COVID-19 Security Threats and Challenges

As our University and country respond to the challenges of the COVID-19 (coronavirus) outbreak, cyber criminals are also actively attempting to take advantage. The University Computer Services Center and Information Security Offices want to warn you of the need to be especially vigilant.

Email threats

Malicious email phishing scams about the COVID-19 virus are at a heightened level, taking advantage of fears and increased business communication surrounding the Coronavirus. These phishing attempts may ask you to enter credentials, click a link, or urge you to open an attachment to learn more, potentially installing malicious code on your machine.

Please take the following precautions:

- Be skeptical of emails claiming to be from the Centers for Disease Control (CDC), the World Health Organization (WHO), or experts saying they have information about the virus. Find the authoritative web sites for those entities rather than clicking on links in the email.
- If you receive an unsolicited email which includes a link requiring you to enter passwords, STOP and assess the situation. Contact the sender before acting, or request the email be reviewed by campus’ CSC or USA Health’s IT department, see information below.
- Verify the sender’s email address, but be aware that even a legitimate sender might have been compromised.
- Unless you are CONFIDENT of the email’s integrity, do not click on any links, or download/open any attachments in any unsolicited emails you may receive - even if from someone you routinely correspond with.
- Remember, USA will never ask for sensitive information via an unsolicited email.

Social Engineering

Social engineering is a type of attack that leverages human kindness and may involve impersonating a USA affiliate or asking for information on behalf of one.

- These methods often create fake situations that appear to be urgent in order to retrieve sensitive information, elevated permissions, or a response that would normally require an approval or verification process to provide.
- These targeted attacks are commonly observed in phishing emails that request you to perform an action such as download an attached document or click on an embedded link, but can be conducted through other methods such as phone calls, social media, or in person.
Guidance:

- Remain vigilant.
- Do not bypass proper approval channels that would normally be required by your department.
- Common sense is your best defense
- Verify the source of all requests before engaging in a conversation
- If your department is responsible for providing services to the USA community and you have questions on your verification processes or policies, please consult your supervisor for additional information.

Further Information

The University Information Security Office has published a more detailed advisory on this topic. On the main University of South Alabama web site, use the A-Z index to find “COVID-19 Security Threats”

Where to Get Help and Report Incidents

General Division Faculty and Staff may email helpdesk@southalabama.edu or infosec@southalabama.edu Call (251) 460-6161 for highly urgent circumstances, such as an obvious computer infection or ransomware attack.

USA Health employees may email hsis.emailreview@health.southalabama.edu or call the Help Desk at (251) 445-9123