How to Protect Yourself, Family, & Friends

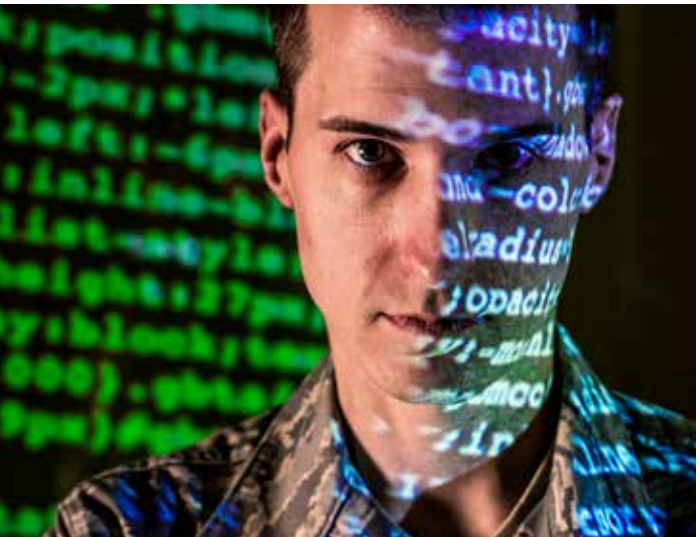
A few minor changes in the habits you may have for checking email, using social media, or the strength of the passwords you use could go a long way to ensure that you, your family, and friends are protected.

For your email, try to follow these easy steps:

1. Ensure you know who the sender is.
2. Never click on links in an email without verifying the link.
3. Never send personal information, passwords, or account information.

For social media and other online accounts:

1. Use Multi Factor Authentication (MFA) when available.
2. Ensure that your password contains letters (upper and lower case), numbers, symbols, and is at least 8 characters long.
3. Ensure that you never use the same password or variations of the same password for multiple logins.



Contact Information

Wanda T. Jones-Heath
Chief Information Security Officer
(CISO), USAF

Twitter: @SAF_DCIO
@Marion_CIO
@SAF_CISO

https://www.safcioa6.af.mil/ciso/
https://cs2.eis.af.mil/sites/13057/CISO

Air Force Cybersecurity
To assure the effectiveness of Air Force's core missions by increasing the cybersecurity and resiliency of
systems and information

DEFENDING THE FAMILY

Chief Information Security Officer (CISO), USAF

The Importance of Cybersecurity

With the increased use of digital technology, advancements in technology and improved tactics from cyber criminals you should do everything you can to ensure that you protect yourself, your family, and friends.

Cyber criminals will use various tactics to gather information on your identity, banking institutions, or social media accounts for their personal use or to be sold on the dark web. With access to your email or social media accounts they could target your family and friends by sending messages and emails from your account with links that could download viruses or malware or solicit other personal information from them.

Any of these has the potential to happen and if they do, it could cost you thousands of dollars, hours of your time, and issues with reclaiming your identity. Luckily there are some easy steps that can be followed to ensure that you, your family, and your friends do not become easy targets for cyber criminals.

Password Vaults & Managers

Password vaults or managers are a great way for you to ensure that you are using passwords that are strong, are different, very complex, and (in most cases) can be randomly generated. It is also very convenient if you have several logins across multiple sites, as it will normally auto fill the logins on the site your trying to access.

It may seem a little counter-intuitive to store all of your login information in one location and yes, there have been issues with using a password manager or vault. There have been flaws found that expose user credentials that were stored in the computer memory while the computers were locked. However, you should still use a password manager or vault because the vulnerability is only accessible with direct or remote access to your system.

If you decide to use a password manager of vault, it is recommended that you close the manager when you are not using it and use MFA if it is available.

Multi Factor Authentication

Phones, Email, and Tokens

This is one of the simplest tools that you can use and the easiest way to protect your accounts as well. MFA adds an additional level of security to your logins and is available on almost every social media, banking, and email sites.

MFA works by using your smart phone, authentication token, biometrics, security questions, or email and linking it to that specific site or login. Any time you log into that site it will ask you security questions or to input a one time password or pin number that you can have sent to you through a text message, phone call, or email. Some sites or applications even allow you to use your biometrics (fingerprint or facial recognition) as a second authentication method.

This very simple and very easy to use tool could be the one thing that keeps cyber criminals from having access to your or your families accounts.