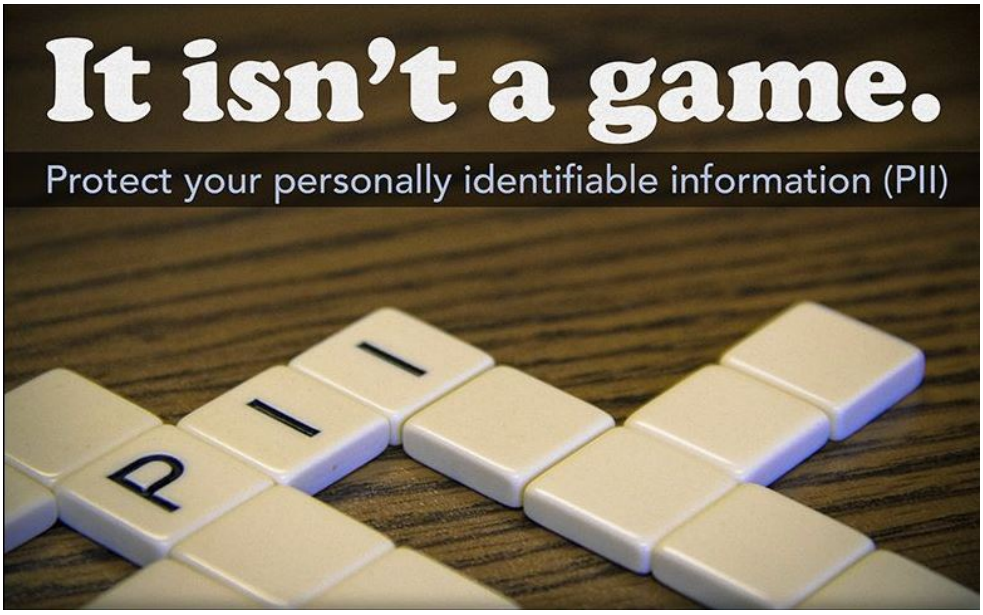

What is PII?

PII, or personally identifiable information, is sensitive data that could be used to identify, contact, or locate an individual.

What are some examples of non-PII?

Info such as business phone numbers and race, religion, gender, workplace, and job titles are typically not considered PII. But they should still be treated as sensitive, linkable info because they could identify an individual when combined with other data.

Why is PII so important?

On a personal level, our PII is necessary to acquire some goods and services, such as medical care and utilities. But in the wrong hands, PII leads to identity theft and other forms of fraud. If left unprotected, we could face damages to our reputations or have our identities stolen.

Best practices to deter PII violations

Be familiar with current information on security, privacy and confidentiality practices:

- Where applicable, obtain written authorization before using sensitive or critical applications.
- Lock or logoff device/application before leaving it unattended.
- Act in an ethical, informed and trustworthy manner.
- Protect sensitive records.
- Be alert to threats and vulnerabilities to systems.
- Do not click on random links and attachments.
- Destroy sensitive documents beyond recognition.
- Set social media profiles to fully private.

How to identify PII loss in the work area

- Leave a document with personal information on an unattended desk.
- Leave an electronic device open that is displaying PII without locking the device.
- Leave a document with PII unattended at a printer or fax machine.
- PII of your customers is found on unauthorized websites.
- PII is sent via e-mail to unauthorized recipients.
- Loss of electronic devices or media storing PII.

Cyber Security is our shared responsibility!

– Cyber Security Center, IT Department