Cyber Security Awareness
Newsletter
Protecting yourself and information
from cyber security threats

What is Social Engineering?
Social Engineering, in cyber security terms, are methods that are used to obtain personal or confidential information for the purpose of infiltrating an asset to do damage or use for personal gain. Being cybersmart doesn’t necessarily mean being conscious about your computer use. Attackers do find other ways besides technical means of compromising assets.

Social engineering has been and is a threat that has persisted throughout the ages. Obtaining credentials for access, creating a ransomware scenario, destroying a competitor’s data, and gaining trade secrets, defaming a website to discredit integrity and trust, etc. are just some of the threats where it is necessary to understand your role in cyber security. This month we wanted to make you aware of some of the social engineering threats we face at the institution and how you can protect yourself and your data from falling victim.

PHISHING, VISHING, SMISHING, AND PHARMING...Oh my!

What is phishing, vishing, smishing and pharming?

PHISHING
Phishing is a type of online scam where criminals impersonate legitimate organizations via emails and websites, in attempts to compromise a system and/or steal sensitive information. Threat actors usually infiltrate and steal information through links in e-mails or websites. Always be aware of the “from address” in e-mails, think about the legitimacy of the received e-mail messages and do not click on any links that may be embedded for any messages that were unexpected. Instead, if you believe the e-mail to be legitimate, consider visiting their site by typing in the main URL.
VISHING

Vishing, also known as “voice phishing” is another type of phishing scam. Instead of e-mail, the interaction is done over a phone call. Threat actors on these phone calls may attempt to impersonate legitimate organizations, threaten legal action, etc. all in an attempt to coerce their targets into giving up information. Never provide account passwords or other sensitive information to anyone claiming the need to have it.

SMISHING

Smishing attacks are another type of phishing attack that tricks an unsuspecting victim via SMS text messages on a phone. With the advent of phones becoming an everyday computer carrier of information and authorization, links in text messages can gather locally stored information and put you at risk. Text messages on your phone regarding a locked account, suspicious activity, a cancelled order, an expected delivery, etc. all requesting for you to click on a link can be malicious. Never engage by clicking on a link or replying STOP. If you believe there is some legitimacy to the text message sent by a vendor, we recommend going straight to the vendor website or calling them and addressing them yourself.
PHARMING
Pharming occurs when DNS and/or organizational website has been compromised and the site or links on the site redirect a target audience to a fake website. An example of this occurrence can be found here: https://www.bbc.com/news/technology-54568784

Always register your website with the BSD ISO office for security integrity and weekly scanning.

Phishing attacks and scams have thrived since the COVID pandemic began in 2020. Today, phishing attacks account for more than 80 percent of reported security incidents (Verizon Data Breach Investigations Report) and according to the FBI, phishing was the most common type of cybercrime in 2020, with the bureau receiving 241,342 complaints in 2020. (FBI)
Be wary of emails, text messages or chat boxes that come from strangers or someone you were not expecting. Think before clicking on suspicious emails, links or attachments and make sure to report any suspicious emails to security@bsd.uchicago.edu.

Follow us on Twitter: @UofCBSD_Infosec

****As a reminder: Make sure you enable Multi-Factor Authentication where possible.****