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. 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. 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 email.
- Do not open files with suspicious extensions, such as .exe, .scr, .vbs, .hta, .reg or .bat.
- Always install updates for your installed software.
- Encrypt sensitive data. To know more about encryption safeguards, please email us at infosec@gwu.edu.
- Back up your data securely.
- Use secure sites (designated by “https” in the URL or a padlock �短缺) 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 6-digit passcode (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, stow 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.
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 IT.GWU.EDU/accounts.

- **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 https://identity.gwu.edu/claim.

- **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 here. To request access, work with your supervisor to submit a request to go.gwu.edu/digitalworkplace.

- **Banner and VPN**: To make a request, work with your supervisor to submit the appropriate forms at go.gwu.edu/digitalworkplace.

- **Phone/Voice Setup**: For setup, work with your supervisor to submit a request to go.gwu.edu/digitalworkplace.

- **Time and Attendance Setup**: Kronos is the university’s time-keeping system, and it is used to track time for non-exempt employees. Additional information, including payroll-related forms, can be accessed at http://payroll.gwu.edu/payroll-forms.

- **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 visit http://acadtech.gwu.edu/guest-account-form.

- **Two-Step Authentication**: This system secures online access and information through the use of a password and a second code sent to your mobile device. For details or to set up your two-step authentication process, visit IT.GWU.EDU/two-step.

Tips for Safe Use of Social Media:

- Read the privacy statements on every social network 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.

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), ITHelp@gwu.edu or IT.GWU.EDU.
The Division of Information Technology (IT) is the largest 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 IT.GWU.EDU.