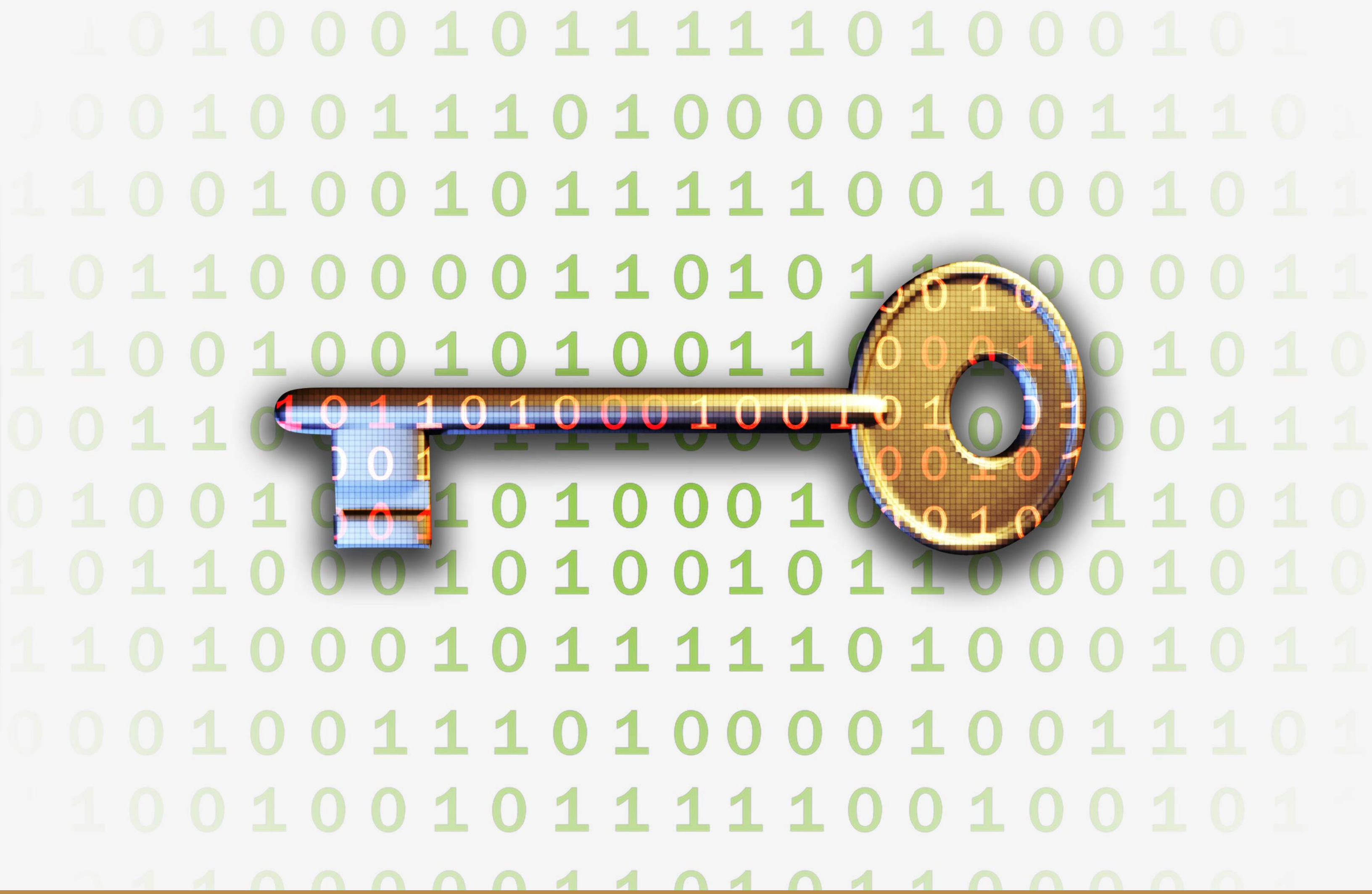
Encryption

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.



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

Encryption

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 7,000 Word documents or 2,000 images. To put this into perspective, a USB flash drive or smartphone can store over 128 Gigabytes of data. A new laptop can store thousands of Gigabytes (called a Terabyte) of data. Each of these devices is simple to carry with you, enabling you to leave the office with a huge amount of highly sensitive information -- information such as confidential emails or thousands of work documents. Unfortunately, it is also easy to lose one of these devices. Once one of these devices is lost, all of your and our organization's sensitive information can potentially be compromised.

Solution

What is the solution? One method would be to simply never travel 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 that data. That method is encryption.

Encryption is the process of taking normal information (called unencrypted data or plaintext) and changing it into something unreadable (called encrypted data or cipher text). Encryption uses mathematical formulas, called algorithms, and a unique key to convert your information into cipher text. The key is what locks or unlocks your information, just as a key can lock or unlock a door. A common example of a key is a password, and only people who have that key can decrypt and unlock your information. You need to protect your key to protect your encrypted information.   For example, if your laptop is encrypted and you lose it while travelling, the data on your laptop is safe as long as no one knows your password. The only way a person could access your data on your laptop is if they knew what your password for decrypting the data was.

Traditionally, encryption was difficult to setup. You had to identify the information you wanted to encrypt on your computer and configure complex programs to encrypt it. You then had to manually decrypt the data every time you needed it. This approach was inconvenient and took a lot of time. Today's solutions are much simpler. In general, the best approach is to simply encrypt everything on your system, which is often called

Encryption

Full Disk Encryption (FDE). This means you do not have to worry about what data to encrypt or how because absolutely everything on your device is automatically encrypted. When you log into your laptop or your device with your password, everything is decrypted automatically.

In addition, encryption can not only help protect the information on your devices, but also help protect your information when it is transferred over the network. For example, when you use your browser to connect online to your bank, that connection should be encrypted to protect all of your sensitive financial information. You may also be provided something called Virtual Private Network (VPN) software by our organization. This is an additional layer of encryption that protects all of your online activity.

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

Encrypting Personal Devices

Encryption is not just for work. We highly recommend you consider using it for your personal life as well. You are walking around with a tremendous amount of highly personal information, from the family photos on your smartphone to the personal emails on your laptop. Just like work, if any of these devices are lost or stolen, people may access your information. Fortunately, most devices support encryption nowadays.

For Windows users, depending on the version of Windows you have, your computer may come with a free encryption technology you can use called Bitlocker. For Mac OS X users, you can encrypt your laptops using the free technology called FileVault. Many mobile devices also support encryption. However, the encryption is usually only enabled if you put a PIN or password lock on it. As such, always be sure to password protect your mobile devices.

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