help you avoid becoming a blackmail victim:



- Be cautious about the information you share on social networking sites, such as LinkedIn, Facebook, or Twitter. Consider everything online as public, so if you don't want to share the information then don't post it.
- Shred personal documents instead of throwing them in the trash.
- Never provide sensitive financial or personal information via e-mail. A legitimate service provider will not ask for this via e-mail.
- Be careful to not put yourself in compromising situations.

DO NOT agree to pay blackmailers under any circumstances.

Do not hesitate to call your local Security professionals if you have any questions.