Security is Everyone’s Responsibility: The “90/10” Rule

In order to ensure that GW data in your jurisdiction is kept secure during your time in GW, 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.

Most Common Ways Users Get Compromised

1. Trojans (network software applications that can access users’ personal data) that are hidden in games, videos and programs
2. 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
3. Phishing attacks through social networking sites and email
4. Malicious ad providers
5. File-sharing websites

Tips for Staying Safe on Your Devices

- Use strong passwords that are hard to guess. If your password is a word that can be found in the dictionary, it is not a strong password.
- Enable Two Step Authentication, where it is available.
- Never share your passwords with anyone.
- Do not open messages or click on links sent by unknown users.
- Do not open files with suspicious extensions, such as .exe, .scr, .vbs, .hta, .reg or .bat.
- Keep your software up to date by installing the latest updates.
- Use secure sites (designated by “https” in the URL or a padlock 🗼) for the following:
  • Entering sensitive information on a website.
  • Entering information on a public wireless network.
- Do not store sensitive information on your mobile devices.
- Backup your data securely.
- Lock your devices when they are not in use, and enable automatic locking on your mobile devices. Add a 6-digit pass-code (instead of a 4-digit one) to your mobile device for increased security.
- Before you e-cycle a device, work with an IT support analyst to wipe your data.
- When traveling or driving, store your laptop in a place where people will not see it, such as the trunk of your car.
- Avoid using administrator privileges when they are not needed.
- Read the warnings and pop-ups that appear when you use applications.
- Enable remote locator and wiping services on your mobile devices. These services can help recover lost or stolen property and/or delete a device’s data remotely if the device cannot be recovered.
- Avoid saving your passwords on apps and mobile websites. Instead, use vetted password management applications.
Accounts and User IDs

- **GWID**: A GWID is an alphanumeric identifier used 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, use the GWID Retrieval Request form.

- **NetID and Email 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 email and calendar systems. To claim your NetID, visit the NetID Claim site.

- **Two-Step Authentication**: This system provides the GW community an extra layer of security when accessing online systems and information. It is used in conjunction with the GW Single Sign-On service. For details or to set up your two-step authentication, visit the Two-Step Authentication site.

- **Digital Workplace**: This is a great starting point to request any IT assistance. Help with email, phone communications, Internet access, and more - it’s all on the Digital Workplace site.

- **Banner and VPN**: To make a request, work with your supervisor to submit a request in Digital Workplace.

- **Phone/Voice Setup**: For setup, work with your supervisor to submit a request in Digital Workplace.

- **Time and Attendance Setup**: Kronos is the university’s time-keeping system. Additional information, including payroll-related forms, can be accessed on the GW HR Payroll site.

- **Classroom Computer Guest Accounts**: Classroom computer accounts are for guests and members of the GW community that do not have a GW NetID. To request an account, please fill the Classroom Computer Guest Account Request form.

Tips for Safe Use of Social Media:

- Read the privacy statements on every social network you use to learn what they collect and share about you. If a site’s privacy settings are weak or nonexistent, consider using another application instead. At least limit what personal data you post.

- Google you - By searching for your information or using your name in a search engine, you will be able to view your online presence and shared details.

- Remember that what you post online stays online and can be found. Your family members, professors and future employers may find that embarrassing post or photo in which you were tagged!

- 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 social media, as these can give game providers access to your account settings and other information you may not want to disclose.

To Recap:

1. **You receive an email from the university asking you to provide your email username and password. What should you do?**
   
   Do not respond! GW will never ask you for your username and password via email. Forward suspicious emails to abuse@gwu.edu.

2. **What can you do to protect your personal information and computer?**
   
   Adhere to the following safe computing practices: lock your devices when they are not in use; encrypt sensitive data; use strong passwords and do not share them; back up data; avoid clicking on unsolicited links and do not download unrecognized files.

3. **Who can you contact with any IT-related questions or concerns?**
   
   Contact the IT Support Center at 202-994-GWIT (4948), email ITHELP@gwu.edu or visit the GW IT site.
GW Information Technology ("GW IT") is the chief provider of technology infrastructure, services and applications at the George Washington University.

GW IT partners with stakeholders across GW to equip students, staff and faculty with the technology know-how and tools necessary to achieve academic excellence. Importantly, GW IT serves as a trusted technology partner including, 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, GW IT Security operates to protect the university from potential threats and vulnerabilities, such as hackers and ransomware, respond to and mitigate any incidents that may arise.

If you have questions or require technical assistance, please contact the IT Support Center at 202-994-GWIT (4948), email ITHELP@gwu.edu or visit the GWIT site.