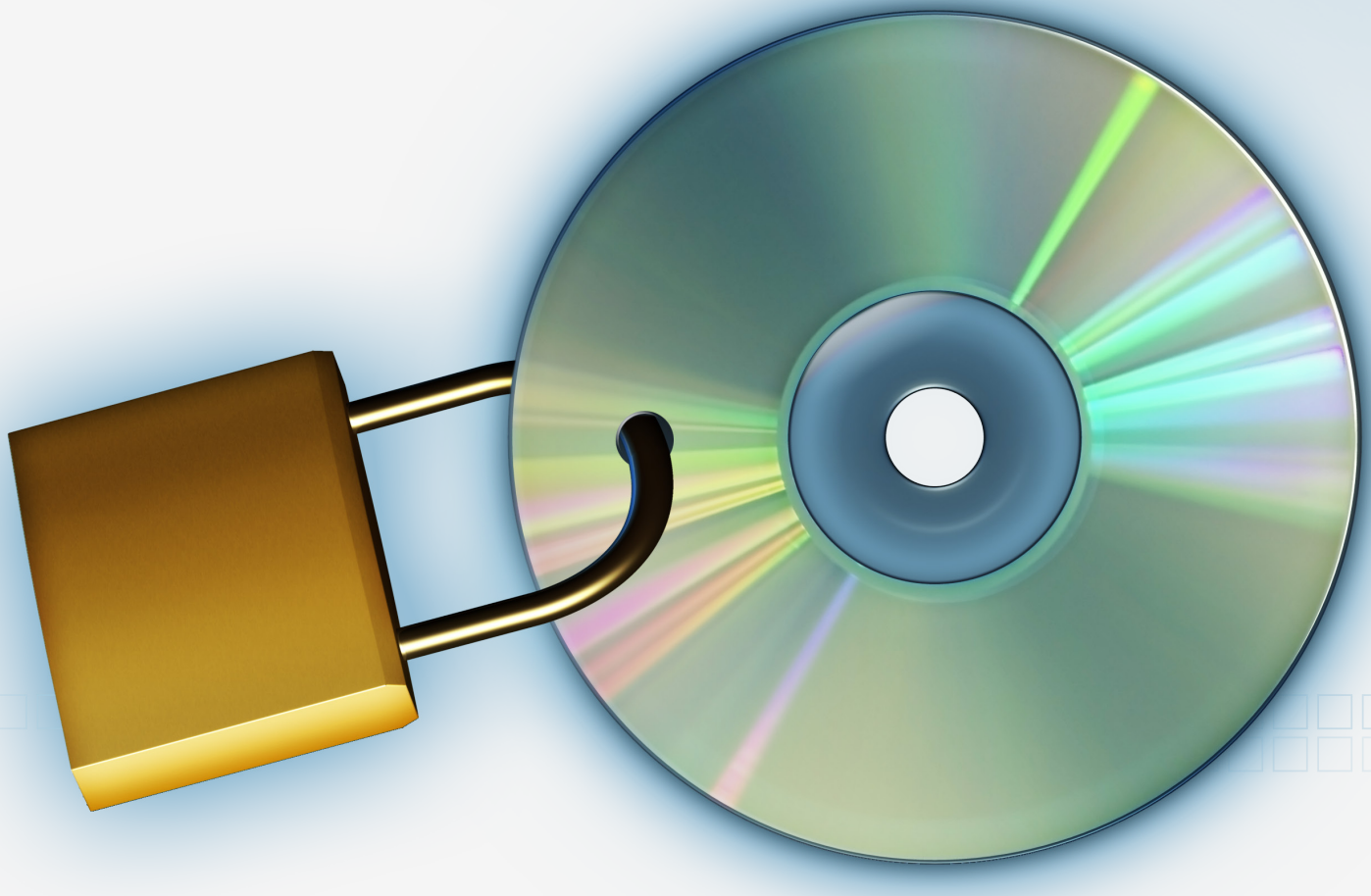
Data Security

Our information is our greatest asset. It is also the primary target for many cyber attackers. Technology alone cannot protect our highly valuable data; we need your help. It is critical you follow the steps provided to help protect our sensitive information.



This newsletter is published by Villanova University's security team.
For more information, please contact us at:

support@villanova.edu

UNIT INNOVATIVE TECHNOLOGY SOLUTIONS & SERVICES

© SANS Institute 2015

Data Security

A great deal of our security focuses on keeping your devices secure. While this is important, understand that most attackers are not after your devices; they are after the sensitive information that resides on them. Examples of sensitive information can include organizational secrets, financial statements, medical records, credit card numbers and personally identifiable information. As such, you should take the following steps when handling sensitive information:

- Always understand the sensitivity of the information you are working with. If you are uncertain about the sensitivity of any information or the steps you should take to secure it, ask your supervisor.
- Only use systems authorized by our organization to store, process or transmit sensitive information. Do not copy or store sensitive information to any unauthorized systems or accounts, such as personal laptops or personal email accounts.
- If you are authorized to have privileged access to a system, always log in with your unique, non-privileged user ID and elevate your privileges only when needed. Never log in directly as a privileged user.
- If you transfer sensitive information, use secure, authorized methods that support strong encryption. Do not transfer sensitive data using insecure means, such as email, unless you are using specialized encryption software that you have been properly trained to use.
- You must have prior approval to store sensitive information on removable media or portable storage systems, such as CDs, DVDs, USB flash drives and external hard drives. If you have prior authorization, then all sensitive data should be encrypted using approved encryption software.
- Never store or share sensitive information on public Internet or cloud services, such as Dropbox, Apple iCloud or Google Drive, unless you have prior authorization from management.
- Be careful when responding to any emails or phone calls in which someone is asking you to send them sensitive information. Always authenticate the person first using approved procedures, and then ensure they are authorized to access such information before sharing anything.
- Never leave any sensitive documents at your desk while it is unattended. Instead, secure sensitive documents when you leave them, such as locking them in a secure cabinet. In addition, make sure your computer screen is password protected whenever you leave it. This helps to ensure that unauthorized personnel cannot access your computer while you are away.

© SANS Institute 2015

Data Security

- Use only authorized software for work-related activities. Never install or use unlicensed or unauthorized software.
- Any third-party vendor provided with sensitive information, or given access to it, must be required to safeguard the data. This may require a contract and evaluation of their security controls to ensure adequate protection of the data.
- Any sensitive information that is no longer necessary or appropriate to store should be properly destroyed, shredded or rendered unreadable in a way that is consistent with our record retention practices.
- Be sure to contact the help desk or security team immediately if you believe any sensitive data has been lost, stolen or compromised. The sooner our organization is notified, the quicker we can respond to minimize damage.

These steps should be applied in a way that is consistent with our policies. Your understanding and following of our data security policies is key to securing our sensitive information and our organization.

Advanced Threats Targeting Our Data

There are many different threats targeting our data. One of the most common is cyber criminals. These are individuals or organizations who know they can steal our sensitive data and use it to commit fraud or simply sell it to others. Unfortunately, there are several other threats targeting us that are far more advanced than common cyber criminals.

One is our competitors. Some of our competitors may be unethical in the ways they operate. They may attempt to compromise our organization and steal our data to gain a competitive advantage. Another threat is countries that target our data for economic, political or military gain. These countries often have highly skilled hackers whose full-time job is to hack into our organization. You may not think our data has value to others, but it does.

This newsletter is published by Villanova University's security team.
For more information, please contact us at:

support@villanova.edu

UNIT INNOVATIVE TECHNOLOGY SOLUTIONS & SERVICES

© SANS Institute 2015