Safe Computing

1660 Laurie Sherrod May 10, 2023 Security

Security is a part of our everyday thinking in this day and age. Clemson University takes security seriously and wants our users to be vigilant and practice due diligence when it comes to security. It is important that our users understand what is expected of them in securing Clemson's resources as well as what concerns they should have to avoid falling victim to a security incident. This guide serves as a best practices guide to aid the user in following good security practices to help keep Clemson a safe and secure environment.

STAY CURRENT WITH CYBERSECURITY ALERTS

CCIT's Office of Information Security regularly updates its Cybersecurity Alerts page, detailing the latest cybersecurity threats and the best ways to keep your information safe online.

ADHERE TO CLEMSON COMPUTING POLICIES

By agreeing to be a part of Clemson, you are also agreeing to abide by the policies established at Clemson. These policies are not intended to restrict or limit your effectiveness as a Clemson user but rather to help guarantee a safe environment for all users. It is important that users are aware of these policies and guidelines so that they can put them into practice as well as being alert for abuse of those policies.

Please refer to CCIT's Clemson IT Policy & Standards site for more information.

PROTECT YOUR IDENTITY

It is vital that you safeguard your personal information as well as your Clemson account while working here at Clemson. Here are some helpful tips to assist you in protecting your identity at Clemson:

- Keep all electronic/physical items containing personal/account information secure at all times.
- Email is NOT a means of secure communication. Never email personal information such as SSN's or your password information.
- Never store personal information or SSN's on removable media such as USB keys, portable hard

drives, etc. Use strong passwords and take appropriate measures to safeguard them as outlined in the Accounts & Password Management Policy.
- Never give out your password to another user or an IT administrator.
- Be careful of emails that ask for you to go to a web page and enter login information. Instead, open a browser yourself, and type the web address manually rather than clicking on a link within the email.

SAFEGUARD YOUR COMPUTER

- Lock your computer before walking away from it
- Do not allow other users to work on your machine under your sign-on
- Be careful of downloading “free” programs because they could include spyware
- Do NOT install any file-sharing programs

BE ALERT

Clemson’s IT staff can only provide a layer of protection, but it is up to the users to be vigilant and alert of threats to Clemson users and resources. Here are some things to always be mindful of doing:

- NEVER give out your password to someone requesting it. Clemson IT staff will never ask for your password. Please report anyone attempting to do so.
- Be alarmed if someone posing as a support person wants to “work” on your machine. Only the CCIT Support Desk should work on your machine. Report any suspicious users or actions that you feel could be malicious behavior.
- Report any suspicious behavior on your machine to your support person such as wondering mouse activity, deceiving pop-ups, or spontaneous programs.
- Report any harassment witnessed whether physical or electronic.
- Report any attempts to circumvent our security protections for personal gain or malicious intent.

WHAT IS A "SECURITY INCIDENT"?

- Attempts to gain unauthorized access to a system or its data.
- The unauthorized use of a system to process or store data.
- Changes to system hardware, firmware, or software without the owner’s knowledge, instruction, or consent.
- Non-electronic Information Security Incident: real or suspected theft, loss, or other inappropriate access to physical content, such as printed documents and files.
- Theft or other loss of laptop, desktop, phone, tablet, or any other device that contains Highly Sensitive information, even if the device is not owned by Clemson University.

REPORTING A SECURITY INCIDENT

Anyone who becomes aware of an information security incident should immediately report it to CCIT at ithelp@clemson.edu.

For more information email ITHELP@clemson.edu or call 863-656-3494.