Howard University
Enterprise Technology Services
Information Security
2301 Georgia Ave, NW
Suite 334
Washington, DC 20059
infosec@howard.edu

Questions?
Contact the Help Desk at
(202) 806-2020

Information Security Guide
2014

Partnering with you to protect Howard’s Information and Technology Assets.

Enterprise Technology Services
Q. What is Phishing?
A. Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. This is usually combined with a threat or request for information: for example, that an account will close, a balance is due, or information is missing from an account.

Q. What should I do if I receive an email that looks suspicious?
A. If you receive any email that looks suspicious, or from anyone unknown to you, before forwarding to any other recipient please call the ETS Service Desk at 806-

Q. I received an email from a non-University website that asks for my HU username and password. What should I do?
A. Your HU username and password should only be used at howard.edu sites.

Q. How do I know if I’m accessing a legitimate HU website?
A. Look at the address between the // and the first / - it should end with howard.edu
Fake: http://www.sample.ru/js/mail/howard.edu
Real: https://mobile.howard.edu/owa/auth/logon.aspx

Q. The email contains a link from ETS to a website requesting me to enter my HU username and password?
A. When HU upgrades its computers or email systems, we will NEVER send a link inside an email which will go to a website requesting that you login or enter your username and password. If a login is necessary we will just tell you what site you need to access (i.e., outlook.com/howard.edu/owa) with no link to click. ETS, including the Service Desk (formally the Help Desk) and Information Security Services, will NEVER ask you for your password via email, phone or in person. Never reply to an email that requests your username and password.

Be suspicious of any unsolicited emails asking for information and do not click on links within emails.
We are serious about our technology policy.

Howard owns all university-purchased computers, network infrastructure and software assets, including e-mail, Internet access, data, documents, software residing on its systems, etc. HU’s information resources are provided for university purposes, including academic, research, administrative, and collaborative uses. Computers and the network should be used in a manner that maintains confidentiality and protects the information contained on the system.

In order to protect our information resources as well as the rights and privileges of Howard’s faculty, staff, and students, the University has the right to monitor and ensure that these systems are not used in a way that damages the university, its students, or its employees. Howard requires that access to the network and university information be done in strict accordance with relevant local, state, and federal laws and Howard University’s policies.

Howard ETS is responsible for creating and managing operational practices that underlie this Acceptable Use Policy. Pertinent practices related to information security can be found at http://howard.edu/technology/services/security.

For more details on Howard University’s “Acceptable Use of Computing and Information Technology Resources” policy, please go to http://www.howard.edu/secretary/policy/byseries.htm.

Information Security is a Collective Responsibility

You Can Make a Difference!

As an institution of higher education, Howard University encourages active transfer of knowledge for learning, teaching, and research. Indeed, Howard is committed to a collaborative and open environment where discourse and discovery prevail.

In today’s technology intensive world, the exchange of information increasingly takes place through electronic means and extends to administrative information such as student data, employee records, grants funding, and other proprietary areas. With the ubiquitous use of Internet-based tools, information can be transmitted around the world within seconds. As such, it is critical that each of us at Howard do our part in protecting the integrity and confidentiality of our information resources.

This Information Security Guide is intended to assist you in your daily activities and help safeguard you from situations that could inadvertently disclose university information, compromise privacy, or impair the functionality of the computer.

Please keep this guide close at hand and use it.

Be respectful of policies
**Handling Sensitive Information**

**Restrict access on a need to know basis.**

If you have access to sensitive information, you must safeguard it from damage, loss, misuse, or unauthorized disclosure. Sensitive information includes, but is not limited to, personally identifiable information about Howard’s students, faculty, and staff; medical and health information; research and technology initiatives; business and financial matters; and fundraising and alumni issues.

As a matter of practice, treat the information you possess in the course of your work as sensitive and follow these practices:

- Maintain the confidentiality of the information stored on your computer by using only Howard-approved hardware and software for processing sensitive information.
- Lock or log off computers when away from your desk (ALT-CTRL-DEL, then lock workstation or logoff).
- Use a password-protected screensaver.
- Keep sensitive files from inadvertent disclosure by ensuring they are not on freely accessible servers (web, FTP, unauthenticated file shares).
- Report any breach of security in any system that stores sensitive information (including lost or stolen laptops, access cards, PDAs, etc.) immediately to Campus Security at 202-806-7777, 202-806-1103 or Information Security at InfoSec@howard.edu.

**Disclose information selectively.**

**Human Capital & Financial Management Systems**

**PeopleSoft** facilitates HR and financial management functions at Howard.

PeopleSoft enables Howard employees to easily access payroll and benefits data and securely manage personnel and financial tasks.

This system meets the highest standards for information security. Social security numbers are completely masked, and banking information is partially masked.

To maximize the existing robust security safeguards of PeopleSoft data, please follow the following security guidelines:

- **Do not share your network password with anyone.** Along with your network ID, it is the key to your personal data.
- Follow the Howard University’s password guidelines posted at http://www.howard.edu/secretary/policy/byseries.htm
- Do not enable automatic login on the PeopleSoft website.
- Be sure to log out each time you visit the PeopleSoft website, no matter how quickly you plan to log back in.
- Avoid using your Howard ID and password combination for other personal accounts (bank accounts, ISPs, local machine accounts, web services, etc.)
- Keep your network password private.
FERPA, a federal law, applies to student records and information.

The Family Educational Rights & Privacy Act (“FERPA”) protects the privacy of student education records.

Persons with access to student data should become familiar with FERPA basics:

- Student education records are considered sensitive and may not be released without the written consent of the student.
- Howard community members have a responsibility and obligation to protect student education records in their possession. FERPA information is to be stored and transmitted using practices for sensitive information.
- Before releasing any student information, including directory information, you should consult the University Registrar’s Office to ascertain whether the information can be disclosed.
- Students may request FERPA suppression of their directory information by contacting the University Registrar’s office.
- Access to student data is restricted to individuals who need this information for legitimate educational purposes. Faculty and staff requesting access to student information must first contact the University Registrar’s office.

Be respectful of student privacy.

---

E-mail and Instant Messaging

E-mail and IM are not risk free.

Always use care when sending e-mail. E-mail systems are porous, and typically messages go through multiple machines before they finally arrive at their intended destination. Once messages have been sent, you no longer have control over any subsequent distribution. Moreover, as a recipient, you have no assurance of a message’s security and authenticity.

However, a few simple things can reduce e-mail risks:

- Be cautious about what you send. Unless the message is encrypted, you should assume that someone other than the intended recipient could read your mail. You also do not know where your message may be forwarded, so exercise caution in crafting your message.
- Be wary about the actual source of received e-mails. E-mail can be forged. Treat each e-mail message cautiously and double check with the sender if you are in doubt.
- Set up spam and junk mail filtering to reduce your mail volume and risk.
- Do not open an attachment that seems odd or out of context. It might contain a virus.
- Always check the “To:” distribution line before sending a message. Be particularly careful when using the “Reply All” feature. This can result in the proliferation of numerous messages or sending messages to unintended recipients.
- Howard’s e-mail system is provided for university related purposes; personal usage should be kept to a minimum.
- Ensure that your e-mail client (program) is configured to use encrypted protocols between the client (program) and e-mail server (e.g. SSL or TLS).

Call the sender to verify authenticity of suspicious attachments.
Passwords

Keep your Network ID, Passwords, and PINs Confidential.

To access many Howard information systems and network services, a network-ID and password are required. The Howard login process ensures that only authorized individuals can access the university’s systems and data. Robust password practices are important in safeguarding against unauthorized access. Keep in mind the following guidelines to help keep your password confidential and secure:

- Be creative and careful when selecting a password. Don’t use anything that can be easily guessed, including personal information such as names, hobbies, or commonly used words. Never use your social security number as a password.

- Strong passwords should be at least 12 alphanumeric characters in length. They should contain a combination of lower and upper case letters, numbers, and symbols. One technique for selecting and remembering a password is to pick a phrase you find significant. Construct a password using any letter from each of the words in the phrase. Minimum password guidelines can be found at http://www.howard.edu/secretary/policy/byseries.htm

- Passwords should be changed often (we recommend every 90 days) or whenever you believe confidentiality has been compromised. You can change your network password at any time.

- Passwords should not be shared, posted, written down, or recycled.

- Passwords should be unique for each of the different services to which you subscribe (i.e., pick a different password for your banking accounts, for credit cards, Howard, Yahoo, AIM, etc.).

- Do not include your password in an automated logon process. Make the extra effort to type it in each time.

- Passwords should also be used on laptops and mobile devices (e.g., mobile phones, BlackBerrys, and PDAs) to protect information on these devices.

Be creative with your password and keep it to yourself.

HIPAA Security Rule

HIPAA mandates the protection and privacy of patient health information.

HIPAA’s (Health Insurance Portability and Accountability Act) security rule requires that everyone with access to electronic personal health information (ePHI) implement safeguards to protect against inappropriate and unauthorized access to patient health data.

As stipulated in HIPAA rules and regulations:

- Protect all ePHI you might create, receive, maintain, or transmit.

- Ensure that patient data is safeguarded against potential hacking and unauthorized access.

- Partner with HIPAA experts at Howard to ensure that you are in compliance with the requirements of the HIPAA Security Rule.

To find out more about HIPAA, please contact the Howard Compliance Office at huh_compliance@howard.edu.

Protect electronic patient health information.
Electronic viruses are rampant. Protect yourself.

Computer viruses can be debilitating to individual systems and entire networks. Viruses have the capability to spontaneously spread throughout the network, often without any intentional action on the part of the victim. You can mitigate virus infections by following these procedures:

- Never open an unexpected e-mail attachment.
- Make sure that you understand the source and purpose of any attachment before opening it.
- When in doubt, you should verify the authenticity of any attachment with the actual sender before opening it.
- Do not allow files to execute macro commands without understanding what they do and where they originated. Macro commands can propagate viruses and may be embedded in files.
- Make sure that your computers are always running current anti-virus software with routine virus prevention updates. You can download the most recent anti-virus software from the Howard Software Center at http://secure.howard.edu.
- Update your virus patches weekly.
- Be wary of unusual system behavior and report it to the Help Desk.

Computer Viruses

Practice safe computing.

Spam Protection

Spam is more than a nuisance.

Spam continues to grow at exponential rates, consistently outpacing the growth in legitimate mail volume at Howard and elsewhere. Also known as UCE (unsolicited commercial mail), spam is not only a nuisance, but can transmit viruses, malware, and spyware.

The following tips can assist in reducing spam:

- Be careful about giving your email address when completing forms online.
- Consider using a separate e-mail address for some public activities such as chat rooms, in order to protect your main e-mail address from spammers.
- Never respond to unsolicited e-mail. Spammers will use your reply, even your unsubscribe messages, as evidence that the e-mail address is valid.
- Never buy anything advertised in spam. Most of it is dubious at best.
- Never post your e-mail address publicly on the Web. Spammers have ways to collect and use these e-mail addresses.
- Always opt-out of company solicitations you do not wish to receive.
- Do not use an unsubscribe link from an e-mail as it legitimizes your e-mail address; can download malware that turns your computer into a proxy for sending spam, or can enable remote access to your computer.

It’s best to just delete suspected spam right away.
**Internet**

**Be aware of Internet risks.**

An extraordinary resource, the Internet is, nevertheless, an unregulated environment. To minimize unnecessary and risky exposure while on the Internet, be attentive to the following:

- When viewing or requesting web content, programs may be automatically initiated. Do not choose to execute such programs without being sure of their source, their function, and their effect on your machine’s operation.
- Your Internet activities may occasionally cause security warnings to appear. Pay attention to these messages and act cautiously.
- Don’t assume that information found on the Internet is necessarily accurate or up to date.
- Make sure that all materials you download comply with all applicable laws, copyright restrictions, and Howard policies.

![Image](image1.png)

**Always double-check facts gathered on the Internet.**

---

**Public Wireless Hotspots**

**Wireless networking requires vigilance.**

Wireless access is now ubiquitous at major airports, coffee shops, hotels, and other public venues. While convenient, public access points are obviously public. To protect yourself and your personal information, take the following precautions with public wireless access:

- Use a VPN (virtual private network) encrypted connection when you access proprietary information wirelessly. Also make sure your VPN is configured correctly. For information on accessing Howard University information through a VPN connection, go to http://www.howard.edu/technology/services/network.
- Don’t sign up for wireless service at the hotspot itself especially if the provider requires that you create a login and supply personal information. Instead bookmark the sign-up page and then sign up from a secured location such as your home or office computer.
- Pop-ups are a common trick for installing spyware, viruses, and other infections. If you get a pop-up message on your screen while using a public hotspot, read the pop-up carefully before you click OK. Unless you are confident about the authenticity of the pop-up, close it promptly.
- Do not enter sensitive information on the web wirelessly (or otherwise) unless you are sure the information is encrypted. Sometimes this is indicated by the image of a lock usually in the lower right hand corner of your browser or by the letter “s” as in https:// in the URL of the website.
- In public hotspots, it is prudent to be offline until you actually need to be connected to the internet. Enable your wireless adapter only when you are ready to be online.
- If the public network is acting unusual, assume it’s compromised. Get off the network and disable your wireless connection immediately.

![Image](image2.png)

**Use VPN to access proprietary information wirelessly.**
Spyware

Protect yourself from spyware intrusions.

Spyware surreptitiously can capture and transmit personally identifiable information (ranging from surfing habits to credit card information) from a computer to a third party over the Internet. Spyware sometimes comes bundled with otherwise seemingly legitimate programs and typically installs secretly in the background of your computer as the legitimate program installs.

Combating spyware requires software and vigilance.

- Use an anti-spyware product from a trusted vendor. Since no product provides 100% protection, the most prudent strategy is to combine two anti-spyware scanners. Make sure you download from legitimate sites; otherwise you may find yourself installing spyware.
- Use a personal firewall product and keep it updated.
- Examine your web browser setting for active content controls.
- Do not accept downloads from pop-up windows or unknown websites.
- Read licensing agreements before installing software, especially freeware, shareware or peer-to-peer applications.
- Be very careful when installing free, ad-supported software and be wary of programs that flash ads in the user interface.
- Be sure to setup file sharing software correctly. Peer-to-peer file sharing is a source of many spyware programs.
- Be aware of your computer’s performance. Changes in settings, sluggish performance, and instability are signs of spyware. The cumulative effect of spyware can bring a PC to a near standstill.

Phishing

Protect yourself from identity theft.

Phishing is a form of Internet fraud that scams people into unwittingly providing sensitive information under false pretenses. Identity theft is a multi-billion dollar industry fortified by phishing.

The “phisher” will broadcast emails that appear to be sent from legitimate enterprises such as banks, brokerage houses, online retailers, etc. The recipients will be asked to update their credit card information, account information, passwords, etc. They might also be prompted to enter their social security number, date of birth, and other important identifying information. Generally the user is redirected to a website that also looks authentic and is branded appropriately.

Keep in mind that:

- Legitimate organizations NEVER request personal information in such a way.
- A phishing e-mail is seldom addressed to you directly, but uses a general salutation such as “Dear Valued Customer.”
- A phishing webpage will look authentic. Anyone with a little HTML code experience can create fraudulent sites that look real.
- If you are unsure, call the organization to verify that it did indeed send the e-mail. Do not use the phone number provided in the phishing e-mail. Look up an alternative number in your records or in the phone book.
- Phishing is rooted in information and identity theft, which permits online theft of millions of dollars.

Never respond to online requests for personal information.

Run anti-spyware programs regularly.
Identity Theft

... is the fastest growing crime in the United States.

A few safety precautions can help mitigate against identity theft.

- Never print social security numbers on checks.
- The next time you order checks, print only your first initial along with your last name and do not print your home address.
- When paying your credit card by check, DO NOT put the complete account number on the “memo” line.
- The last four digits will suffice to process your payment.
- If your wallet is stolen, cancel all credit cards immediately (see organizational tip below).
  - File a police report as quickly as possible in the jurisdiction where the theft occurred.
  - Contact all three national credit reporting organizations and the social security administration (listed below) to place a fraud alert on your name and social security number.
    - Equifax: 1-800-525-6285
    - Experian: 1-888-397-3742
    - TransUnion: 1-800-680-7289
    - Social Security Administration fraud line: 1-800-269-0271
- Audit your credit report on a regular basis.

Organizational Tip:

Photocopy (on one sheet of paper) the front and back of all the credit cards you regularly carry in your wallet. This will help consolidate all your account numbers and phone numbers in one place. Be sure to keep this sheet in a safe place. When you travel, make sure you can quickly access this information, if needed.

Be proactive about protecting your identity.

Anti-Hacker Checklist

Never divulge information to strangers.

Hackers often obtain confidential information by contacting employees who unintentionally respond, thinking that they are being helpful.

Here are some tips that can help minimize the potential for unauthorized access to confidential information:

- Verify the identity of callers requesting information. If you can’t immediately identify them, insist on calling them back. You should make sure that they are legitimately entitled to receive any information being requested.
- Don’t give out information about yourself or other employees. Refer all inquiries to Human Resources, or relevant authorities.
- Don’t discuss Howard’s computer hardware, software, or environment (including network connectivity) unless you know the person or can verify both his/her identity and his/her need to know.
- Don’t let yourself be pressured or manipulated into giving out information. When someone calls asking for your help in some way that is unusual, be cautious and purposeful in your reaction.
- Never respond to online inquiries about banking, credit card, or other personal information. Banks, credit card companies, and ISPs never request information in this way. Neither will Howard.
- Never under any circumstances give out your password to anyone, no matter how urgent the request.
- If you believe that you received an inappropriate request for information, report the incident immediately to your supervisor, or designated authority.

Hackers use computers, phones, and casual conversations to gather important information.
**Software Piracy and Copyright**

*Use only licensed software on your computer.*

The University provides many approved software programs and packages generally at no cost to Howard faculty, staff, and students. To download the latest versions of many popular HU-approved software packages, please go to: [http://www.howard.edu/technology/services/network](http://www.howard.edu/technology/services/network)

In general, when downloading software, follow these general guidelines:

- Do not install any unauthorized software on your PC. When in doubt, consult the Help Desk for guidance.
- If you have a requirement for a specific software package that is not available at the Howard Software Center, please contact your business manager or the Help Desk.
- Creating unauthorized copies of vendor software can result in serious legal complications, including civil and criminal liability. If you are using unauthorized copies of software, promptly remove them from your computer.
- Howard takes immediate action upon the report of copyright violations.

**Removable Media**

*These powerful tools can be full of important and proprietary information.*

Removable media such as CDs, DVDs, hard drives, zip drives, USB drives, and other media often contain important information and should be secured. 

- Lock up removable media containing confidential information when not in use.
- Do not place disks or other removable media near magnets or other magnetic devices, as these could destroy information.
- Properly label all removable media.
- Be careful not to damage the removable media.
- Do not dispose of a disk that contains important data without ensuring the destruction of that information. Remember that simple file deletion does not permanently erase files; in such cases, the information can still be restored. If the disk contains sensitive information, reformat the disk or physically break it.
- Be sure to inventory the contents of your media on a regular basis.

Howard’s Software Center is a resource for all faculty, staff, and students.
**Voice Mail**

Ensure voicemail confidentiality.

To avoid voicemail intrusion, you should keep in mind the following procedures:

- Select passwords that have at least four characters; however eight character passwords are recommended, as these are typically harder to decode.
- Do not tell anyone else your password.
- Avoid writing your password down.
- Change your password immediately if you think that someone else knows it.
- Change your password periodically.
- Review your greeting message from time to time to ensure it has not been changed without your knowledge.

Do not forward confidential information through voice mail.

**Mobile Devices**

Be cautious when using mobile devices.

Mobile devices such as laptops, pagers, mobile phones and handhelds (e.g., PDA, Smart phones and BlackBerrys) are a convenient way to take information and databases anywhere you go. Unfortunately, their portability makes them a popular target for thieves. Sensitive information is often maintained within mobile devices.

The following tips will assist you in safeguarding mobile devices, as well as the sensitive and proprietary information they may contain:

Do...

- Backup your data regularly and keep an updated copy in a separate location.
- Keep mobile devices out of sight and secure whenever possible.
- Know what you have stored on your devices and periodically inventory their content.
- Require passwords to access your mobile devices.

… Do Not

- Do not store sensitive information (e.g., your password, credit card information, bank information, etc.) in the device. Such devices often have limited security and are usually unable to withstand a determined attack.
- Do not leave the mobile device unattended. Mobile devices are easily lost or stolen. When traveling, carry the device as hand luggage and be cautious in public places (e.g., airports or hotels).
- Do not discuss or view confidential information where others may be able to hear or view the information.
- Do not cache your Howard ID in auto-logins from mobile devices.

Password protect your mobile device.
Protect your electronic equipment from theft.

Computers are valuable assets with expensive hardware, valuable software, and, most importantly, proprietary data and information. A few common-sense physical security practices can easily help deter equipment theft.

♦ Restrict physical access of machines to trusted and authorized individuals. Make sure you are aware of who uses or services your computer.

♦ Never leave a laptop unattended and, if you must, make sure it is secured with a cable lock, locked into docking station, or out of sight in a cabinet or drawer.

♦ Notify Campus Security at 202-806-7777 or 202-806-1103 of any suspicious persons or activity.

A five-step proactive security approach.

Step 1: Set Security Configurations

Ensure that security configurations are enabled.

Step 2: Use an Internet Firewall

An Internet firewall can help prevent outsiders from getting access to information on your computer through the Internet. Microsoft Windows comes with its own firewall. Make sure it is enabled. If you have an older version of Windows, consider upgrading to newer version of Windows. If this is not an option for technical reasons, please install alternative firewall products as specified by your operating system.

Step 3: Update Your Computer

Update your computer regularly by downloading the latest patches. Windows Automatic Updates feature will automatically download the latest Microsoft security updates when your computer is connected to the Internet. If you have an older version of Windows, you can go directly to the ETS site.

Step 4: Use Up-to-Date Antivirus Software

Anti-virus software programs will help protect your computer against most viruses, worms, Trojan horses, and other malicious code. Many new computers come pre-installed with anti-virus software. Remember to keep your anti-virus software subscription current. Your computer will be vulnerable to new threats if your subscription lapses.

Step 5: Secure your Home Wireless Network

Make sure you secure your home wireless network against access from unauthorized users. The instruction manual to your wireless router will have complete instructions on setting up a secure home wireless network.

Be aware of your surroundings.

Be sure to activate anti-virus software before using email or the Internet.