The Division of Information Technology (IT) is the chief provider of technology infrastructure, services and applications at the George Washington University. The Division of IT partners with stakeholders across GW to equip students, staff and faculty with the technology know-how and tools necessary to achieve academic excellence. The Division of IT serves as a trusted technology partner with the university, evaluating and delivering innovative and collaborative technology solutions that promote and advance teaching, learning, research and support for the GW community.

In addition to providing high-quality services and support, the Division of IT works to protect the university from potential security threats and effectively detect, respond to and mitigate any incidents that may arise. The division works to enable GW community members to safely and securely create, consume and distribute information on campus.

If you have questions or require technical assistance, please contact the IT Support Center at 202-994-GWIT (4948), ithelp@gwu.edu or http://itsupport.gwu.edu. Technical assistance is available through the IT Support Center 24 hours a day.
IT Security is Everyone’s Responsibility: The “90/10” Rule

In order to ensure security, users should follow the “90/10” rule. Only 10 percent of security safeguards are technical, and the remaining 90 percent is based on following safe computing practices, such as locking your devices, creating strong passwords and not opening attachments from unknown sources.

The Top 5 Ways Users Get Compromised

1. Malicious ad providers
2. Phishing attacks through social networking sites and e-mail
3. File-sharing websites
4. Worms (self-replicating malware programs that can send copies of themselves to other computers on a network) on social networking sites that lead to malicious websites
5. Trojan software applications that can be downloaded unknowingly

Tips for Staying Safe on Your Devices

- Use strong passwords. If your password is a word that can be found in the dictionary, it is not a strong password.
- Never share your passwords with anyone.
- Do not open messages or click on links sent by unknown users.
- Never give out your personal information, such as passwords, via e-mail.
- Do not open files with suspicious extensions, such as .trojan, .exe, .scr, .vbs, .hta, .reg or .bat.
- Always install updates for your installed software.
- Encrypt sensitive data. To know more about encryption safeguards, please e-mail us at infosec@gwu.edu.
- Back up your data securely.
- Use secure sites (designated by “https” in the URL or a padlock icon) for the following:
  - If you are about to enter sensitive information on a website
  - If you are on a public wireless network and entering information
- Do not store sensitive information on your mobile devices.
- Lock your devices when they are not in use, and enable automatic locking on your mobile devices.
- Add a 5-digit passcode (instead of a 4-digit one) to enable automatic locking on your mobile devices.
- Before you e-cycle a device, work with an IT support analyst to wipe your data.
- When traveling or driving, stow your laptop in the trunk of your car.
- Do not store sensitive information on your mobile devices.
- When you are about to enter personal information, such as passwords, via e-mail. Forward suspicious e-mails to abuse@gwu.edu.
- Avoid clicking on unsolicited links and do not download unrecognized files.
- Pop Quiz:
  1. You receive an e-mail from the university asking you to provide your e-mail username and password. What should you do?
     - a. Do not respond! GW will never ask you for your username and password via e-mail. Forward suspicious e-mails to abuse@gwu.edu.
     - b. If you suspect the e-mail is unauthorized, make a call to your supervisor to verify whether this request is legitimate.
  2. What can you do to protect your personal information and computer?
     - a. Read the privacy statements on every social networking site. Ensure that you customize and verify your privacy settings and statements.
     - b. Ensure that you change your password periodically.
     - c. If you suspect an unauthorized person gained access to your account settings and other information, you may want to contact the university.
  3. Who can you contact with any IT-related questions or concerns?
     - a. Technical assistance is available through the IT Support Center 24 hours a day.
     - b. Avoid malicious ad providers and third-party games on mobile websites.
     - c. Do not store sensitive information on your mobile devices.

Tips for Safe Use of Social Media:

Read the privacy statements on every social networking site you use to ensure that each site has features you can enable to minimize your exposure. If a site’s privacy settings are weak or nonexistent, consider using another application instead.

- A good test is to search for yourself on Google or another search engine to see what information others can access.
- Some sites such as Facebook have been known to change their privacy settings and statements. Ensure that you customize and verify your privacy settings, and be aware of sites’ privacy policies and end-user agreements.
- Do not accept friend requests from unknown individuals.
- Avoid sharing confidential work or personal information on social networking sites.
- Avoid apps and third-party games on Facebook, as these can give game providers access to your account settings and other information you may not want to disclose.

Accounts and User IDs

- **GWid**: A GWid is an alphanumeric identifier used in place of a Social Security number to recognize your records within the university’s administrative systems. Your GWid is the letter G followed by an 8-digit number. To retrieve your GWid, visit https://banweb.gwu.edu.
- **NetID and E-Mail Account**: Your NetID is a single username with a corresponding password that gives you access to applications such as the MyGW Portal, GW’s wireless networks, Blackboard and GW’s e-mail and calendar systems. To claim your NetID, visit https://identity.gwu.edu/claim.
- **Novell Accounts**: Novell accounts are used to obtain access to group- and home-shared drives on which you can securely store data. To request an account, work with your supervisor to submit a form at http://helpdesk.gwu.edu/accounts/novell/index.cfm.
- **Banner, EAS and VPN**: To make a request, work with your supervisor to submit the appropriate forms at http://financeoffice.gwu.edu/comptroller/fss/fss_forms.html.
- **Phone/Voicemail and Long Distance Setup**: For setup, work with your supervisor to submit a request to itorder@gwu.edu.
- **Time and Attendance Setup**: Kronos is the university’s time-keeping system, and it is used to track time for non-exempt employees. The request form is available at http://www.gwu.edu/~payroll/forms/TRS_AccessRequest08.pdf.
- **BMC Remedy**: BMC Remedy is the university’s most widely used incident management system. To request access, work with your supervisor to submit a request to itorder@gwu.edu.
- **G1 Accounts**: Students, faculty and staff must create G1 accounts in order to use the computers in university computer labs. To create a G1 account, visit http://acadechgt.gwu.edu/pages/computingaccount.

Pop Quiz:

1. You receive an e-mail from the university asking you to provide your e-mail username and password. What should you do?
   - a. Do not respond! GW will never ask you for your username and password via e-mail. Forward suspicious e-mails to abuse@gwu.edu.
   - b. If you suspect the e-mail is unauthorized, make a call to your supervisor to verify whether this request is legitimate.
2. What can you do to protect your personal information and computer?
   - a. Read the privacy statements on every social networking site. Ensure that you customize and verify your privacy settings and statements.
   - b. Ensure that you change your password periodically.
   - c. If you suspect an unauthorized person gained access to your account settings and other information, you may want to contact the university.
3. Who can you contact with any IT-related questions or concerns?
   - a. Technical assistance is available through the IT Support Center 24 hours a day.
   - b. Avoid malicious ad providers and third-party games on mobile websites.
   - c. Do not store sensitive information on your mobile devices.