

CYBER SECURITY

Newsletter

ENCRYPTION – PROTECTING SENSITIVE INFORMATION

Problem

It is simply amazing how much information you carry today. One of the most common ways to measure information is the Gigabyte. A single Gigabyte can store over 500 books, 20,000 web pages or up to 100,000 text emails. The average USB flash drive can store over 16 Gigabytes, smartphones can store over 64 Gigabytes while a new laptop can store hundreds of Gigabytes.

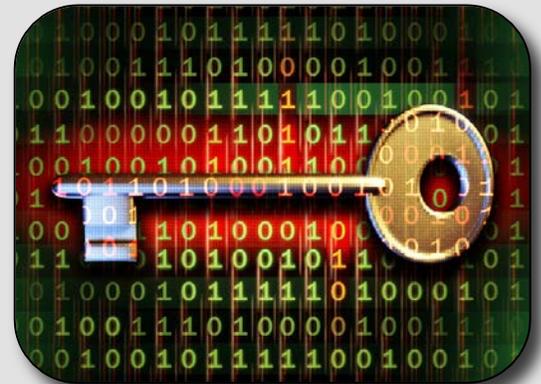
Each of these devices is simple to carry with you and this allows you to leave the office with a huge amount of confidential information, information such as our customer database, sensitive emails or thousands of work documents. Unfortunately, it is also simple to lose one of these devices.

Once one of these devices is lost, all of your confidential information can be easily recovered. Once recovered, this information can be used to steal your identify or steal our organizations data.

Solution

So, what is the solution? One method would be to simply never leave the office with any sensitive information. This may be the case for your position. However if your supervisor has given you permission to travel with sensitive information, you need a way to protect the data. That method is encryption.

Encryption is the process of taking normal information (called unencrypted data or cleartext) and changing it into something unreadable (called encrypted data or cipher text). When information is encrypted no one can read or understand it. This way if you lose your laptop or USB flash drive outside the office, no one will be able to access or read the information, it will be protected. The best way to protect your information while maintaining access to it is to encrypt the information before leaving the office or home.



Encrypting Sensitive Data

Your laptop, mobile devices and USB flash drives store a tremendous amount of sensitive data. However, if you lose any of these devices anyone can read your information, including your emails, documents and photos. By encrypting your data you prevent unauthorized people from accessing it.

JUNIATA
COLLEGE 

This newsletter is published by
Campus Technology Services. For
more information please contact
us at:

help@juniata.edu

What And When To Encrypt

Traditionally encryption was difficult to setup. You had to identify which information you wanted to encrypt on your computer and configure complex programs to encrypt the information. You then had to manually decrypt the data every time you needed it. This approach is inconvenient and takes up a lot of time. Today solutions are much simpler.

In general, the best approach is to simply encrypt everything on your system, often called Full Disk Encryption (FDE). This means you do not have to worry about which data to encrypt, when to encrypt it, or how to encrypt because absolutely everything on your device is encrypted. This way you login or access your device and everything is decrypted automatically.

For supported encryption programs that automatically encrypt your information, please contact the help desk or information security team.

HOW ENCRYPTION WORKS

Step 1

First we begin with un-encrypted, or cleartext, information. This is information anyone can read and this is how information normally looks when stored on a device. While simple to use this is unfortunately not safe. If you lose any of your devices with unencrypted data someone can easily recover the information and then steal your identify, sell the information, or use it to harm you or our organization.

Step 2

Encryption is the process of converting cleartext data into an unreadable format. To encrypt your data you first need a key. Usually this is a password, but other things can be used such as tokens or even parts of your body such as your fingerprint or face.

Step 3

Your key, combined with an encryption program, turns your information into unreadable garbage. No one can read or understand it. The only way the information can be recovered is with your encryption key. Now if you lose a device the information is not exposed. No one but you can recover and read the information. This protects you and our organization.

Alice was beginning to get very tired of sitting by her sister on the bank, and having nothing to do: once or twice she had peeped into the book her sister was reading, but it had no pictures or conversations in it, 'and what is the use of a book,' thought Alice 'without pictures or conversation?'



hQIOA8LMpVyVlexFEAf+JwNE3vQTmG
A/RbtX80dCIMnNQXCbCcQUUHdy4GN
Yaba4n5KUsVuht30unFdyr5AIGw4UBj
Erv5Z4/YYNmLxrZj1gpjPXkNrspV+rIrF
G+E7+YnK/tjVKEKu2yJQo0kPgA5d+6o
AdDPMrb+ct/S5NSIJ6ttW2bYPZch9fjSs
pZH5ipF5PflmuoHSIEuBzHkVFXtYCReL
E3QFKBhxTnFgtro63/zGLY+klhys4pxn
