TECHNOLOGY NEWS

October 2009

Our Mission:

"The mission of the Office of Information Technology is to support and enhance the academic and administrative activities of Southern Methodist University.

To fulfill its mission, IT provides computing, information processing, and communications resources to satisfy the needs of faculty, students, and staff, and offers comprehensive support services to help them use technology effectively and creatively.

IT is dedicated to actively seeking input from it customers, understanding their needs and challenges, and working with them to implement appropriate solutions. In its leadership role, IT is committed to creating and nurturing the vital information technology environment required for SMU to achieve its vision of excellence in education".

Questions, comments, or suggestions?
Contact
IT Communications
oitcommunications@smu.edu

Security Awareness Month

October is national cybersecurity awareness month. Information Technology has planned a number of events throughout the month to increase campus awareness of the various security threats and best practices.

- ***October 2*** Kickoff the month with our Popcorn Event: Hughes Trigg Crossing, 10:00 am – 2:00pm. Pick up a bag of popcorn and some security awareness SWAG!
- ***October 2*** Brown Bag Session: Identity Theft, Hughes Trigg Forum, 12:00-1:00
- ***October 8*** Brown Bag Session: Yours, Mine and Ours-Protecting Personal Information, HR Training Room #208 Expressway Tower, 12:00-1:00
- ***October 16*** Brown Bag Session: Passwords Are Like Underwear… Blanton Building 112, 12:00-1:00
- ***October 23*** Brown Bag Session: Phishing, Spyware and Worms, Oh My! Hughes Trigg Forum, 12:00-1:00
- ***October 30*** Brown Bag Session: Desktop Security, Hughes Trigg Forum, 12:00-1:00
- ***October 30*** Technology Fair Hughes Trigg East Ballroom, Prefunction Area, and Promenade AB, 10:00am-3:00pm

The Technology Fair includes presentations from Apple, Dell, and IT Staff. These presentations will cover a wide range of new technology, IT services, computer security, and other topics. In addition, we'll have a number of fun giveaways and activities. We look forward to seeing you during Security Awareness Month!

SMU Computer Stolen… Do you know what to do?

If you notice that an SMU owned desktop, laptop, cell phone, or other device is missing, you are responsible for reporting that missing asset immediately! SMU is required to investigate the type of information that could potentially be on the device and follow necessary reporting/notification procedures if it involved personal information. SMU is also responsible for notification procedures if a personal device containing sensitive data is stolen. If either a University asset or personal device containing sensitive data is missing, please do the following:

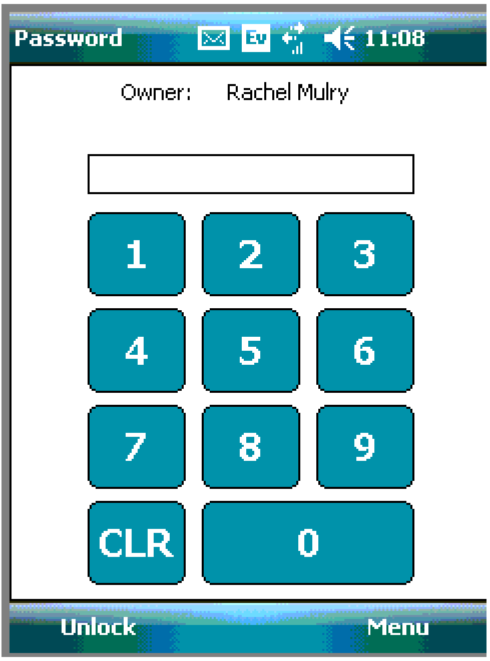
The first step is to contact the IT Help Desk and the SMU PD. The Help Desk will open the appropriate workflow for the investigation. Information Technology will work with the SMU PD to compile the information about the asset.

Second, you will receive a questionnaire about the types of information stored on the machine. It is imperative that you complete that information and return it as quickly as possible. That information determines the notification path that SMU is required to follow.

The rest of the process will be managed by IT and the SMU PD according to internal procedures. Please be sure to report any theft as quickly as possible to limit the potential impact to the University.

Cell Phone Security--- Pin Number to be required

During the month of October, IT will be applying a security policy to help protect SMU data on your cell phones. This policy will configure both personal and departmental cell phones to require a basic 4 digit pin number in order to access the email and contacts on a phone. This policy will affect any Windows Mobile phone configured with active sync, iPhones, and the Palm Pre.



Owner: Rachel Mulry

Cell Phone security is a concern as the password for both email and contacts are stored within the phone. This means that anyone could pick up an SMU Employee phone and potentially access sensitive data contained within the email account. Any sensitive data stored on the phone could also be accessed easily. IT has been researching and testing a number of different security options to ensure that any solution meets the security requirements with minimal impact to the customers.

On October 12, a policy will be applied to all Staff email accounts to enforce a cell phone pin number. At that time, any phones that use Active Sync technology (most Windows Mobile phones) or Exchange Push technology (iPhones), will prompt the owner to accept a security policy from the server. Once this policy is accepted, you will be prompted to configure a 4 digit numerical pin on your device.

You will be able to receive incoming calls and dismiss appointment reminders without entering the pin number. However, to access your contacts, email or place a call, you will need to enter the 4 digit pin number. The pin number will expire every 180 days.

The SMU email servers offer several features for managing your mobile device. These options are available by logging into webmail.smu.edu. Click Options—Mobile Device. Any device that has created a partnership with your SMU account will be listed. You can select the device and display a recovery password in the event that you forget your pin number. If your cell phone is lost or stolen, you can remotely erase the phone as well.

IT has been testing this policy for several months on a variety of phone devices. The policy has worked very well with minimal impact to the customer. Please note, this policy will not affect phones configured with either an IMAP or a POP email account. If your SMU email account is configured using these options, please manually configure a pin number to protect your data. Thank you for helping us protect University information.

Frequently Asked Questions

Will the PIN expire and need reset?

Yes. The Pin number will expire every 180 days and you will receive a request to reset it at that time.

Has this service/policy been tested?

IT has been testing this policy for several months on a variety of phone devices. The PIN policy has worked very well with minimal impact to the customer.

Does this policy impact my phone if I am using POP3 or IMAP protocol?

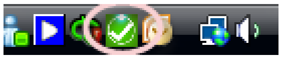
No. This policy will not affect phones configured with either an IMAP or a POP3 email account. If your Smartphone is receiving SMU email using protocol these options, please manually configure a PIN number to protect your data.

Will this affect personal as well as University owned devices?

Yes. This will affect any staff cell phone configured with Active Sync.

Forefront--- Red, Blue, Green, Yellow… do you know what it means?

All SMU Windows computers should have Microsoft Forefront installed providing Anti Virus and Anti Spyware protection. The Forefront icon displays in the system tray located at the bottom right corner of your screen. You may notice, that the icon changes colors depending on the state of the software and your computer system. Do you know what the various colors mean?



- ***Green***: A green icon means that Forefront is correctly installed, updated and working properly.

- ***Grey***: Forefront is configured to run a daily quick scan of your computer to detect any malware or suspicious items. When this scan is running, the icon changes to a grey icon with a spinning wheel. No action is required.

- ***Yellow:*** A yellow icon means that Forefront is reporting a warning. Typically this indicates that the definitions need to be updated or that a system scan has not completed in three days. Simply double click on the icon to determine what action is required.

- ***Blue:*** The Forefront icon will turn blue whenever a non-approved system change is detected. This could include changing your home page, installing a new plug in or other changes to the Windows directory. A pop-up window will appear when the icon changes to this state indicating that Forefront needs your help determining how to handle the item. Simply double click on the Forefront icon and review the list of items. If you initiated the change, simply select Permit as the default action. If you did not initiate the change, please exercise caution!

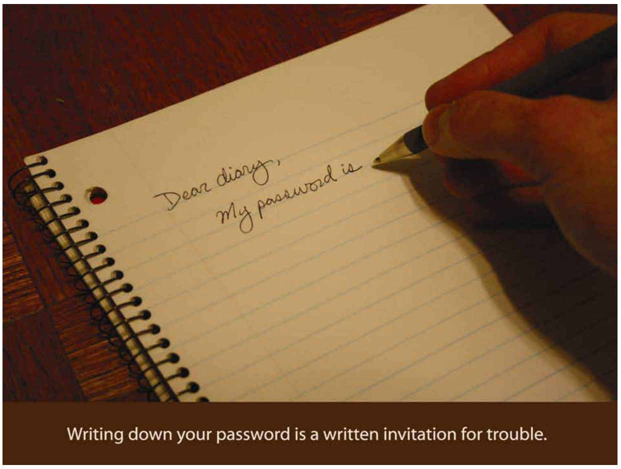
- ***Red:*** The Forefront icon will turn red if malware is detected. In most cases, Forefront will be able to clean the malware for you. Double click on the icon and then select Smart Clean. Once Forefront removes the item, please reboot your computer. In many cases, the remediation is not complete until the computer system is restarted.

The faculty and staff computers on campus are configured to report the status of Forefront to the IT managed server. The IT staff review the malware reports on a daily basis to determine any computers that need follow up attention. This allows IT to respond more quickly to malware infections on a machine and better protect the SMU network.

Please note, home computers or computers in the residence halls with Forefront installed do not report to IT. Please observe the Forefront icon and ensure that your system is adequately protected.

Password Security

Your passwords are very important to the security of all the information you access. Your personal information is equally as important as the personal information of our SMU community. Many of us at SMU handle personal information such as: credit card information, medical information, insurance, grades, donor names, donation amounts, salaries, etc. A single password giving access to the right information could compromise thousands of accounts. Every bit of the information on our computers, networks, and online accounts must be treated as being confidential, even if you don't think it is.



Writing down your password is a written invitation for trouble.

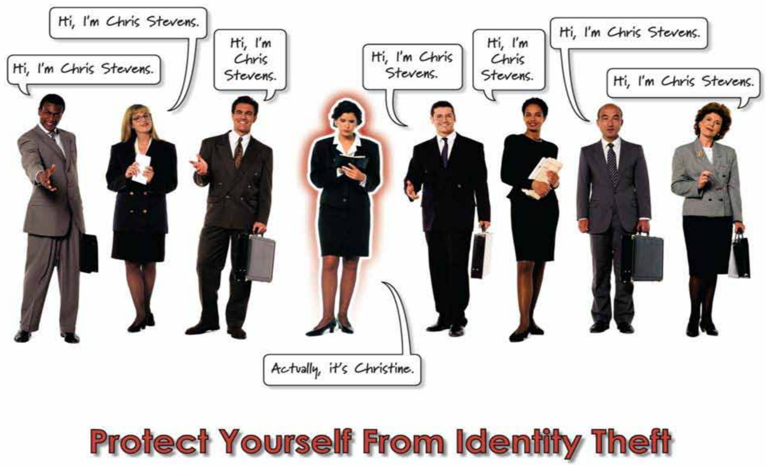
Keep in mind, passwords are like underwear….

- Change them often
- Don't share them
- Don't leave them lying around
- The stronger the better

A strong password should use a mix of upper and lower case letters, digits, and special characters. Avoid using words that can be found in a dictionary and do not use personal information such as birthdates, names, or anniversary dates. Consider using a "pass phrase" as your password. Use the first letter of each word in a sentence, phrase, poem, or song title as a password. Be sure to add in upper and lower case, numbers, and special characters. The longer a password, the stronger it is. If you have established a password but it is not strong – change it!

To test out a password and determine its strength, try the password checker from Microsoft: www.microsoft.com/protect/yourself/password/checker.mspx

Preventing Identity Theft



Identity theft is a growing problem that affects thousands of individuals annually. Sometimes it occurs as the result of negligence on the part of a company or business that has access to your personal information. Sometimes, it is the result of our own behaviors.

What can you do to help prevent identity theft?

- Verify that your computer is in good health (see the Desktop Security article for a checklist)
- If you have an SMU laptop, ensure that it is encrypted. That way, if it is stolen, the information contained on that machine can not be retrieved
- Protect your various accounts with a strong password
- Be careful of clicking links in suspicious emails
- Never respond to email that requests your information, such as account numbers, passwords, personal data
- Never supply credit card information via email, fax or on any website that doesn't display the "security lock" icon

There are a few additional steps that do not involve a computer!

- Be wary of any phone calls requesting personal information
- Shred all paper or store them securely

Desktop Security Checklist

Regardless of your computer platform (Mac, Windows or Linux), desktop security is a concern for all of us. Malware and other security threats can not only jeopardize information stored on our computers, but can also threaten information stored in other accounts—such as bank accounts, Enterprise Systems, etc. The following checklist should be completed on a regular basis.

- ***Run all security updates for the operating system***: These updates are released on a monthly basis although some critical updates are released outside of the normal cycle. It is imperative that these patches are applied promptly.
- ***Run all security updates for the various applications installed on your computer:*** Each application vendor provides updates for their application which addresses functionality issues as well as security issues. It is important to apply these updates whenever they are available from the vendor.
- ***Double check your security software***: Whatever security software you have installed on your computer, it is important to check that it is updating and working correctly on a regular basis. Many viruses will target the an-

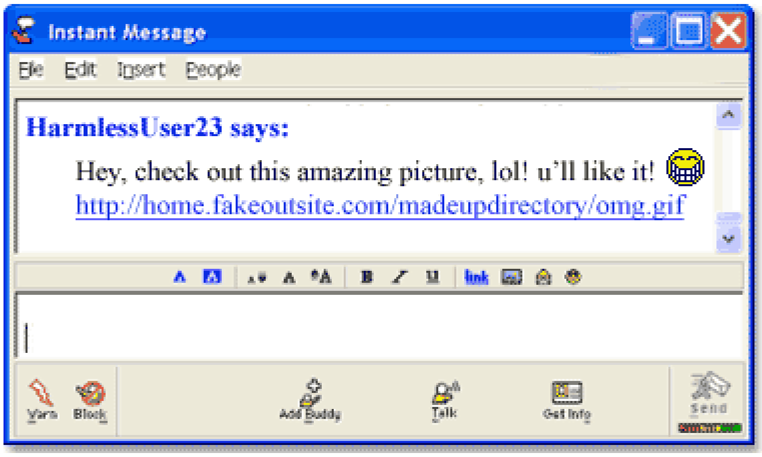
tivirus applications and shut down key components. Although the anti virus application appears to still be working, the application may not be receiving updates or other features may be preventing it from scanning. Verify that your antivirus and antispyware software is enabled, updating and scanning regularly!

- ***Verify firewall settings***: A desktop firewall should be enabled on your computer. Both Mac and Windows Operating Systems have built in firewall capabilities. Some security products also offer this functionality (such as Norton). Each computer should have a firewall enabled to prevent or minimize the danger of an incoming or outgoing attack.
- ***Be careful of file sharing***: If you have file sharing enabled, verify that the shares are not open to everyone but restricted to a specific group or individual. Be very careful of any type of application which incorporates a shared folder (such as LimeWire or other Peer to peer applications) as these render your computer vulnerable to attack. If you need to share files, consider using locker.smu.edu as a safer alternative.
- ***Protect your computer with a password and screen saver lock:*** Once you have logged into your computer, the data stored on that computer and any accounts that are accessed with stored passwords are available to anyone with physical access to your machine. Protect this data by requiring a start up password. Be sure to also set a screen saver password so that the data is always protected.

IT has several client security management procedures in place to help protect IT Managed computers. However, you are responsible for checking your home computers and ensuring the security of your office machine as well.

Email, Texting, and IM Security

Most of us rely heavily on electronic communication. Whether we use it to stay connected to others or to solve business problems, we extend a great deal of trust to these technologies. However, individuals who write virus or malware programs target these technologies to capture your data.



HarmlessUser23 says:

Hey, check out this amazing picture, lol! u'll like it!
http://home.fakeoutsite.com/madeupdirectory/omg.gif

Much has been shared about email security over the past several years. Phishing emails still run rampant, but individuals are exercising a little bit more caution in responding. These emails specifically request that you provide personal information such as account information, passwords, social security numbers, etc. The messages are typically poorly written and the from and reply to address does not match the company they supposedly represent. Please continue to exercise caution with any email that requests that you provide personal information.

Because people are generally becoming more cautious about these emails, malware writers are turning to other mediums including Texting and Instant Messaging. These messages typically include a link which delivers the malware to your device. In fact, a majority of the latest viruses and network threats are being released through these mediums.

- Make sure your password is strong.
- Don't automatically accept incoming messages or file transfers. Change the privacy settings within your IM client to ensure that you have control over who can contact you.
- Don't discuss confidential information via IM. Most IM clients do not offer the same level of security as an email client. Therefore, the conversations are sent over the internet in plain text. Confidential information could easily be intercepted if transmitted via IM.
- Watch for security updates for your IM client or cell phone.
- If you don't recognize the sender of the message, don't continue the conversation.