CYBER SECURITY Newsletter

PROTECTING PII

Problem

Our organization handles a great deal of confidential information, including data known as Personally Identifiable Information, commonly called PII or Personal Data. PII is targeted by attackers because it is highly valuable information that can be used for identity theft, fraud, or used to attack other organizations. PII is any information that can identify a specific individual, such as Social Security numbers utilized in the United States, international passport numbers utilized in Europe, driver's license numbers, or any other personally identifiable information.

Solution

Because this information is so valuable, and because we are committed to protecting the rights and privacy of others, all employees need to take the following steps to protect PII or any other highly confidential information. Following these steps will help ensure our organization and information is secure:

1. Authorized Systems

Our organization takes extra measures to protect PII and other confidential information. One step is to ensure data is only stored on authorized systems. These systems have strong security measures in place, such as strict controls on how they are configured and who has access to them. To protect important data, you should only use authorized systems to enter, process, or store PII or other confidential information. Do not enter, process, or store PII on unauthorized systems, such as personal devices.

2. Sharing Data

Another step to protecting PII is ensuring only authorized people have access to it. These individuals must have prior management approval to access such data. They must also need access to the data to accomplish their job duties. Simple curiosity is not a sufficient need for access.

Protecting PII

Ultimately, it is our data, including PII, which cyber criminals are after. The key to protecting both yourself and our organization is to protect the confidential information you work with on a daily basis.

Idaho State UNIVERSITY

This newsletter is published by Idaho State University, for more information please contact us at:

help@isu.edu

Personally Identifiable Information

The concept of Personally Identifiable Information (called Personal Data in Europe) is not new. For thousands of years, civilizations have had ways to identify individuals by their full name, birthplace, and date of birth. However, a variety of factors have made this type of information more valuable and easier to steal.

First, there is far more personal information collected than ever before. Every action you take is tracked, such as the clothes you purchase, the phone calls you make, or the music you listen to. This information is much easier to associate with specific people, as we now have many different identification numbering systems.

By taking all this information and remembering there are numerous copies of it stored around the world in digital format, you begin to understand how easy it is for cyber criminals to steal this information. Once stolen, it can then be use for numerous crimes, including fraud and identity theft. It is because of risks like this that we must take extra steps to protect all PII.

3. Mobile Media

Be careful when connecting USB flash drives, memory cards, or CD-ROMs to your computer. Quite commonly, worms and viruses spread via these mobile devices. For example, by plugging a USB flash drive into an infected computer at home, then using the USB flash drive at work, you can accidently infect our entire organization. This is why you never use mobile media found in parking lots or received from strangers, and why you should only use authorized mobile devices our organization has approved. In addition, whenever you connect mobile media to your computer, scan all contents with current anti-virus software before opening any files.

4. Transferring Data

At times, you may need to transfer PII or other confidential information to authorized individuals. There are tremendous risks to transferring data, such losing it, having it get stolen or even intercepted. For example, if you copy confidential data to a USB flash drive and lose it, what are the consequences? If you store the information on your laptop, what happens if your laptop is stolen? If you email the information, someone can easily intercept and read it.

As such, if you transfer PII or any other confidential data, you should only use secure, authorized methods that support encryption. Never transfer sensitive data using insecure means, such as email.

5. Data Destruction

A common way PII is compromised is by employees improperly disposing the information. For example, throwing out an old USB flash drive or donating computers that are no longer used could allow sensitive information to be retrieved by unauthorized people, as these devices often still contain the sensitive PII data.

To protect against this danger, all physical and electronic PII -- and other confidential information that is no longer necessary or appropriate to store -- should be properly destroyed, shredded, or rendered unreadable. For digital media such as hard drives or USB flash drives, this means they should either be physical destroyed or the media should be entirely wiped, ensuring the information is truly gone and cannot be recovered.