



## Monthly Security Tips

# NEWSLETTER

Department of Accounting and General Services  
Information & Communication Services Division

April 2012

Volume 7, Issue 4

### Creating a Secure Password

Your password is more than just a key to your computer or online account. It is a gateway to all of your important information. If your password falls into the wrong hands, a cyber criminal can impersonate you online, access your bank or credit card accounts, sign your name to online service agreements or contracts, engage in financial transactions, or change your account information.

Unfortunately, many users are still not taking the necessary steps to protect their accounts by using strong passwords. Far too often, passwords with simple combinations such as 123456, password, qwerty, or abc123 are being used. In other cases, people simply use their pet's name or their birth date -- information that can be easily found online, such as on a Facebook or genealogy page.

#### How to Create Secure Passwords:

Cyber criminals have developed programs that automate the ability to guess your passwords. To protect yourself, passwords must be difficult for others to guess but at the same time easy for you to remember. Here are some recommendations:

- Passwords should have at least eight characters and include upper case (capital letters) and lowercase letters, numbers and symbols.
- Avoid words and proper names, regardless of language. Hackers use programs that try every word in a dictionary.
- Don't use personal information -- name, children's name, birthdates, etc. that someone might already know or easily obtain.
- Change passwords regularly -- at least every 60 days. If you believe your system, or an online account you access, has been compromised change your passwords immediately.
- Use different passwords for each account you have.
- Make sure your work passwords are different from your personal passwords.

#### Protecting Your Passwords:

- DO NOT write down your passwords. If you need to remember your passwords, write down a hint to a password, but never the password itself. Store the hint in a safe place away from your computer.
- Do not share your password with anyone -- attackers may try to trick you via phone calls or email messages into sharing your password.
- Do not reveal your password on surveys, questionnaires or security forms.
- Decline the "Remember Password" feature in browsers.
- Always remember to logout when using a public computer.
- If you need a utility to store your passwords, an "electronic vault" may be a viable option. When

deciding which password manager/electronic vault to use, look for programs that use powerful encryption algorithms, keylogger and phishing protection, and lock-out features. (Note: The MS-ISAC does not endorse any particular password vault or software for storing passwords.)

- At work, follow your organization's password policy.

**Resources for more information:**

**MS-ISAC Newsletter – Challenge or Secret Questions:**

<http://msisac.cisecurity.org/newsletters/2009-01.cfm>

**US-CERT – Choosing and Protecting Passwords:**

<http://www.us-cert.gov/cas/tips/ST04-002.html>

**US-CERT – Supplementing Passwords:**

<http://www.us-cert.gov/cas/tips/ST05-012.html>

**Microsoft: Create strong passwords:**

<http://www.microsoft.com/security/online-privacy/passwords-create.aspx>

For more monthly Cyber Security Newsletter tips, visit: [www.msisac.org/awareness/news/](http://www.msisac.org/awareness/news/)

**Brought to you by:**

 <p>STATE OF HAWAII <b>CYBER SECURITY</b> INFORMATION &amp; COMMUNICATIONS SERVICE DIVISION</p> <p>Information &amp; Communication Services Division (ICSD) <b>Cyber Security Team</b> <a href="http://www.cybersecurity.hawaii.gov">www.cybersecurity.hawaii.gov</a></p> <p>The mission of the ICSD <b>Cyber Security Team</b> is to preserve the confidentiality, integrity, and availability of the State of Hawaii's electronic information resources.</p>	 <p>Multi-State Information Sharing &amp; Analysis Center <a href="http://www.msisac.org">www.msisac.org</a></p> <p>The mission of <b>MS-ISAC</b> is to provide a common mechanism for raising cyber security readiness and response in each state and with local government.</p>
---	---

*The information provided in the Monthly Security Tips Newsletters is intended to increase your security awareness and to help improve the organization's overall cyber security posture.*