

Tips for Choosing and Protecting Passwords

Passwords are the most common type of authentication and are often the only barrier to unauthorized access to personal and work information.

Weak passwords provide an opening for attackers to guess or "crack" passwords widely available hacker software; weak passwords are an open door.

Choosing good passwords and keeping them confidential, is the first defense to prevent an unauthorized person from gaining access your personal information or enterprise sensitive or proprietary information.

Why do I need a password?

Keeping track of multiple passwords and PINs to access different websites or other password protected services can be frustrating and seem like too much of a bother.

Email accounts and commercial web-site accounts may not seem to pose much of a threat, however, unauthorized access to email and websites and databases can make you personally vulnerable to security risks such as identity theft and fraud. **For Federal agencies, unauthorized access to critical data and systems has the potential to be catastrophic to national safety and security.**



Authentication is the process of verifying that someone is the person they claim to be. Passwords are usually the Front Line protection from unauthorized access to information and systems. **Weak passwords or passwords that are not kept confidential, are almost as ineffective as not having a password at all, because they provide an easy opening to casual or even inadvertent unauthorized access.**

How do I choose a good password?

- Do not use passwords based on personal information that can be easily accessed or guessed. (e.g. "mother's maiden name");
- Do not use words that can be found in any dictionary. (e.g. "computer2");
- Develop a mnemonic for remembering complex passwords. (e.g. "Je%Yn8S" can be remembered as "John eats 96 Yams in eight Summers");
- Use both lowercase and capital letters;
- Use a combination of letters, numbers, and special characters that is at least 8 characters long;
- Use "passphrases" when you can. (e.g. "1_RmD\$puRPI*PepL8r": "One Armed Purple People Eater");
- Use different passwords on different systems; and
- Do not "recycle" passwords; come up with new passwords instead.

How can I protect my password?

- Do not leave it laying around, especially near your computer or in your desk;
- Do not store the password and system name together;
- Do not provide passwords to anyone that asks for it (even Help Desks); and
- Do not "save" user names and passwords on internet sites.

What other forms of authentication are there?

- High tech complex authentication (including biometrics, such as fingerprints and iris scan screenings), are becoming more common;
- Lower tech complex authentication includes the use of "challenge questions" that utilize answers to personal questions; and
- DOECOE users utilize "two factor" authentication for off-site or mobile access and potentially to access systems and data that warrant extra protection. DOECOE "two factor" involves the use of a password and a unique and frequently changing "key code" that is obtained through a user-specific device.

General Reference: CERT OnGuard; May 21, 2009 National Cyber Alert System Cyber Security Tip ST04-002

How Much Do You Know?

How often should you change your password?

- 1) Every 30 days;
- 2) Every 3 months;
- 3) Once a year; or
- 4) After someone has guessed it.

Answer: 1) Every 30 days or more frequently if desired or necessary; and
4) Whenever you think someone may know your password.

What password below is safest? Which is the most common?

- 1) Oscar#1;
- 2) I_love_oScaR!;
- 3) rAc\$1E&vol;
- 4) Outlook#1pswd;
- 5) Password; or
- 6) Bosco.

Answer: 3) Is the safest password. (It is a code variation for #2 above);

- 5) Is the most common (in 2009).



True or False?

If you call the Help Desk for assistance, they will ask for your password.

Answer: False; the Help Desk will never ask for your password. Also never give your password to anyone over the phone, through email, or in person.

True or False?

Questions that ask for commonly known information about you, such as the color of your car, your birth date, and your mother's name are secure "Challenge Questions".

Answer: False. Challenge questions should solicit specific personal information that is known only by you and is not a matter of public record.

What does Two Factor Authentication mean?

- 1) Two people must know a password for authorized access;
- 2) Biometric measures are necessary for authorized access; or
- 3) Two authentications are necessary for authorized access.

Answer: 3) Two authentications are necessary for authorized access. For DOECOE, a password and a coded key (PKI: public key infrastructure) are used for two factor authentication.

True or False?

There are software tools that can make password management easier for the user.

Answer: True. Random password generators can ease the burden of "coming up" with new passwords. Encrypted password safes protect passwords while providing accessibility to the user.