Security Awareness

SIENA ITS STAFF WILL NEVER ASK FOR YOUR PASSWORD OR OTHER CONFIDENTIAL INFORMATION VIA EMAIL

Siena College has implemented many security mechanisms to protect data. One of the most important mechanisms is security awareness training across the Siena College community as social engineering has become the dominant way hackers attempt to gain unauthorized access to private data.

SECURITY AWARENESS TRAINING

	SO, WHAT CAN YOU DO?
STOP:	• Stop hackers from accessing your accounts – set secure passwords. • Stop sharing your password with others. • Stop sharing too much information – keep your personal information personal. • Stop – trust your gut.If something does not feel right, stop what you are doing. Contact ITS for assistance. • Stop clicking on links in emails from people and businesses you do not know, even from what may appear to be trusted sources (e.g. your bank). Often these are lures to phishing (hoax) web sites designed to trick you into revealing your password. • Stop – before you enter your password into a web browser check to see you are on the correct website. • Stop unauthorized access to your computer – lock your keyboard or log off before leaving your computer unattended. • Stop unauthorized access to your laptop or mobile device – set passwords, encrypt data, password protect your files, use a cable lock. • Stop leaving documents containing PII in work areas where unauthorized individuals can see them.This can even include your co-workers. • Stop leaving PII unattended on your desk and remove PII immediately from printers, fax machines, copiers and scanners. • Stop – dispose of PII properly.Do not just throw it in the trash.Use a shredder or other method which destroys the information.
THINK:	• Think about the information you want to share before you share it. • Think before you act – do not automatically click on links. • Think about why you are sharing information online. Is it going to be safe?
CONNECT:	• Connect with people and businesses you know to be legitimate. • Connect with care and be on the lookout for potential threats.Contact ITS immediately if you observe or experience any behavior or conditions you feel are not normal. • Connect with people and sites your trust when you are online. Look for the “https” designation and a locked padlock at the bottom of the browser screen.

It is the responsibility of everyone within an organization to support information security efforts and to watch for abnormal events.

If assistance is required, please do not hesitate to contact ITS.

Do the right thing……..Keep Personally Identifiable Information Confidential!