Information Technology Security

A successful security program can only be achieved with everyone's participation.

Whether you are a staff, faculty, student, visitor, or alumni, you have the ability and the responsibility to manage the risk when you interact with American University's network and data.

If you have any questions, please contact the Help Desk at 202-885-2550, or helpdesk@american.edu, to request a security consultation.

OCTOBER
NATIONAL CYBER SECURITY AWARENESS MONTH

American University

Office of Information Technology
Information Security Team
4620 Wisconsin Ave., NW
Washington, DC 20016

Phone: 202-885-2550
E-mail: helpdesk@american.edu

4 P's of Security

- Phishing
- Policies
- Privacy
- Protecting Data

Is your sensitive data secure?

Inside are 4 tips to minimize the risk when you share, store, and transmit data

AMERICAN UNIVERSITY
WASHINGTON, DC

Protecting Sensitive Data

In the paper world, if a document is marked "CLASSIFIED" or "CONFIDENTIAL", we can easily protect it by placing it face-down on our desk when someone walks by that does not have a need to know, lock it in a file cabinet when it is not being used, or when needing to share use a courier or hand-deliver to the appropriate person, and finally when it is no longer needed we can shred it. We need to take these same precautions in the computer world.

OIT is here to help, if you ever have questions about the security of a system or an electronic document you are handling. In general, Information Security professionals suggest that protecting sensitive data requires a combination of people, processes, polices, and technologies.

Phishing

Phishing is a technique criminals use to gain their victim's trust by sending a convincing e-mail message or leaving an official-sounding phone message to pose as a legitimate organization—like American University, a bank, or government agency.

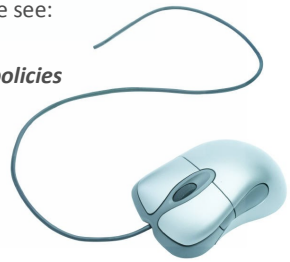
- OIT and other AU organizations will never ask for your password by e-mail or phone message.
- Treat all such requests with high suspicion.
- If you receive a message from someone purporting to be your bank, employer, or other trusted organization, double check the correct number on correspondence from the organization or their Web site.

Policies

Information technology security is the responsibility of all students, faculty, and staff. Every person handling information or using university information resources is expected to observe these security policies and procedures both during and, where appropriate, after his or her time at the university.

For a complete description of information technology security policies, please see:

- ***http://www.american.edu/policies***



Privacy

While American University strives to protect its users' personal information and privacy, it cannot guarantee the security of any information you disclose online and you do so at your own risk.

As a Web user, keep in mind that whenever you give out personal information online information can be collected and used by people you don't even know.

Learn more about organizations working to protect your privacy at:

- ***http://www.eff.org/issues/privacy***

Protecting Data

Cyber Security means not only protecting your data from malicious threats, but also from unforeseen accidents or physical theft. Consider your personal backup strategy so you won't be caught unprepared. There are options from "set it and forget it" cloud backup services which automatically back up data for a yearly fee, to using your AU network drive to periodically back-up data

Google drive - ***https://drive.google.com/***
Apple iCloud - ***https://www.apple.com/icloud/***
Backblaze - ***https://www.backblaze.com/***
Carbonite - ***http://www.carbonite.com/***
AU Network Drives - ***http://www.american.edu/oit/network/netstorage.cfm***