INFORMATION TECHNOLOGY

Guidelines & Answers

Information Technology's general guidelines and answers to frequently asked questions at the University of Oklahoma Health Sciences Center

OUHSC SERVICEDESK

Located in the
David L. Boren Student Union
Room 105

(405) 271-2203
Toll Free:)888) 435-7486
Email: servicedesk@ouhsc.edu

http://www.ouhsc.edu/it/

PHISHING

Protecting your information

Phishing scams are one of the fastest growing internet crimes. Cybercriminals use phishing to steal information such as account usernames and passwords, social security numbers, or credit card numbers. In a typical scam, the cybercriminal sends an email with the intent to impersonate a person or business you know or trust. Phishing messages often include distressing or enticing statements to provoke an immediate reaction or they may threaten consequences if you fail to respond.

What Can You Do

- **Trust but verify.** If you are unsure of an email message, contact the sender for confirmation.
- **Before clicking a link,** hover over it with your mouse to reveal the address. Make sure it is legitimate. If it appears suspicious, do not click and report it to IT Security.
- **Never submit** confidential information via forms embedded within email messages.
- **Don't open attachments** in your email unless you were expecting the attachment.
- **Don't download software** from the Internet without first receiving approval from your technical support group.
- **Don't** automatically follow the directions that you receive in an email stating to immediately delete files or execute the following attachment to update your antivirus. These emails are hoax emails attempting to coerce you to execute their virus. Always make sure to contact your technical support group to clarify instructions that might be sent through emails.
- **Do update Antivirus definitions on a daily basis.** Schedule Automatic Updates for your anti-virus and Microsoft Windows to scan ALL fixed disks. For assistance contact the IT Service Desk.

OUHSC Antivirus Download Website
http://it.ouhsc.edu/services/desktopmgmnt/antivirussoftware.asp

HOT TOPICS

Things you should know

What are the highest priority Do's and Don'ts on the OUHSC Campus?

Encryption

All portable computing devices such as laptops, tablets, and smart phones, regardless of ownership, must be encrypted for use on OUHSC information systems.

Theft or Loss

Laptop computers, tablets, and smart phones have become a target of choice for thieves all over the country. Remember the following when using portable computing devices:

- Don't leave your devices in an unlocked vehicle, even if it is in your driveway or garage, and NEVER leave it in plain sight.
- Lock your device in a safe place when not in use.
- Don't leave a meeting or conference room without your laptop or personal electronics. Take them with you.
- Enroll in "find my device" services.

Cloud Services

Services such as Dropbox, OneDrive, and iCloud have **not** been approved for University business at OUHSC.

Do's and Don'ts

- Do not forward emails to any distribution lists without prior approval from the list administrator. OUHSC email is for work related business only.
- Do not forward emails about houses or apartments for rent, individuals giving away or needing free money, items for sale, jokes or stories, or emails that state "Forward to all of your friends or co-workers".
- Do not forward complaints about other people posting unwanted email to distribution lists. List administrators notify us when someone has forwarded unwanted email to their distribution list.
- Do utilize the campus notices website for the posting of items for sale, lost & found, and miscellaneous.

Campus Notices Website
http://apps.ouhsc.edu/campusnotices/

SECURITY AWARENESS

Important tips

Important security awareness tips.

Do's and Don'ts

- **Do Use Antivirus software and keep it updated.** You are required to use an antivirus program and keep the virus definitions updated.
- **Do stay clear of so called 'required downloads' and patches.** Be wary of any website that requires you to download software to view a page, unless it's something familiar like a Flash plug-in or Acrobat Reader. The file may contain a virus, a Trojan horse, or some type of auto-dialer.
- **Do keep your Operating System up to date.** Operating system vendors issue many critical updates to fix identified security flaws. Run operating system updates once a week and whenever update warnings are issued.
- **Do not reply or unsubscribe to SPAM, this only verifies that your email address is valid and then it can be sold on the Internet**. Delete SPAM Immediately.

Policy Links and Information

Acceptable Use Policy:
http://it.ouhsc.edu/policies/AcceptableUse.asp

Mass Email Policy:
http://it.ouhsc.edu/policies/MassCommunications.asp

OUHSC IT Security Policies:
http://it.ouhsc.edu/policies/

Contact Information For Computer Incidents

Information Security Services
Phone: 405-271-2476 Option #1
Email: it-security@ouhsc.edu

Acceptable Use

General Principles

By using University information systems or computing resources, you agree to abide by and comply with the applicable policies, procedures and laws. Acceptable use must be ethical, reflect academic honesty, and show responsible use in the consumption of shared resources.

You MUST NOT:

- use another person's system, files, or data without express authorization;
- use another individual's user ID or password;
- use computer programs to decode passwords or access control information;
- attempt to circumvent or subvert system or network security;
- engage in any activity that might be harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, damaging files, or making unauthorized modifications to or sharing of University data;
- use University systems for commercial, private, personal, or political purposes, such as using electronic mail to circulate advertising for products or for political candidates;
- harass or intimidate another person including, but not limited to, broadcasting unapproved, unsolicited messages, repeatedly sending unwanted or threatening mail, or using someone else's name or user-ID;
- waste computing resources or network resources including, but not limited to, intentionally placing a program in an endless loop, printing excessive amounts of paper, or sending chain letters or unapproved, unsolicited mass mailings;
- attempt to gain access to information or services to which you have no legitimate access rights;
- engage in any other activity that does not comply with the General Principles presented above, University policies and procedures, or applicable law.

(Acceptable Use Continued)

You MUST:

- comply with all University policies, procedures, and local, state, and federal laws;
- use resources only for authorized administrative, academic, research or clinical purposes; or other University business;
- protect your user-ID and system from unauthorized use. (you are responsible for all activities on your user-ID or that originate from your system);
- access only information that is your own, that is publicly available, or to which you have been given authorized access;
- comply with all copyright laws, licensing terms, patent laws, trademarks, trade secrets and all contractual terms;
- be responsible in your use of shared resources (refrain from monopolizing systems, overloading networks, degrading services, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.

Find Answers…

Find information on getting connected to the Internet, account questions, changing passwords, help with your email, setting up a website, or getting virus and security information. Get help with on-campus telephone billing questions, making long-distance phone calls, and other telecomm questions. Also, get information on buying computers, hardware, and software through the university.

Goto: **http://help.ouhsc.edu**

Revised 8/4/2016