STOP | THINK | CONNECT™

Password Security – Think about it and take action!

From email and banking to social media and mobile apps, the average user has a long list of passwords - and the list keeps getting longer as our lives become increasingly interconnected in cyberspace. Password security continues to be one of the most critical safeguards you can take to protect your personal information and career-related proprietary information. Although keeping track of numerous account logins can be tedious, take a moment to think about the negative consequences if a cybercriminal gains access to your personal information. If you do not create strong passwords or keep them confidential, they are almost as ineffective as not having any passwords at all.

Remember that passwords are the keys to your personal digital 'kingdom' at home and at work. By following simple password security tips and practices, we can greatly enhance our ability to protect information.

- Do not use words that can be found in any dictionary of any language; use a combination of upper and lowercase letters, numbers, and symbols.
- Do not use passwords that are based on personal information or that can be easily accessed or guessed such as birthday, names of pets, or favorite movies and books that can be found by a quick search on social networking sites.
- Use passphrases ("Thispasswdis4myemail!") when you can and develop a mnemonic device for remembering complex passwords. If necessary, write down your password and store it in a secure place away from your computer or device.
- Use different passwords for different accounts and be sure to change them regularly.
- Do not visit dubious websites that might infect your computer to avoid malware that logs password keystrokes.
- If your mobile device has the capability, change the PIN number to an actual password.

The Internet is a shared resource and securing it is Our Shared Responsibility

U.S. DEPARTMENT OF ENERGY | Office of the Chief Information Officer

What in the world is Supply Chain Risk Management?

Supply chain risk management (SCRM) is another way to protect the quality and integrity of information technology (IT) products and their components, by making sure that the parts are genuine and operate as expected. It is an important consideration in building and maintaining DOE's mission critical systems and networks, and also for anyone who buys and uses IT, such as cell phones, laptops, and tablets, at home.

All IT products rely on globally sourced components. While these components provide innumerable economic and innovative benefits, the global production, distribution, and maintenance expose IT products to significant risk of exploitation through counterfeits, planned product failure, or embedded malware. Unscrupulous actors can take advantage of the global nature of the supply chain to purposefully manipulate IT components.

The number-one warning for technology users is to buy only from vendors they can trust – that means, know where things come from. For example, a "bells and whistles" cell phone at an unbelievable price from an unknown seller on an Internet auction site should be viewed skeptically. A known brand from a reputable vendor – either online or in-store – is ultimately a better deal because of the assurance of quality and customer service if something goes wrong.

Aside from the money lost in poor performance or failure, products that have no traceable ancestry can jeopardize the safety and privacy of the technology and its information.

Does DOE have supply chain issues?

DOE buys and maintains numerous IT systems and is concerned that supply chain risks could jeopardize not only the technology but also the Department's critical information. An enterprise SCRM (eSCRM) effort has been put in place to provide resources to help IT owners and users address and mitigate evolving SCRM risks. The eSCRM program includes training and awareness, threat assessment, and a resource portal to assist in making risk-based decisions about the integrity of critical information assets.

So, what can you do to help protect the Department from cybersecurity and supply chain risk?

1. **Use only DOE-provided IT components at work.** DOE assesses system components and has a good idea of how each will perform. Using a personal thumb drive or other memory device, particularly a "gift" one from a vendor or conference, may inadvertently introduce targeted malware. These devices are also prone to failure.
2. **Help your Program Manager prioritize IT components based on mission need and impact.** Identify those IT components that support critical systems and prioritize them.
3. **Know the Supply Chain.** Be aware of where you do business and who their suppliers are.
4. **Be willing to pay for the assurance of quality.** "Lowest-price, technically acceptable" doesn't support a safe and secure IT infrastructure.

SCRM is another significant part of the evolution of cybersecurity. If you have any questions, please contact us at enterprisescrm@hq.doe.gov.