Security Awareness

ITS Security Training

Spring 2016

THE UNIVERSITY OF MEMPHIS

Why is Security so Important?

- Technology can address only a fraction of security risks.
- You are a primary target, or rather, your data and access to data are a target.
- Gaining access to your personal data allows criminals to take your research or your personal information. It also allows them to impersonate you, or your computer, to gain access to other systems and data.

Security Basics

- University Policies
- Passwords
- Browsing
- Email
- Desktop and Mobile Device Security
- Data Security and Encryption
- Remote Access / VPN
- Securing The Human Training
- Reporting an incident
- Reminders
- Other Resources

University Policies

- UM1337 – Data Access
- UM1535 – Acceptable Use of IT Resources
- UM1691 – Campus Data Security
- FERPA – Federal Educational Rights and Privacy Act
  - http://www.memphis.edu/registrar/faculty/ferpa.htm

University Policies Site – http://policies.memphis.edu

Passwords

- Password Complexity
  - Hackers and tool kits anticipate patterns and context, so avoid words like “memphis” in your UofM password or “credit” on your credit card account.
  - Using personally identifiable information will also be anticipated, so avoid passwords containing words or names from your family and public record.
  - The University of Memphis enforces a standard set of complexity requirements.
- Password Change Frequency
  - Frequency can be as important as complexity. Expired passwords are useless.
  - The University of Memphis currently enforces a 6 month expiration policy.
- Password Reuse
  - Maintain different credentials per service. Hackers know it’s hard to keep up with multiple passwords. If they get one, they will use it against other services hoping to gain additional access. Never use your University of Memphis credentials with another service.

Password Management

- Password Management/Identity Vault
  - ITS will never ask you for your password.
  - Avoid writing passwords down or keeping them in a text file or document.
  - Email is not a password management system. Never email your password to anyone (including yourself).
  - A password management utility is one option for storing personal passwords. Many exist that work on desktops and mobile devices. These encrypt your passwords and many will also help you generate nicely complex passwords.
    - 1Password and LastPass are examples of password management utilities.

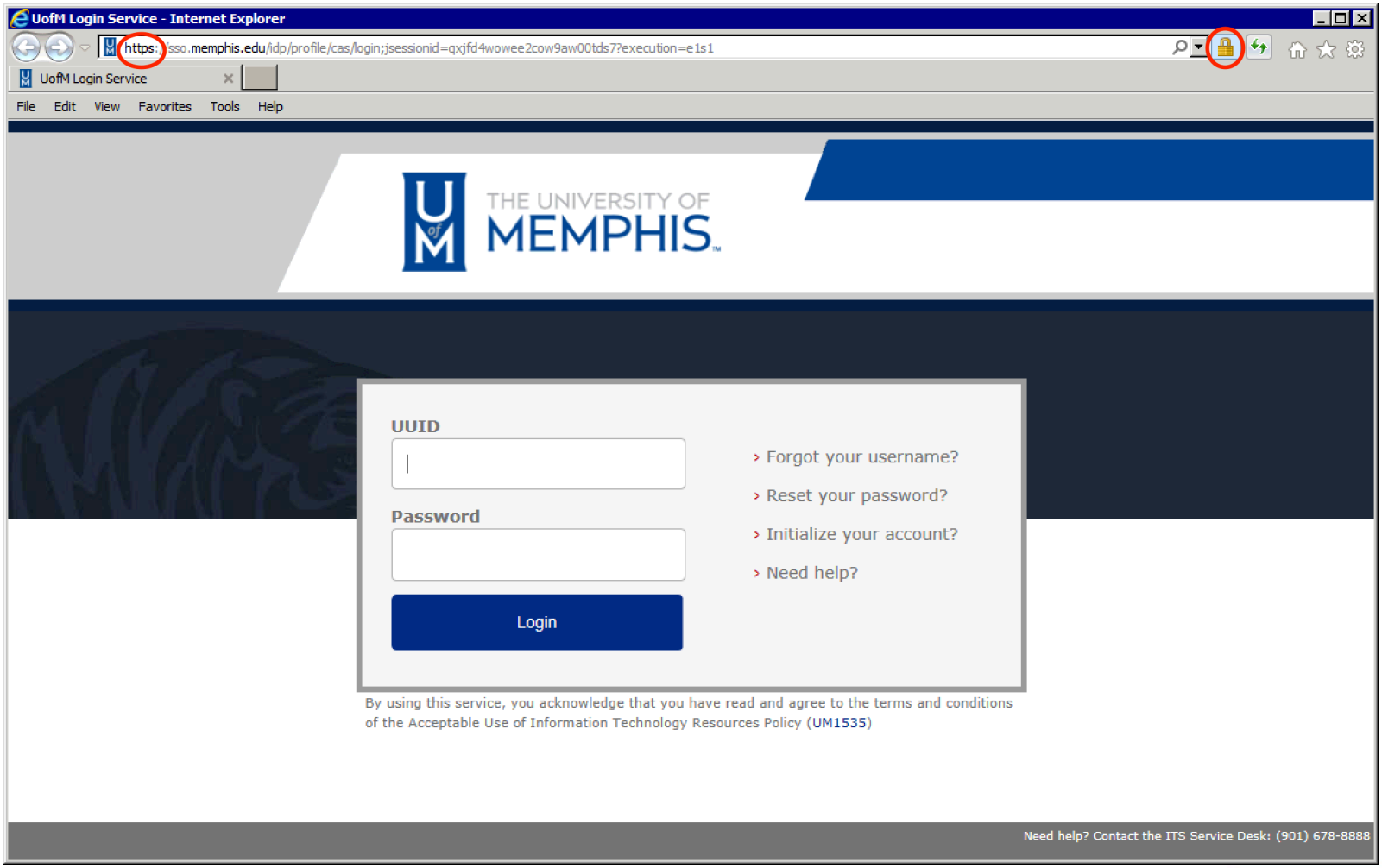
Browsing

Safe Browsing

- Keep your browser software version up-to-date.
- Keep any browser plug-ins up-to-date; especially Adobe Flash and Java, as these are targeted frequently.
- Hover over URLs and links.
- Make use of pop-up and ad blockers.
- Be careful when downloading software from the internet.
- Social networking sites, by definition, collect, maintain, and share personal identification. Be mindful of this when interacting with these sites both on and off campus.
- If a website requests user information of any kind, make sure that website is using HTTPS.
  - HTTPS is the secure web protocol. This can be seen in a web address such as https://www.google.com. This ensures that the specific web session between your browser and the https website is all transmitted in an encrypted manner.

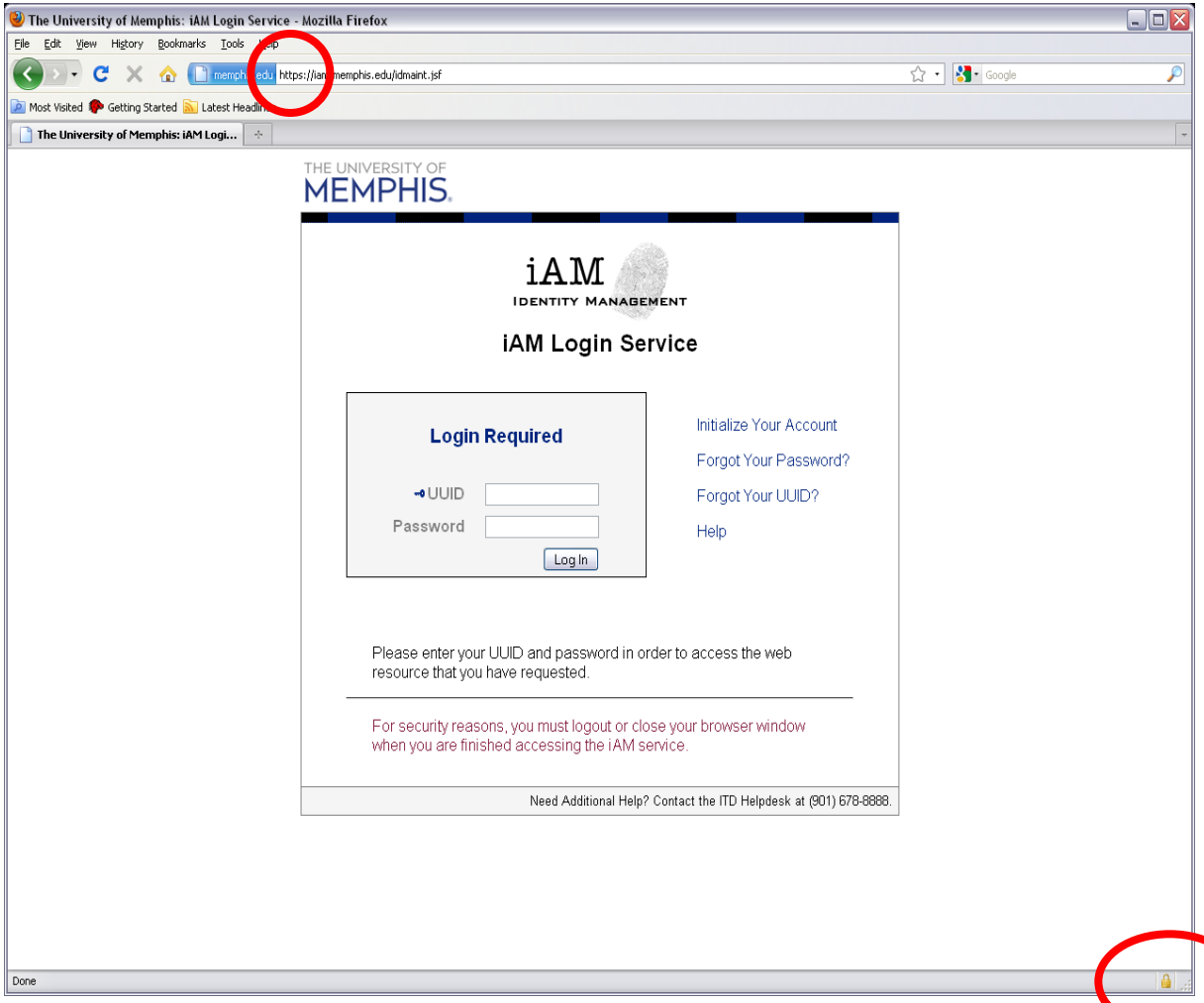
Safe Browsing

Confirming a secure connection (https) with Internet Explorer



Safe Browsing

Confirming a secure connection (https) with Firefox

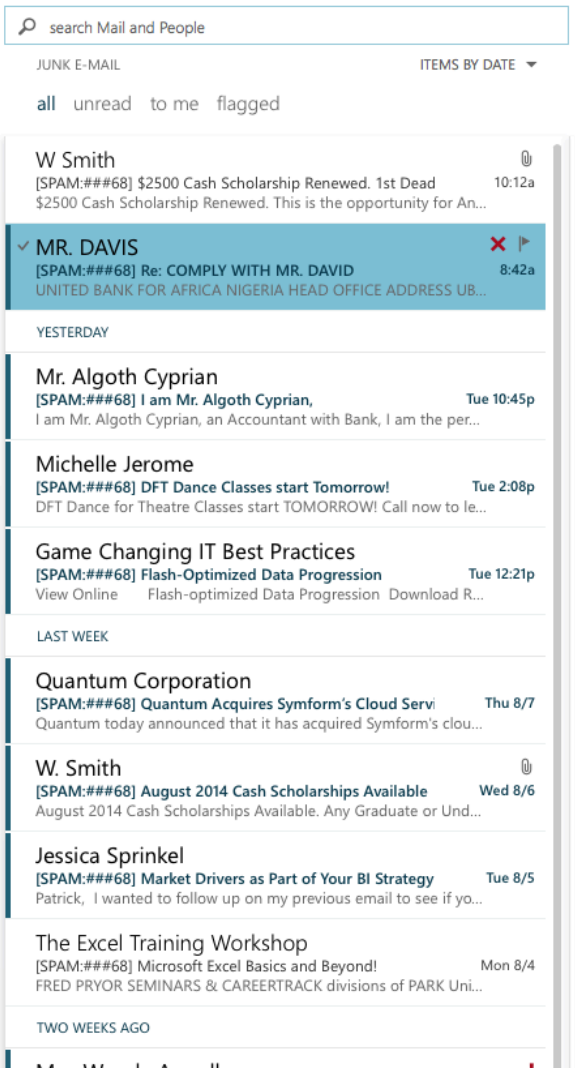


Email

- Keep your email program up-to-date.
- Most email programs do not encrypt your messages, subjecting them to possible interception by others.
- Email Messages can contain a virus or other malicious software that could infect your computer or device
- Never click on a link sent to you in an email unless you are absolutely sure it is safe.
- Never click on or download an attachment from an email unless you are absolutely sure it is safe.
- Be wary of email from an unknown sender.
- Use the “Report Junk” option to mark spam. Review/Empty your “Junk E-Mail” folder periodically.
- The University of Memphis email service (UMMail) includes special server tools to help recognize and quarantine suspicious email.

Email

Be wary of SPAM email. Here is an example of SPAM:



[SPAM:###68] Re: COMPLY WITH MR. DAVID

REPLY

MR. DAVIS <mmurk@exchangenet.net>
Wed 8/13/2014 8:42 AM
Junk E-mail

UNITED BANK FOR AFRICA NIGERIA
HEAD OFFICE ADDRESS UBA HOUSE
57 MARINA P.O. BOX 2406 LAGOS NIGERIA
PHONE: +234 9034075271
WEBSITE: WWW.UBAGROUP.COM
EMAIL: david.mooreu@gmail.com

Hello,
Am David Moore, director cash processing unit, united bank for Africa [UBA the only bank appointed by the A.U. Members lea
Abdel Aziz.Because of the frauds going on in West Africa countries where some innocent beneficiaries were asked to pay in ac
money owed to them. The above Africa union held meeting in Nigeria and resolve to pay all beneficiaries in cash through mea
service. We receive your files from international monetary fund (I.M.F.) as one of the beneficiaries.

Take note; three thousand united state dollars (usd$3,000) have been mapped out for all expenses in taxes and other doccum
want you to bear it in mind that your total fund will be no more one million five hundred thousand united state dollars ($1,50
hundred and ninety seven thousand united state dollars ($1.497,000.00).
If anybody tells you that he is paying you in bank draft or telegraphic money transfer both western union and money gram, d
because due to this frauds no international bank honors our remittance instruction any more that is why we settled to pay in
.

We also received a security report that you paid the fraudsters who have been deceiving you, telling you that they are going t
as a senior banker, controlling this cash payment now, I advise you not to waste your money by paying any body in advance a
instruction, you will receive your money in three days time.

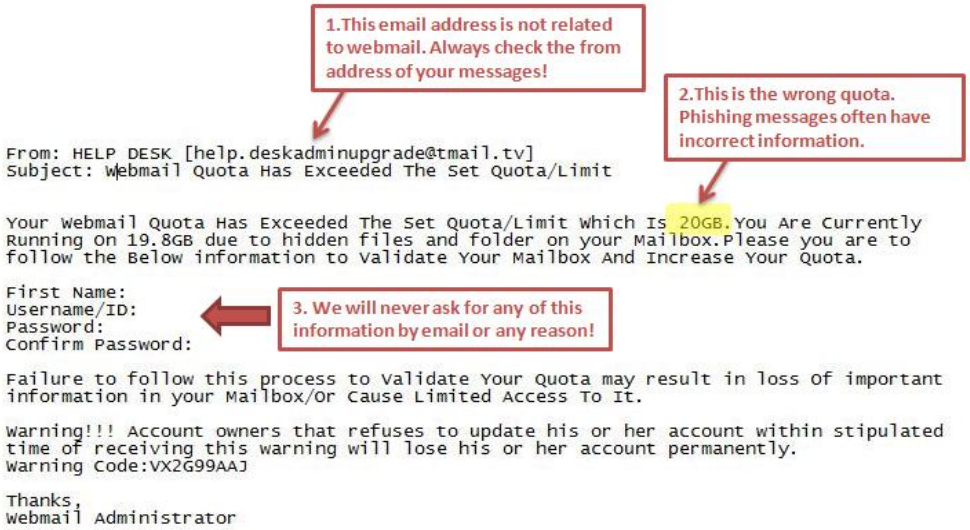
Your fund will now be packaged in box and take to the diplomatic courier service for immediate shipment, I will also send the
attachment to you to see how the money is packed, and I will send you more mails to give you more information for you to k
transaction.
Therefore, do forward your home address and direct phone number to me for quick delivery because time is not in our side.
All the documents will be sent to you if I am assured that you have stopped sending money to those fraudsters.
Am waiting to hear from you with the required information of yours.

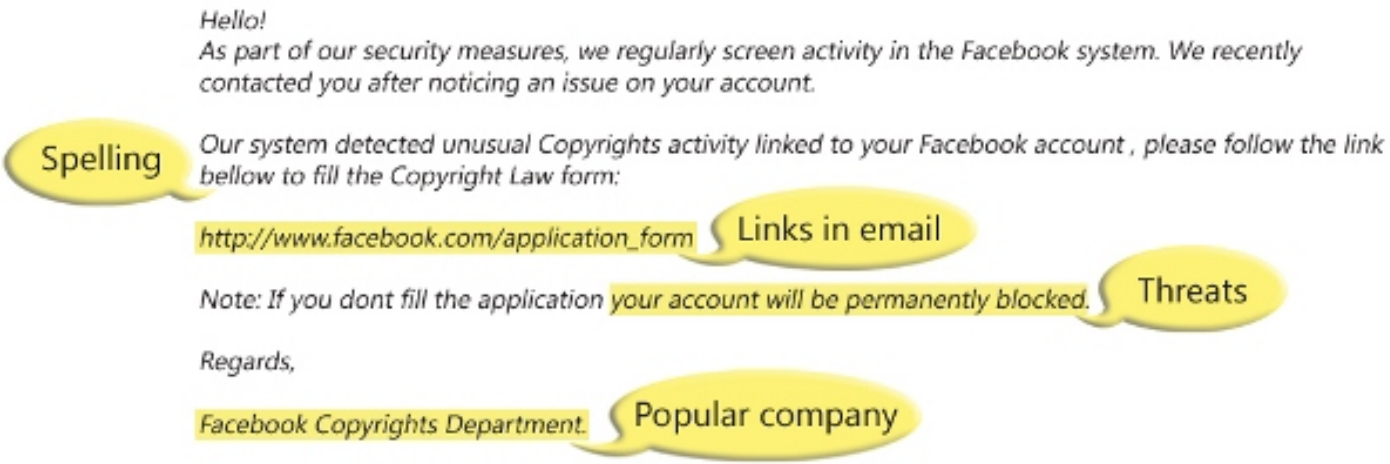
Email

- Phishing
  - A phishing email attempts to fool a user into thinking it originated from a trusted person or business. These often contain web links or attachments asking for personal information or leading to a questionable web site that attempts to collect sensitive information.
  - Typically, phishing emails appear to come from:
    - A trusted source, such as the University of Memphis
    - Co-workers, friends, or family
    - A “help desk” or “service desk”
    - Financial institutions
    - Social media sites

Email

Examples of phishing emails:





Desktop and Mobile Device Security

- Never leave your laptop or device unattended. Thefts do happen.
- Your PC/device should be set to automatically install security updates.
- Have anti-virus and anti-spyware software installed and enabled.
- Ensure your firewall is turned on and set to block all incoming traffic, allowing only the specific services you need.
- The SafeConnect NAC (Network Access Control) requires users to login before accessing the campus network, and also ensures your PC has the latest security updates and anti-virus protection.
- Ensure access to your mobile device is protected with a passcode.
- Consider using a remote tracking/wipe function if supported. For iOS devices, iCloud provides the "Find my iPhone" service for free. Android and other mobile operating systems also have similar functionality.

Data Security and Encryption

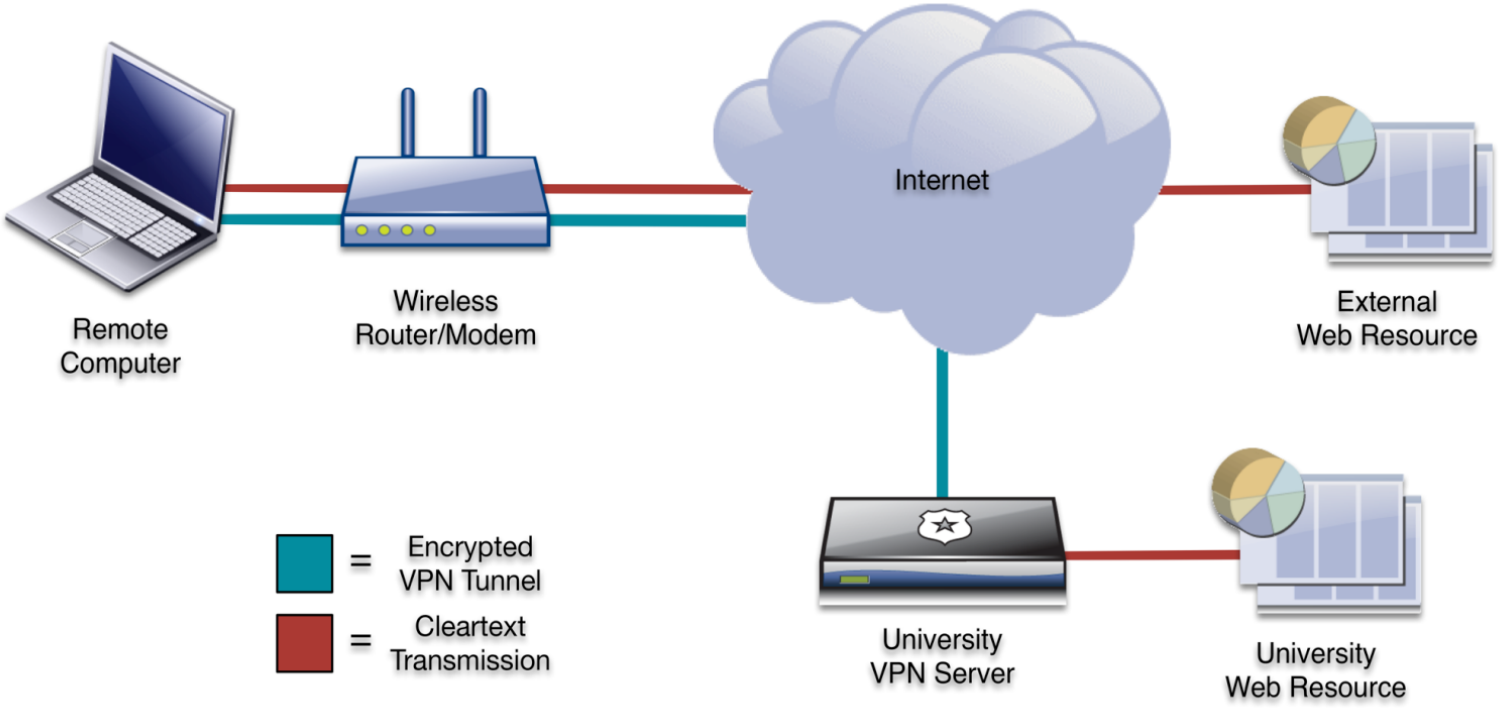
- Sensitive data should be encrypted whenever possible. Here are some examples:
  - Research data
  - Student data (FERPA)
  - Personally Identifiable Information
  - Financial Information
- There are a variety of disk encryption methods available:
  - Microsoft Bitlocker (Windows)
  - Apple FileVault (Mac OSX)
- Keeping sensitive data on campus servers alleviates the risk of a stolen mobile device or compromised home computer.
- When disposing of old devices (desktops, laptops, flash drives, phones), ensure all sensitive data has been securely deleted.

Remote Access / VPN

- VPNs provide secure, encrypted communication between off-campus devices and on-campus resources.
- The VPN application is freely available and fully supported on Windows, Mac OSX, and iOS (iPhone, iPad) devices.
- Some of the typical campus resources accessed via the VPN are Remote Desktop, Banner INB and departmental file shares.
- Remote Desktop applications allow you to control your desktop PC from off-campus. This allows sensitive data to remain on campus.

Remote Access / VPN

The following diagram illustrates how the VPN encrypts your network traffic. Note that only specific connections to on-campus resources are protected by the VPN tunnel.



SANS Securing The Human

- New training in Summer 2015 is mandatory for all Banner Finance / Banner HR users.
- Training must be taken once a year and consists of a group of short videos followed by short quizzes.
- Certificate of completion can be printed at end of assessments.
- http://www.memphis.edu/its/security/security-awareness.php

Reporting Incidents

- Phishing / Spam email messages can be reported to abuse@memphis.edu.
- Real security incidents, such as compromised credentials, compromised system or evidence of data exposure/release, can be reported using an online form at https://www.memphis.edu/its/security/incident-report.php.

Reminders…

- ITS will never ask…
  - … for your password via email or over the phone.
  - … for you to “confirm” your account via email.
  - … for you to follow a link to clean a virus from your email mailbox.
  - … for you to update or increase your email quota.
- When in doubt, forward suspicious emails to abuse@memphis.edu.

Other Resources

- ITS Security website
  - http://www.memphis.edu/its/security
- CIO blog
  - http://blogs.memphis.edu/cio
- Stay Safe Online – National Cyber Security Alliance
  - https://www.staysafeonline.org
- SANS Cyber Security Awareness
  - http://cyberaware.securingthehuman.org

Open Discussion

THANK YOU!

ITS Security

http://www.memphis.edu/its/security/