Georgia Tech

CYBER SECURITY BEST PRACTICES

Welcome to Georgia Tech!

The Georgia Tech Cyber Security Team is committed to protecting our community. We are here to help not only students, but also faculty and staff on campus.

Here are some general tips on how to keep yourself protected using the networks on campus, when you're out and about, and even at home.

Our Site:
security.gatech.edu

General Computer Tips

- Be sure to install and update anti-virus software.
- Update operating system and applications regularly by patching.
- Back up files on your computer either to an external drive or to the cloud.
- Only use flash drives that you know has a trusted source; e.g. buying one at Burdell's or B&N @ GT.
- Connect to GT VPN when you're on a public network or one you don't trust. Be wary of 3rd party VPN applications.
- Disable automatic connections to unknown wireless networks and turn off Bluetooth when not in use.
- Remove old saved wireless network connections.

Mobile Device Tips

- Assign at least a 6-digit pin or fingerprint authentication to unlock your phone.
- Enable services to locate lost or stolen devices.
- Limit the information that apps are allowed to access; e.g. location, address book.
- Disable automatic connections to unknown wireless networks and remove old wireless network connections.
- Turn off Bluetooth if you don't need to use it.

Safe Web Browsing

- When in doubt, don't visit a web page of which you are unsure if it is legitimate or safe.
- If you're asked to enter sensitive personal information or payment information, confirm you are on the correct webpage and it is not a spoofed website. Be especially vigilant if it was a link in an email or electronic message.
- Review browser security settings and consider using a popup blocker extension.

Password Tips

- Use a password manager application so that you will only have to remember one password and can have a unique complex long password for every website. Also, consider randomizing your passwords and using the password manager to enter your passwords on webpages.
- Never use the same password on multiple sites. A password manager will help you achieve this securely.
- Avoid passwords based on a dictionary word or something about you. A password manager will help you achieve this securely.
- Do not reveal something in a password hint that tells someone else your password; e.g. "Mom's name". A password manager will help you achieve this securely.
- Be sure to activate Multi-Factor Authentication on any site that has it available.
- Visit this page for some more information about creating secure passwords: https://security.gatech.edu/securing-your-password

Social Media

- As a rule of thumb, assume anything you post could be seen by the world.
- Do not post your whereabouts.
- Be sure to look at your profile without logging in to see what others would see.
- Adjust your privacy settings to align with what you're most comfortable with sharing.
- Consider how a post will affect yourself and others before posting.

Travel Safety

- When traveling, be sure to take extra precautions with your electronic devices and data; e.g. never leave your device unattended.
- Consider using GT VPN on networks you don't trust.
- Avoid storing sensitive information directly on your devices.
- Consider changing the passwords you used during your trip when you return.

USING GEORGIA TECH SYSTEMS

As a top-ranked public college and one of the leading research universities in the USA, Georgia Tech has many computing resources as well as services available to students on campus.

When using Georgia Tech systems and resources on campus, be sure to keep the following things in mind.

Acceptable Use Policy

Institute IT Resources must be used in accordance with applicable licenses and contracts, and according to their intended use in support of the Institute's mission.

All users must comply with federal, state, and local laws, as well as Georgia Tech policies, when using Georgia Tech IT Resources.

Georgia Tech students may use the ResNet, EastNet, and LAWN networks for recreational and personal purposes to the extent that such use is not unacceptable as defined in the Unacceptable Use section of the policy.

Unacceptable use can include but is not limited to:

- Activity that violates federal, state, or local law
- Activities that lead to the destruction or damage of equipment, software, or data belonging to others or the Institute
- Impeding or disrupting the legitimate computing activities of others

More information on Acceptable Use can be found here: https://policylibrary.gatech.edu/information-technology/acceptable-use-policy

QR Code to Acceptable Use Policy:

Email

Georgia Tech email is housed on Office 365. Your campus email account should be used to communicate between yourself and other Georgia Tech users on campus.

Avoid Emailing Sensitive Data

We recommend other ways to send sensitive information instead of direct email. For example, share links to where you're storing your data in the cloud instead of sending sensitive data in attachments.

Look Out For Phishing

Phishing is the fraudulent attempt to obtain sensitive information by acting as a legitimate sender. To keep yourself protected, follow these guidelines:

- Be sure to check the message details when you receive emails.
- Look for typos in a message from a sender that appears official.
- Avoid opening attachments if they seem suspicious.
- Mouse over hyperlinks to make sure the destination address matches the text.
- If anything asks you for a login and everything else seems okay, try going to the official site via a web browser instead and confirm what's being asked.

If you receive a message which you suspect may be a phishing attack, please forward the message as an attachment to: phishing@gatech.edu

QUESTIONS?

SITE: HTTPS://SECURITY.GATECH.EDU
EMAIL: ASK@SECURITY.GATECH.EDU
PHONE: 404.385.CYBR (2927)

Georgia Tech Cyber Security